Академія правових наук України
Науково-дослідний центр правової інформатики

НОРМАТИВНО-ПРАВОВІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ УПОРЯДКУВАННЯ ІНФОРМАЦІЙНИХ ВІДНОСИН

Київ - 2009

Академія правових наук України
Науково-дослідний центр правової інформатики

НОРМАТИВНО-ПРАВОВІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ УПОРЯДКУВАННЯ ІНФОРМАЦІЙНИХ ВІДНОСИН

НАУКОВО-МЕТОДОЛОГІЧНИЙ ПОСІБНИК

За редакцією
В. Тація, В. Тихого, М. Швеця

Київ - 2009

УДК 342.9
ББК 67.401

Рекомендовано до друку
Вченою радою Науково-дослідного центру правової інформатики
Академії правових наук України
(протокол № 12 від 12.10.2009 року)

Нормативно-правові та методологічні засади упорядкування інформаційних відносин: науково-методологічний посібник / авт. колектив: В. Брижко (науковий керівник проекту), В. Цимбалюк, М. Швець; за ред. В. Тація, В. Тихого, М. Швеця. – К.: ТОВ "ПанТот", 2009 р. – 324 с.

Рецензенти: Р.А. Калюжний, доктор юридичних наук, професор,
академік Міжнародної академії інформатизації,
начальник кафедри Київського національного
університету внутрішніх справ України
О.В. Кохан, доктор юридичних наук, старший науковий співробітник,
начальник відділу Міжвідомчого науково-
дослідного центру з проблем боротьби з організо-
ваною злочинністю при Раді Національної безпе-
ки і оборони України

ISBN 978-966-1531-05-4

Науково-методологічний посібник містить методично оброблений та систематизований навчальний матеріал з теоретичних та практичних питань упорядкування суспільних відносин щодо інформації, інформатики та інформатизації у зв'язку із становленням інформаційного права як нової юридичної науки та навчальної дисципліни в умовах формування інформаційного суспільства.

Рекомендується для фахівців з державного управління, юристів, викладачів, аспірантів, студентів юридичних та інших закладів щодо законотворчої, правозастосовної, правоосвітньої діяльності у сфері інформаційного права та інформаційного законодавства.

Підготовлене та видано в рамках реалізації науково-дослідної роботи за темою "Дослідження у сфері упорядкування інформаційних відносин в контексті розбудови в Україні розвинутого інформаційного суспільства" бюджетної програми: "Виконання загальнодержавних організаційних, інформаційно-аналітичних та науково-методологічних заходів з питань євроатлантичної інтеграції" за сприяння Державного управління справами та Національного центру з питань євроатлантичної інтеграції України.

ISBN 978-966-1531-05-4

УДК 342.9
ББК 67.401

З М І С Т

Перелік скорочень

ВОІС – Всесвітня організація з інтелектуальної власності
ДСТУ – державний стандарт України
ЗАС – апаратура зв'язку, що засекречує
ЗМІ – засоби масової інформації
е-гроші – електронні гроші
е-документ – електронний документ
е-банкінг – електронний банкінг
м-банкінг – мобільний банкінг
е-підпис – електронний підпис
е-платежі – електронні платежі (електронні розрахунки)
е-пошта – електронна пошта
е-середовище – електронно-інформаційне середовище
е-урядуванне – електронне урядування
EVROVOC – багатомовний тезаурус інститутів ЄС для роботи з документальною інформацією
ЄС – Європейський Союз
ІКТ – інформаційно-комп'ютерні технології
ІПС – інформаційно-пошукова система
ІП – інформаційні продукти
ІР – інформаційні ресурси
ПК – персональний комп'ютер
PIN-код – персональний ідентифікаційний номер
РЄ – Рада Європи
СОТ – Світова організація торгівлі
ТЗОІП – технічний захист обробки та передачі інформації

ВСТУП

Згідно зі статтею 3 Конституції України людина, її життя і здоров'я, честь і гідність, недоторканість і безпека визнаються вищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави.

Виконання зазначеного обов'язку держави перед людиною та суспільством значною мірою пов'язано з упорядкуванням та регулюванням (управлінням) інформаційних відносин.

В сучасних умовах завдяки розвитку процесів інформатизації поширення інформаційно-комп'ютерних технологій та мереж, упорядкування та регулювання юридичними та організаційними засобами інформаційних відносин щодо реалізації потреб людини, суспільства і держави в політичних, економічних, технологічних, медичних, освітянських, духовних, правоохоронних та інших процесах набуває значення цільового напряму суспільного розвитку, заснованого на пізнанні його законів та аналізі наслідків. Інформатизація суспільного життя все більш активно впливає на прискорення розвитку світової економіки, чим зумовлює соціальну трансформацію суспільства. Таке трактування приводить до розуміння ролі інформації як керівного фактора управління суспільного життя, за яким будь-яка динамічна система органічно пов'язана з перебігом інформації. Зазначене в аспекті методологічних та інформаційно-правових засад потребує від державної інформаційної політики корегування у напрямі приведення її до системності в упорядкуванні інформаційних відносин. У цьому є сутність проблеми, що підтверджується також наступним.

Упродовж багатьох років державна інформаційна політика в Україні охоплювала, головним чином, проблеми, пов'язані з діяльністю засобів масової інформації. На початку 1990-х рр. зміст державної інформаційної політики було дещо розширено і до неї потрапили окремі елементи захисту прав громадян й організацій на загальнодоступну інформацію, гарантованих Конституцією країни, запроваджено право власності на інформацію, а також визначені аспекти інформаційної безпеки.

З кінця 1990-х рр. формулюються і розвиваються принципи і положення державної політики інформатизації, вираженої в різних програмах інформатизації. Основний зміст цього зводився з невеликими варіаціями до забезпечення науково-технічних, виробничо-технологічних і організаційно-економічних умов створення і застосування інформаційної інфраструктури та інформаційних технологій. При цьому політика інформатизації практично була відокремлена від політики, що ведеться державою у сфері засобів масової інформації.

Новий імпульс в розвитку державної інформаційної політики виник у зв'язку з усвідомленням необхідності розвитку в Україні так званого інформаційного суспільства як однієї з головних умов її політичного і соціально-економічного руху вперед і закріплення статусу самостійної держави. Необхідність вирішення зазначеної масштабної задачі вимагає ефективності в управлінні діяльністю відносно усіх видів інформаційних ресурсів, елементів інформаційно-телекомунікаційної інфраструктури, державної підтримки ринку інформаційних технологій, засобів, продуктів і послуг, регулювання діяльності державних електронних і друкованих засобів масової інформації тощо.

Ефективність державного управління передбачає наявність не тільки доктринальних положень щодо інформаційної політики, а й необхідність у застосуванні науково-методологічних підходів до систематизації у створенні та, в подальшому, удосконаленні нормативно-правової бази інформаційної сфери. Мова йде про актуальну потребу у створенні "інформаційної конституції України", яка відповідає принципам Основного Закону України – Конституції України, а також – положенням відповідних європейських стандартів, вироблених практикою світової цивілізації. Для вирішення такої задачі має бути розроблена система інформаційного права та інформаційного законодавства як форма організації упорядкування та регулювання інформаційних відносин на основі функціонального призначення інформаційного забезпечення, спрямована на становлення інформаційного права як нової галузі права та систематизацію інформаційного законодавства України у вигляді кодифікованого акта.

В Україні дослідженню питань інформаційного права та систематизації інформаційного законодавства присвячені роботи учених І. Арістової, О. Баранова, В. Брижка, В. Гавловського, М. Гуцалюка, І. Жиляєва, Є. Захарова, Р. Калюжного, О. Копана, А. Новицького, Н. Новицької, В. Речицького, Р. Романова, А. Семенченка, О. Фролової, В. Фурашева, В. Цимбалюка, В. Хахановського, М. Швеця, А. Яременко та ін.

Вченими та практиками країн пострадянського простору ведеться значна робота щодо дослідження проблем інформаційного права та інформаційного законодавства. Ці проблеми находять відображення у працях таких російських учених, як А. Агапов, Ю. Батурин, І. Бачило, А. Венгеров, О. Гаврилов, Б. Герасимов, О. Городова, В. Дозорцев, А. Єфремов, В. Іванський, В. Ісаков, С. Ігошін, П. Ковальова, В. Копилов, Б. Кристальний, О. Кутафін, М. Лапчинський, А. Левенчук, І. Маміофа, А. Миньков, С. Мунье, М. Рассолов, І. Рассолов, Ю. Тихомиров та багато ін.

Роботи вказаних та інших авторів, безумовно, мають наукове і практичне значення, але слугують лише забезпеченню освітньої діяльності щодо інформаційного законодавства. На превеликий жаль, на сьогодні нема цілісного уявлення про єдину систему інформаційного права та інформаційне законодавство, а також щодо методології удосконалення інформаційного законодавства. Так, наприклад, книги О. Городової [61], Н. Ковальової [62] мають назву "Інформаційне право", хоча йдеться в них про аспекті інформаційного законодавства, де фрагментарно вкраплені думки про інформаційне право, та нема мови про систему з наукового становлення інформаційного права та інформаційного законодавства.

Щодо поняття "методологія", то маємо зазначити наступне. Наукова методологія, як сукупність принципів, способів, операцій та прийомів наукового дослідження ("дослідження" – від грец. "історія") щодо пізнання дійсності, у неекспериментальних (зокрема, юридичних) науках є розумовим процесом діяльності людини завдяки використанню досягнень формальної і діалектичної логіки із збирання різних за предметом пошуку, аналітико-синтетичною оцінкою, систематизацією, обгрунтуванням достовірності відомостей щодо нових знань, які й складають науково-експертну оцінку пропозицій. Головне у цьому – систематизація відомостей, отримання нових знань та наявність вибору.

Раніше у школі, вузі, на превеликий жаль, не звертали та й зараз не дуже звертають уваги на цю дисципліну ("Методологія"). Усе було обмежено ідеєю планового ведення господарства завдяки "експертним" висновкам, які спрямовані відповідним керівником, а неминучість прогресивного розвитку суспільства пояснювалась гаслами єдиної ідеології. Багато фахівців і зараз виконують роботу аналітичного змісту за своєю

спеціальністю, не дуже звертаючи уваги на знання методології науково-експертної оцінки проектів, пропозицій тощо. І це має місце де завгодно, навіть у такій "тонкій" і делікатній сфері, як юриспруденція (приклад див. у [214]) – подібно як у Наполеона, який у свій час наказав юристам – *пишіть* (конституцію) *коротко та незрозуміло*. Ця конституція вважається кращою у світі, яку продовжують переписувати в сучасні національні законодавства. Тобто можна говорити, що було і має місце виконання замовлень на отримання бажаних результатів усупереч результатам наукових досліджень, наукової експертизи та необхідності спрямування до порядності у людських стосунках.

Даніель Белл, один з авторів концепції "постіндустріального суспільства" [67], зазначив, що *"ідеологія вмирає і на її місце приходить експертне, наукове знання, бо ідеологія і адекватний опис та розуміння світу несумісні"*.

Відсутність дійсно незалежної наукової експертизи (зокрема, в плані експертизи законопроектів) полегшує життя міністерствам і комітетам, хоча для економіки і соціальної сфери результати такого порядку наводять на сумні роздуми – політики, урядовці приходять, сприяють лобіюванню законів завдяки своїм бажанням та уявленням, беруть після того, що зможуть, і йдуть, а не дуже адекватна реаліям потреб більшості суспільства система продовжує існувати. Це може бути свідченням відсутності у державі громадянського суспільства та справжнього верховенства права.

Об'єктом роботи є інформаційне право як нове явище та система.

Головна мета роботи спрямована на виконання організаційно-правових заходів, що визначені Законом України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 09.01.2007 р. № 537-V, пунктом 2 "Законодавче забезпечення розвитку інформаційного суспільства" Розділу III "Національна політика розвитку інформаційного суспільства в Україні" якого встановлено: *"З метою підвищення ефективності розвитку інформаційного суспільства необхідно створити цілісну систему законодавства, гармонізовану з нормами міжнародного права з питань розвитку інформаційного суспільства, зокрема здійснити кодифікацію інформаційного законодавства"* [37].

Зазначене безпосередньо пов'язано із становленням нової юридичної науки та наукової дисципліни – "Інформаційне право", що передбачає наявність у державі спільних принципів наукового формування інформаційного законодавства, яке схильне до перманентних змін, та потребу у створенні базового, цілісного нормативно-правового акта для всієї інформаційної сфери держави.

Засвоюванню та подальшому удосконаленню знань стосовно інформаційного права та інформаційного законодавства у процесі самостійної роботи над книгою має обов'язково сприяти активна пізнавальна та творча праця.

Розділ 1. ПРАВА ЛЮДИНИ І СВОБОДИ ГРОМАДЯНИНА У ЗВ'ЯЗКУ З СТАНОВЛЕННЯМ ІНФОРМАЦІЙНОГО ПРАВА

1.1. Генезис та розвиток прав людини і свобод громадянина

1.1.1. Становлення прав людини і свобод

Права людини і основоположні свободи громадянина як деякий набір правил поведінки з дотримання взаємних зобов'язань і відповідальності людини, суспільства і держави з'явилися в Древній Греції [68, с. 18].

Застосування історико-правового методу дослідження надає змогу відзначити те, що процеси визнання державою формального закріплення в законодавстві невідчужуваних (природних) прав людини і свобод тісно пов'язані із становленням адміністративного права, про що йдеться, зокрема, у роботах [69, с. 9; 70, с. 355-437]. Разом із тим, погляди щодо важливості існування зазначених правил та необхідності їх судового захисту у відносинах особи з владою тривалий час мали більше морально-етичний, ніж практичний зміст [71, с. 6, 7].

У перших з відомих нам пам'яток античної письмової творчості – поемах Гомера "Іліада" і "Одіссея" (до VIII ст. до н. е.) на основі міфології втілена не тільки сувора героїка воєн, а й радість творчості, творчої праці і мирного життя, заснована на повазі до людини, на пробудженні в неї кращих гуманістичних почуттів. Гомер наводить точні порівняння, що свідчать про глибоку життєву спостережливість, розрізняє добро і зло, але що є добро і зло "самі по собі" – на це в нього відповіді нема. Водночас згадується уже про правила поведінки, що мають законодавчий зміст. За переказом, син одного з богів і смертної жінки Тезей був першим царем, що установив законодавство в Аттиці [68, с. 18].

У роботі [72, с. 21] Л.А. Пальцева вказує, що *"вже у Гомера бачимо чітке уявлення про суд як про обов'язковий атрибут нормально побудованого людського суспільства. Полісу з його розвинутими органами управління у Гомера протистоїть суспільство диких (agrioi), яке не знає ні дорадчих зборів, ні судів, ні того, що Гомер позначає "gevmi" (у множині – gevmiste), тобто усних неписаних законів (звичаїв), на підставі яких провадиться правосуддя (Homer. Od., IX, 112, 189; 215)"*. Як зазначається у [69, с. 10]: *"Судочинство в гомерівському суспільстві відправляли dikaspovloi – наглядачі справедливості (divkh). Але при наближенні до проблеми виявляється, що в ролі суддів виступали царі або геронти – їх радники, близькі родичі"*.

Початком пошуків істини слова, а також щодо цивільних прав та свобод можна вважати так звану "Афінську школу філософії" [73]. Цивільні права в Греції були нерозривно пов'язані з особистісним початком у громадському і господарському житті, з прагненням до свободи і демократії, з формою прямого народного правління.

Вже в V ст. до н. е. в Афінах раз на місяць проходили народні збори, у яких брали участь усі громадяни, і кожний міг висловити свою думку. Рішення приймалися більшістю голосів, усі державні посади заміщалися шляхом жеребкування, що унеможливлювало інтриги. Тільки воєначальники обиралися прямою подачею голосів і переобиралися через рік. Судові справи розглядалися присяжними. Хоча не було ні писаної конституції, ні законів, реальна демократія захищалася контролем над посадовими особами, над всіма органами влади. Будь-який громадянин міг висунути обвинувачення в "протизаконності" проти ініціатора законодавчої пропозиції, звернутися до "Ради п'ятисот" з обвинуваченням проти будь-якої посадової особи в недотриманні суспільної угоди. Афінська демократія не задовольнялася лише частою зміною посадових осіб – вони знаходилися під контролем постійних перевірок. Але рішення народних зборів припинялося до судового розгляду.

Притаманним для греків є відкидання інакомислення, незгоди з волею більшості, про що засновник софістики Протагор з Абдерит (490-420 рр. до н. е.) так й стверджував – *істина визначається більшістю*. Але в такому арифметичному визначенні істини не бачили справедливості ні Сократ (469-399 рр. до н. е.) [75, с. 53-60], ні Платон (428-347 рр. до н. е.) [74; 75, с. 67-76], ні Аристотель (384-322 рр. до н.е.) [75, с. 76-85]. Сократ зауважував: *"Ни кормчего, ни плотника, ни флейтиста никогда не выбирают большинством голосов, – в любом деле, и уж конечно, в деле государственной мудрости требуется специалист"* [73, с. 79]. Разом з тим, англійський філософ К. Поппер вважає, що філософія індивіда почалася з Протагора, а в легендарного чудакуватого мудреця Сократа індивідуальна людина є вже найважливішою. *"Что есть справедливость сама по себе? Пора человеку обратиться к этому вопросу от суетной возни честолюбий. Пора стремиться к знанию, но истинному, а не мнимому, неустанно преследовать истину, но божественную, а не суетную, быть другом мудрости, никогда не считая себя мудрецом. Я знаю, что ничего не знаю"*, – такі вів він діалоги з учнями першої приватної школи (від грецького "схоле" – дозвілля) філософської "любомудрості". Платон, один з його улюблених учнів, говорив: *"Человек есть мера всех вещей. ...Философия должна способствовать тому, чтобы каждая последующая жизнь была справедливее предыдущей"*. Головне призначення філософії – знання справедливості і несправедливості; філософська істина є насамперед справедливість. Пізніше, у II ст. н. е., доброзичливий і щирий Марк Аврелій, що писав про тлінність тіла, нестійкість душі і невірогідність слави, говорить, що в цирої філософії найблагороднішa мета – зберегти людину від марнославства: *"Дело философии просто и скромно: не увлекай меня на стезю тщеславия"* [75, с. 103-110; 76, с. 46-49; 77].

Після насильницької смерті Сократа Платон зненавидів афінську демократію, цей режим, що псував справедливість і убив його вчителя. Він присвятив своє життя ідеї створення моделі нової держави, але помер, не закінчивши книг "Держава" і "Закони". Його філософія була стурбована не тим, щоб розбудити совість у громадянах, а тим, щоб представити їм іншу картину світу, нехай не досконалу, але в який більше істини.

Аристотель, що займався в Академії Платона 17 років, вчив вже своїх учнів духовної цілісності, наставляючи їх не змішувати слова з речами, а думки зі словами, писав: *"Только человек способен к восприятию таких понятий, как добро и зло, справедливость и несправедливость и т.п. Понятие справедливости связано с представлением о государстве, так как право, служащее мерилом справедливости, является регулятором общественных отношений"*. У подальшому, в V столітті, ця думка висловом Цельса увійшла до першого кодексу законів (Юстініановий кодекс), що створив основу законодавства західноєвропейських країн: *"Право есть гармонический порядок интересов и улаживания их столкновений"*.

Коли в Греції вже була могутня школа філософії, історик Геродот (484-425 рр. до н. е.) [76, с. 273-275] відзначав: *"Афины, ранее бывшие силой, теперь, освободившись от тиранов, стали еще сильнее. Афиняне выросли и стали могучи, и обнаружилось ясно, притом во всех проявлениях жизни, что за великое дело равноправность. Очевидно, что, будучи в подчинении, они намеренно работали плохо, потому что работали на деспота. Достигнув свободы, они проявили огромную энергию, так как каждый мог с полной силой отдаться своей цели"*.

З давнини свободу символізував відкритий простір площ-форумів у містах, де різноголосий, невимушений шум життя свідчив про розкріпачення людей і був ідеалом древніх греків, а потім і римлян. Коли ж життя суспільства переходило до спланованої "єдності" маніфестацій і "тиранії" демократів та імперії, то особисті ідеали переміщалися ззовні в середину будинків і храмів, де за їх стінами людина сподівалась зберегти свої почуття і прагнення до свободи.

Неповнота прав, обмеження свободи слова і недосконалість античної демократії призвели до морального падіння і погубили афінський поліс. Філософ Антисфен (445-360 рр.) якось порадив афінянам прийняти постанову – *"Считать ослов конями"*. Коли це сприйняли як безглуздість, він зазначив: *"А ведь вы простым голосованием делаете невежественных людей – полководцами"*.

Щодо правосуддя у Римі, то А. Джонс у книзі "Загибель античного світу" зазначає [78, с. 307-378], що коли до влади прийшов Діоклетіан (римський імператор у 284-305 рр.), в Римській імперії було зовсім мало судів. Муніципальні суди, що ніколи не були особливо впливовими, поступово зникли. Як правило, судом першої інстанції був суд правителя провінції. Деякі з них мали юридичних помічників iuridicus, а проконсули Африки та Азії – відповідно двох та трьох легатів. Всі апеляції надходили імператору або його преторіанському префекту. Діоклетіан значно поліпшив ситуацію. Першою радикальною зміною стало запровадження інституту defensor civitatis, завданням якого був розгляд скарг на ім'я правителя провінції з цивільних питань. Імператор низько оцінював якість правосуддя на місцях. Тому апеляції ним приймалися без будь-яких обмежень.

Крім загальних, у Римській імперії існували і спеціальні суди, зокрема адміністративні. Останні очолювалися керівниками магістратів (адміністрації). Однак метою адміністративного судочинства було передусім забезпечення притягнення до відповідальності за правопорушення у сфері управління громадян та службовців (адміністративний процес відзначався суто деліктним змістом). Тільки привілейовані (багаті) особи могли розраховувати на захист їх публічних прав та інтересів судом магістрату.

Отже, про можливість захисту простим громадянином своїх прав у відносинах із верховною владою у стародавніх Греції та Римі не йшлося. Це не виключало розгляду судом скарг громадян на дії чиновників нижчого рангу, зокрема з приводу захисту приватної власності. Правосуддя того часу мало на меті не стільки захист громадянина, скільки підтримання авторитету влади імператора у свідомості простих громадян. Проте природно права і свободи завжди були та є більш пріоритетними ніж підтримка особистих інтересів владної особи, але далі міркувань про це не йшлося. Марк Аврелій (121-180 рр.), імператор, філософ-стоїк та великий мораліст [75, с. 103-110], у своїх записках "Наодинці із собою. Міркування" [77] наводить слова філософа-стоїка Епіктета: *"Никто не желает быть виноватым, никто не хочет жить в заблуждениях, неправедно, никто не выбирает себе нарочно такой жизни, от которой он будет печалиться и мучиться, никто не скажет, что ему хочется жить скверно и развратно. Значит, все люди, живущие неправедной жизнью, живут так не по своему желанию, а против воли. Они не хотят ни печали, ни страха; а между тем постоянно страдают и боятся Они делают то, чего не хотят делать. Стало быть они не свободны"*.

При всій значимості права громадян Древньої Греції та Риму не можна вважати правами людини. Права ці існували не тому, що визнавалися за будь-якою особою, а випливали з розуміння про особливі властивості вільних людей (не рабів, не варварів) і були нерозривно пов'язані з адекватним державним устроєм. За Аристотелем, держава зобов'язана піклуватися тільки про громадян, але не про рабів. Ціль держави – благо

для обмеженого кола. Рабство, у кінцевому рахунку, означало не тільки несвободу для "негромадян", але й вело до обмеження свободи особи.

Про несправедливість рабства говорилося ще філософами Древньої Греції і Риму. При цьому протиставлялися природа і закон, тобто мали місце передумови виникнення природного права і розмежування його із нормами законів, тобто з суб'єктивно встановленими правилами поведінки в інтересах обмеженого кола осіб.

Вже в стоїків етичні норми ототожнювалися із законами природи – усе має здійснюватися за природною даністю, і не повинно бути повного підпорядкування людини державі. Стоїки вплинули на уявлення римських юристів про природне право. Природне право вони не протиставляли позитивному, а бачили в ньому його складову частину. Визнавалось, що рабство далеке від природного права, огидне природі – за природним правом усі народжуються однаково вільними і рівними, тобто вони вирітул підійшли до ідеї прав людини.

Право є джерелом і мірилом людських законів. Але закони, установлювані людьми, спираються на принципи державного ладу, піддані впливу традицій і звичаїв, а також – інтересам та бажання як окремих суб'єктів влади, так і політичних груп і не завжди справедливі. Справедливість як норма суспільних відносин – це визначений баланс зрівнюваної і розподільної її складових. Зрівнювана складова абстрагується від розходження людей (герой і боягуз рівні для неї), розподільна – визнає розходження людей як суб'єктів суспільних відносин. При пріоритеті зрівнюваної складової суспільство скочується до охлократії, при пріоритеті розподільної – до олігархії. Те й інше призводить до тиранії, що ігнорує всяку справедливість.

Історично римська правова спадщина послужила основою розробки позитивного (конституційного) права буржуазних держав.

У 1190 р. Іоанн Безземельний дав Англії Хартію вільностей, але не надав гарантії її виконання. Англійські барони, що повстали 15 червня 1215 р. під час невдалої війни з Францією, змусили короля прийняти їх вимоги. 49 статей, що декларують права баронів і городян, лягли в основу Великої Хартії Вільностей [81, с. 13-19]. Після цього, безумовно, ще недосконалого документа Англія пішла шляхом утворення правової держави та обмеження деспотичної влади монарха. Буквально 50 років опісля наступний англійський монарх Генріх III, після чергової доповіді міністрів про безлади на вулицях, промовив: *"Ну-ка, давайте сюда главных крикунов. Пусть деруться у меня на глазах, а не стравливают толпы"* [80, с. 76].

У 1265 р. граф Симон де Монфор, правитель Англії, після громадянської війни з королівськими військами скликав збори, що одержали назву парламент (від фр. – "говорити"). У XIV ст. він став двопалатним. У цей час в Англії почали створюватися політичні теорії про обмеження влади монархії законом.

Прологом буржуазних революцій у Європі є епоха Відродження, що закликала до віротерпимості, до правового врегулювання релігійно-політичних конфліктів і миру. Реформація відкрила факт внутрішньої свободи людини, свободи совісті як об'єктивної реальності людської природи, що вимагало вільних дій згідно із совістю. Водночас спроби суб'єктивного насадження релігійної чи соціальної справедливості в державі та суспільстві нерідко закінчувалися крахом моралізму і сплеском розпусти.

22 травня 1498 р. на шибениці загинув чернець Д. Савонарола [68, с. 23] – людина, яка намагалася на практиці довести, що держава лише тоді має право на історичне довголіття, коли її закони засновані на високій моралі кожного громадянина. Ті часи просвітництва і звільнення від пуританства кинули людей в іншу крайність – до епікурейства в житті і скептицизму в думках. У проповідях Савонароли про необхідність радика-

льної реформації життя: виправлення моралі суспільства і відновлення *"найкращої форми правління – республіканської"* постійно підкреслювалося, що республіка лише тоді є благо для держави, коли всі громадяни праведні і чесні люди. Будучи глибоко в цьому упевненим і завдяки надзвичайному правознавчому й ораторському дару, Савонарола переконував слухачів у тому, що глибока релігійність і висока мораль приводить суспільство до справедливого політичного укладу. Сам він відмовився від великої спадщини і будь-якої особистої власності, навіть від бібліотеки, яку з любов'ю збирав довгі роки. Відмовлявся від пропонованих вищих посад і кардинальської влади. Свої думки виклав у роботі "Про правління і законодавство республіки". За короткий час у Флоренції було обрано органи колегіальної влади та проведено реформи. Щоб перекласти тягар податків з бідних на багатих, Савонарола вигнав з міста всіх лихварів і замість них створив кредитний банк із низькими відсотками. Важливе місце в реформі приділялося дуже суворим заходам морального відродження. Так, за участь у звичайних нічних розвагах молодь виплачувала штрафи, що розоряли їх батьків, святотатцям вирвали язики, розпусників спалювали на багаттях, широко використовувалися доноси. Окремі роботи Леонардо да Вінчі, Мікеланджело не лише не зустрічали схвалення ченця, але в запалі загального морального ажіотажу піддавалися руйнуванню. Зрештою, усе закінчилося анафемою – відлученням ченця від церкви. Рим оголосив його єретиком. А зрадлива, як за всіх часів, юрба, що вчора ще плакала і каялася в гріхах, втрачала свідомість від викривань під час його проповідей, цілувала землю, де ступала нога великого моралісга, віддала його на розтерзання кату. Суд виніс вирок – шибениця, потім спалювання тіла. Через 60 років Ватикан виправдає його.

У середині XVII ст. голландський соціолог і правознавець Г. Гроцій (1583-1645 рр.) запропонував доктрину природно-правових поглядів, у якій держава розглядалася як *"совершенный союз вольных людей, который заключается ради соблюдения прав и общей пользы"*.

Думку щодо невідчужуваності природних прав як межі діяльності державної влади продовжив філософ Б. Спіноза (1632-1677 рр.): *"Человек – часть природы. ...Целью государства в действительности является свобода. Естественное право каждого в гражданском обществе не прекращается, поскольку в государстве человек действует по законам природы"*.

У 1679 р. в Англії був прийнятий перший у світі законодавчий акт під назвою "Про свободу особистості" [68, с. 24]. Це знаменитий Habeas Corpus, в основу якого закладено принцип недоторканності особи, зокрема – арештованому зобов'язані пред'явити письмовий наказ від судді, інакше його повинні протягом доби представити до суду, або звільнити. У 1689 р. англійський парламент визнав своїм актом свободу совісті, чим поклав початок конституційному захисту всього простору соціальної свободи.

У 1689 р., при королі Вільгельмі Оранському, англійський парламент прийняв "Біль і декларацію права", де розвивалися ідеї Великої Хартії. Доповнення складалося з 13 пунктів, що містять, приміром, таке – *"Объявляется незаконным приостановление законов или их исполнение без согласия парламента; свобода слова, прений и актов в парламенте не должна быть стесняема и подвергаема контролю в каком-либо суде или комитете, кроме парламента"*.

На початок XVIII ст. Англія була правовою державою з визначеними правами людини і елементами свобод громадянина, із правосвідомістю, що розглядала цивільні права як обов'язковий елемент злагоди у суспільстві. Головна мета держави – забезпечити захист прав, недоторканності особистої свободи та власності, а головний засіб досягнення цього – встановлення справедливих законів.

Ідея про людську, а не Богом дану природу держави породжувала уявлення про те, що держава – це і є той ідеальний інструмент перетворення суспільства, виховання доброчесного підданого, ідеальний інститут, за допомогою якого можна досягти "загального блага" – бажаної, але постійно зникаючої, як лінія обрію, мети людства. Удосконалення відносин у суспільстві можливе, на думку тодішніх філософів, лише за допомогою організації і законів – важелів держави. Удосконалюючи право, домагаючись мети реалізації законів, можна досягти загального процвітання. Людству, що ще недавно вийшло із середньовіччя, здавалося, що знайдено ключ від щастя, варто тільки сформулювати справедливі закони і провести їх у життя. Не випадкова поява і поширення в цей час дуалізму – навчання, що відводить Богу роль першого поштовху, зачинателя світу, який, однак, далі розвивається за властивими йому природними ознаками; потрібно тільки знайти їх, записати і домогтися точного і загального виконання. Звідси й оптимізм людей, віра в необмежені сили людини, що зводить "по кресленнях", на розумних началах свій будинок, місто, суспільство, державу.

На той час було вже ясно, що поділ влади на законодавчу і виконавчу може забезпечити захист людини від свавілля держави. При укладанні договору державі повинна надаватися лише частина природних прав. Питання в тому, яка частина надається.

У 1651 р. Т. Гоббс (1588-1679 рр.) [75, с. 234-242] у трактаті "Левіафан" запропонував теорію, згідно з якою люди передають державі всі свої права, і робить висновок про необхідність сильної абсолютистської держави, але відразу визнає право народу на повстання. Він стверджував, що *"государство строят как дом"*, а життя без ефективної держави, що охороняє порядок, буде *"уединенной, бедной, опасной, грубой и короткой"*. Звідси виникла думка про те, що держава руйнується зсередини, що позбавляє громадян умов стабільного існування – законності і безпеки.

Д. Локк (1632-1704 рр.) [75, с. 257-264] наприкінці XVII ст., спираючись на англійський досвід, уперше створює теорію держави і права, засновану на завжди існуючих природних законах, однаково обов'язкових як для підданих, так і для правителів. Він одним з перших висунув положення про те, що "кожна людина за законом природи має право захищати свою власність, тобто життя, свободу і майно. Забезпечення цих невід'ємних прав становить головну мету договірного об'єднання людей в державу і передачі себе під її владу". Від Д. Локка починається історія правової держави з поділом влади. У його двох трактатах "Про правління" закладені ідеї декларацій прав і свобод. Він виходив з того, що в продуктах своєї праці людина здобуває об'єктивне існування. Люди вступають у державний союз не для того, щоб держава диктувала їм образ думок, розпоряджалося їх життям і створеним їх працею надбанням. Союз цей створюється на базі права і зв'язаний правом. Право – не річ, яку можна комусь віддати, а відносини між людьми, основані на визнанні і захисті людської гідності.

У подальшому Ш. Монтеск'є (1683-1755 рр.) [75, с. 290-298] намагався розкрити причини виникнення того чи іншого державного ладу, аналізував різні форми держави, стверджував, що законодавство країни залежить від форми правління, і вважав, що державі має передаватися лише незначна частина природних прав людини. Слідом за Д. Локком він визнавав необхідність поділу влади в державі.

І. Кант (1724-1804 рр.) [75, с. 343-353] продовжив розробку теорії цивільного суспільства, приділяючи увагу постулатам "практичного розуму" як необхідній передумові розвитку моральності. Центральний принцип етики він засновував на понятті боргу.

Більшість філософів кінця XVIII ст. виходили з примата природного права перед правом позитивним. Багато хто з них прямо підкреслював, що в розумному суспільстві

державні закони зобов'язані відповідати принципам природного права. Тобто, природні права людини повинні бути максимально відображені в нормах законів.

Під прапором уявлень про існування природних, невідчужуваних прав людини відбулися дві революції XVIII століття – американська і французька [68, с. 26-29].

Англійські колоністи принесли в Північну Америку принципи Великої Хартії Вільностей і правосвідомість, засновану на повазі до Закону і Суду. У червні 1776 р. Конгрес народних представників штату Вірджинія прийняв "Білль про права", що проголосив свободу слова, совісті, зібрань, недоторканність особи. Через місяць Континентальний конгрес (13 штатів) прийняв "Декларацію незалежності" Т. Джефферсона (1743-1820 рр.). Ці документи стали в історії першими актами, у яких мова йшла вже про права і свободи кожній людині. Їх фундаментальні принципи майже без змін дійшли до нашого часу: *"Мы считаем самоочевидными следующие истины: что все люди созданы равными, что они наделены Создателем определенными неотъемлемыми правами, среди которых имеются право на жизнь, свободу и на стремление к счастью; что для обеспечения этих прав существуют правительства, осуществляющие свою власть с согласия тех, кем они управляют; что, если форма правления становится гибельной для целей самого своего существования, народ имеет право изменить или отменить ее, учредить новое правительство, основанное на этих принципах, и установить власть в такой форме, какая, по его мнению, лучше обеспечит его безопасность и благоденствие"* [68, с. 26].

У 1787 р. прийнята Конституція США, власне, перша у світовій історії Конституція, викладена в письмовій формі [79]. Філософську базу системи американської демократії склали ідеї Джона Локка. Т. Джефферсон писав: *"Конституционные принципы США родились из соединения принципов английской конституции, идей естественного права и здравого смысла"*. Дотепер ці принципи та ідеї відповідають сучасному розумінню прав і свобод – усі люди рівні, незалежні і мають права, які держава не в змозі в них відібрати.

У 1791 р. Конституція США була доповнена 10-ма поправками за назвою "Білль про права людини" [81, с. 21]:

"1. Конгресс не должен издавать законов установления какой-либо религии или запрещающих ее свободное исповедание, ограничивающих свободу слова или право народа мирно собираться и обращаться к правительству с петициями об исправлении злоупотреблений.

2. Для безопасности свободного государства необходима хорошо организованная милиция, поэтому право народа хранить и носить оружие не подлежит ограничениям.

3. В мирное время ни один солдат не должен помещаться на постой в какой-либо дом без согласия его владельца, во время же войны это допускается только в порядке, установленном законом.

4. Право народа на охрану личности, жилища, бумаг и имущества от необоснованных обысков или арестов не должно нарушаться и ордера на обыск или арест не будут выдаваться без достаточных оснований, подтвержденных присягой или торжественным обещанием. Такие ордера должны содержать подробное описание места обыска, а также подлежащих аресту лиц или имущества.

5. Никто не должен привлекаться к ответственности за тяжкое или иное позорящее преступление иначе как по постановлению или обвинению, вынесенному присяжными; никто не должен дважды отвечать жизнью или телесной неприкосновенностью за одно и то же преступление; никто не должен принуждаться свидетельствовать против самого себя в уголовном деле; никто не должен лишаться жизни, свободы или

имущества вне установленного законом порядка; никакая частная собственность не должна отбираться для общественного пользования без справедливого вознаграждения.

6. Во всех случаях уголовного преследования обвиняемый имеет право на скорый и публичный суд беспристрастных присяжных. Обвиняемый может пользоваться помощью адвоката для защиты.

7. Факт, рассмотренный судом присяжных, не должен подвергаться пересмотру каким-либо судом иначе как на основе положения общего права.

8. Не должны налагаться жестокие и необычные наказания.

9. Перечисление в Конституции определенных прав не должно рассматриваться как отрицание или умаление других прав, сохраняемых за народом.

10. Полномочия, не предоставленные настоящей Конституцией и пользование которыми не возбранено отдельным штатам, остаются за штатами или за народом.

"Декларація незалежності" і "Білль про права людини" з'єднали реалізм принципів Великої Хартії Вільності й англійських правових актів того часу, що містять положення про права людини і свободи громадянина. Інтелектуальну основу підготували філософи-просвітителі XVII-XVIII ст., які вважали, що невід'ємні права є Богом даними, природними правами. Це ті права, що не знищуються при зміні громадянського суспільства. Ні суспільство, ні уряд не можуть відчужувати їх. Перша поправка до Конституції США, як уже було сказано, забороняла конгресу видавати закони, що обмежують свободу слова, віросповідання і мирні зібрання.

Ідеї Д. Локка і Ш. Монтеск'є – про поділ влади і гарантії свободи та Ж.-Ж. Руссо (1712-1778 рр.) – про народне верховенство сприяли проголошенню у Конституції того, що демократія грунтується на принципі, за яким уряд існує, щоб служити народу; народ існує не для того, щоб служити уряду. Народ – це громадяни демократичної держави, а не його піддані. "Батьки-засновники" американської конституції також виходили з бачення Т. Гоббса про те, що "*естественное право* ("jus naturale") *есть свобода человека использовать свои силы по собственному усмотрению для сохранения своего природного естества*". Природний закон (lex naturale) є *"обнаруженное разумом общее правило, запрещающее человеку делать то, что пагубно для его жизни, и упускать то, что он считает лучшим средством для ее сохранения"*. Зазначені ідеї виявилася настільки практичними, що, як писав Г. Редер, – *"Вся буржуазная революция в Северной Америке исходила из убеждения, что политические институты будут прогрессировать в направлении все большего их соответствия природе человека"* [68, с.28].

Безсумнівно справедливо, що застосування людьми своїх природних прав накладає обмеження на будь-який уряд, заснований на демократичних принципах. У цьому розумінні права особи є оплотом проти зловживання державною владою тими, хто в даний момент є політичною більшістю. Т. Джефферсон, побоюючись можливих наслідків довгого перебування при владі недостатньо моральних людей, прагнув попередити всякого роду випадковості таким порядком керування, за якого політично активні громадяни будуть самі керувати країною.

14 липня 1789 р. штурмом Бастилії почалася Велика французька революція. Натхненна ідеями європейських просвітителів і американських правових актів, Франція 26 серпня 1789 р. прийняла "Декларацію прав людини і громадянина" [81, с. 20], де *"вечные, неотчуждаемые, неотделимые и священные права человека"* мала відтримуватися конституцією.

У Декларації, запропонованій М. Робесп'єром (1758-1794 рр.) "Якобінському клубу", визначалося: *"Целью всякого политического объединения является сохранение естественных и неотъемлемых прав человека и развитие всех его способностей. Глав-*

ными правами человека являются: право обеспечения сохранения своего существования и свобода. Свобода есть возможность, которой обладает каждый человек, осуществлять по своему усмотрению все свои способности". Джерелом влади проголошувався народ, а не воля монарха. Декларація затверджувала рівність усіх громадян перед законом, право приватної власності як основу демократії і прав людини, поділ влади на законодавчу, виконавчу і судову, відповідальність і підзвітність службовців, основні принципи законності, суверенітету і права нації обирати владу.

Кращі уми людства сподівалися, що французька революція приведе до благоденства, а вона проігнорувала природу людини і скомпрометувала себе. Уже наприкінці революції М. Робесп'єр говорив у Конвенті: *"Для того, чтобы создать и упрочить среди нас демократию, чтобы прийти к мирному господству конституционных законов, надо довести до конца войну свободы против тирании".* Але звільнений від правових рамок меч законності почав довільно застосовуватися тими, хто знаходився при владі. Чисті наміри Робесп'єра втрачали опору, а через п'ять років з початку революції призвели до якобінського терору, потім – до диктатури і стали предтечею загарбницьких війн Наполеона. Як пізніше справедливо помітив Ф. Хайєк [85]: *"Различие между обществом свободных людей и тоталитарным обществом в огромной степени заключается в том, что в первом случае правительственные решения затрагивают ресурсы, предназначенные для правительственных целей, а во втором применяются ко всем общественным ресурсам, включая сюда и граждан".* Тривала полеміка багатьох передових мислителів про ідею насильницької революції привела наприкінці XVIII-XIX століть до висновку, що військовий деспотизм є результатом "влади натовпу".

У Росії ідеї державності і свободи з'явилися значно пізніше ніж в Англії, Америці і Франції [68, с. 29-33]. Наприкінці XVII століття країна було відсталою у всіх областях. Міст у ній нараховувалося набагато менше, ніж на Заході. Промисловість була відсутня, адміністративний устрій був архаїчним, процвітало кріпацтво. Росію минали і Просвітництво, і Реформація. Духівництво було неосвіченим, літератури майже ніякої не існувало, інші науки ігнорувалися чи нехтувалися. Необхідність і важливість проведення європеїзації і модернізації країни не були очевидним для більшості людей Росії.

З 1698 р., при Петрі I, спостерігалися бурхливий розвиток культу держави і використання досягнутих за кордоном успіхів у точних, природничих науках, що змушували трактувати і громадське життя як процес, близький до механічного. Вчення Р. Декарта про загальну математику – єдину достовірну і позбавлену містики галузь знання, робило свою справу: образ деякої "машини", що діє подібно до точного механізму годинника, став образом для політиків, лікарів, біологів. Ця ідея, трансформуючись відповідно до умов Росії, стала важливим елементом політичної свідомості. Звичайно, було б перебільшенням стверджувати, що Петро I почав реформувати імперію на основі концепцій Р. Декарта, Ф. Бекона, Т. Гоббса, Б. Спінози, Г. Лейбниця та ін. Мова йде про сильний вплив їх ідей на практичну державну діяльність великого реформатора, з робіт яких він узяв думки про керівну роль держави в житті суспільства взагалі, і в економіці зокрема. Петро I, виходячи з концепції раціоналістичної філософії і з традиційних уявлень про роль самодержця в Росії, надавав величезного значення писаним нормам, вірячи, що правильно написаний закон, вчасно виданий і послідовно виконуваний, може зробити майже все, починаючи з постачання народу хліба і закінчуючи виправленням моралі. Так, зокрема, Регламент Адміралтейської колегії від 09.12.1709 р. зазначав: *"Профос должон смотреть, чтоб в Адмиралтействе никто кроме определенных мест не испражнялся. А ежели кто мимо указанных мест будет испражняться, того бить кошками и велеть вычистить".* Точне виконання законів Петро I

вважав панацеєю від усіх бід. Сумнівів щодо адекватності закону дійсності майже ніколи в нього не було.

Що стосується прав людини і свобод, то необмежена воля монарха служила єдиним джерелом права. Творець могутньої бюрократичної імперії був переконаний, що *"подчиненный перед лицом начальствующим должон иметь вид лихой и придурковатый, дабы размышлением своим не смущать оное".* Він, писав В. Ключевський, *"надеялся грозою власти вызвать самодеятельность в порабощенном обществе и через рабовладельческое дворянство водворить в России европейскую науку, народное просвещение, как необходимое условие общественной самостоятельности, хотел, чтобы раб, оставаясь рабом, действовал сознательно и свободно. Совместное действие деспотизма и свободы, просвещения и рабства это политическая квадратура круга, загадка, разрешавшаяся у нас со времен Петра два века и доселе неразрешенная".*

Перший акт про свободи дворянства – "Велика Хартія вільностей" – прийнятий в Англії" у 1215 р. У Росії перший маніфест "Про дарування вільностей російському дворянству" був підписаний Петром III лише через 500 років – у 1762 р. До цього дворяни не були вільними і розглядалися як бюрократично-військовий стан, тісно прив'язаний до державної колісниці.

В часи "освіченого абсолютизму" верховенство державних інтересів і культу монарха також не могли всерйоз розглядатися в контексті утвердження прав людини. Хоча Катерина II училася у просвітителів Заходу і знала, що в ідеальній державі союз народу і правителя засновується на законі, який виконується обома сторонами, але у "Наказі Комісії про створення проекту нового укладення" у статті 10 було зазначено, що *"...всякое другое* (не самодержавное – від авт.) *правление не только было бы России вредно, но и вконец разорительно".* І одночасно, у статті 34 – *"Равенство всех граждан состоит в том, чтобы все подвержены были тем же законам".* Підсумок – кріпосне право було збережено, а "Наказ..." – поступово забутий. Катерина II – іноземка (чужа для Росії людина) та жінка, яка полюбила свою нову батьківщину та хотіла їй добра, зрозуміла – потрібна наполеглива, багаторічна робота.

А. Радищев, що потрапив в опалу за критику кріпацтва, спочатку в дусі Д. Локка, Ж.-Ж. Руссо, а пізніше й Ш. Монтеск'є писав про громадянську свободу і права особи, закликаючи до кардинальних змін у суспільстві. Революція за Радищевим – *"это восстановление свободы народа, а свобода прирожденное право человека. Гражданская свобода должна ограничиваться общей волей".*

Не критика кріпацтва, не осуд рабства, що й сама Катерина не вважала благом, обурило і спонукало її до розправи. Радищев посмів сказати, що її піддані живуть погано, що ніякого благоденства народу насправді нема: *"Бунтівник, гірше Пугачова".* Він вимовив уголос те, що ніхто не наважувався сказати, хоча знали усі; усі, але не Катерина. Вона була переконана, що це неправда, її піддані не можуть бути нещасливі. Міркуючи на теми свобод і гуманізму, Катерина відзначала, що *"молитвенником монархов со здравым смыслом должно быть сочшение Монтескье "О духе законов".* Але водночас, незважаючи ні на політичні договори, ні на історичні, національні та географічні особливості окремих районів імперії, у 1764 р. розпорядилася ліквідувати інститут гетьманства в Україні, за якого була створена і прийнята перша в Європі Конституція 1710 р. Пилипа Орлика, гетьмана Запорізької Січі.

Що стосується дворянства, то в 1785 р. вона підписала "Жалувану грамоту дворянству", у якій пишними виразами оцінювалися його заслуги, давалося визначення дворянства і називалися всі його привілеї, єдині і для російських дворян, і для остзейських лицарів, і для польсько-українських шляхтичів. Серед іншого, вказувалося, що

дворянин не може позиватися з дворянином і піддаватися тілесному покаранню, що він вільний і може володіти кріпаками, купувати і продавати їх, заводити фабрики і заводи, торги і ярмарки і т. д.

Тільки через 100 років після маніфесту "Про дарування вільностей російському дворянству" Олександр II скасував кріпацтво. У більшій мірі це визначалося об'єктивними умовами розвитку капіталізму в Росії і потребами в робочій силі, але й завдяки зусиллям блискучого канцлера А. Горчакова, що витяг країну з конфлікту з усією Європою, зберігши її достоїнство після кримської бойні, а також переконав царя повернути із Сибіру живих декабристів. Олександр II якось з посмішкою помітив: *"Мой папа был гений, поэтому мог позволить себе окружать трон остолопами. А я не гений – мне потребны разумные люди"*. Той же А. Горчаков його повчав: *"Власть – твердая, а меры мягкие. Нельзя углублять пропасть между общественным мнением и властью"*.

До кінця правління династії Романових захисту прав людини і свобод не існувало. Навіть паростки парламентаризму, що виникли в 1905 р., псувалися. Коли Миколі II запропонували видати розпорядження стосовно розширення практики розробки актів щодо реалізації законів, він відповів: *"Зачем? Пусть чиновники разъясняют законы"*.

У другій половині позаминулого сторіччя в Росії утворився вузький прошарок "революційної інтелігенції" (поняття незнайоме іншому світу), яка, начитавшись К. Маркса, відчула презирство до підвалин і зайнялась ідеалізмом загальної рівності. Крайня самовпевненість піднімала народ на боротьбу з режимом, не розуміючи, чим для неї самої це скінчиться. Потім вустами О. Горького буде сказано: *"Хотели разбудить человека, а разбудили зверя"*. Інакше і бути не могло. Народ, на 80 % не писемний, не володіючи політичною культурою, поважаючи тільки силу поліцейських батогів, усвідомить лютневі свободи як ослаблення влади і кинеться палити, трощити, тягти все підряд та гадити в античні урни Зимового Палацу. Багатовіковий шлях створення парламентської демократії, пророблений Європою, виявилося неможливо пройти за короткий відрізок 1905 – 1917 рр. Вже революція 1905 р. показала, що замість тодішньої незамінності інституту монархії наступить хаос. В умовах, коли країну підточували вкрай наївні ліберали й одержимі ідеалісти та насідали на неї зовнішні вороги, важливою була твердість і вивіреність курсу державного корабля. У кризові історичні моменти є необхідним інший рівень державної енергії та інші рішення. Однак за сторіччя не було вироблено механізму обрання на трон дійсно гідного володаря, здатного послідовно вести країну між потребами державного порядку й проведенням реформ в інтересах формування правової держави.

Протягом сторіч велися суперечки навколо понять природного і позитивного права. За концепцією природного права носієм його є індивід, навіть якщо закони держави не забезпечують йому природні права. У концепції прихильників позитивного права носієм цих прав є суспільство і держава. З їх погляду, природне право, незафіксоване в законі, є правом фіктивним. Воно відволікає увагу від розробки конкретних позитивних прав, що могли б реалізуватися державою. Отут є деяка небезпека підміни практичної роботи проголошенням, наприклад, внутрішньої свободи при відсутності фіксації свобод у законах. Однак, усе більше поширення зараз здобуває думка, згідно з якою необхідно продовжувати йти шляхом конвергенції теорії природного і позитивного права. Причому, Аристотель вказував, що *"законы следует издавать применительно к органически утвердившемуся государственному строю, а не подгонять государственное устройство под некий закон"*. Звідси К. Каутський виводив, що *"каждое время можно мерять только присущей ему мерой, что стремления настоящего должны обосновываться условиями настоящего"* [86].

У XIX столітті філософська проблема природного права стала повільно виходити на перший план юриспруденції і почалися спроби застосування поняття прав людини вже в рамках міжнародного співтовариства [68, с. 33-36].

Після завершення наполеонівських війн у 1815 р. на Віденському конгресі був укладений міжнародний договір, що гарантував рівність різних віросповідань. Аналогічний договір був підписаний у Парижі в 1856 р. за підсумками Кримської війни.

На початку позаминулого століття був укладений цілий ряд конвенцій про заборону рабства і работоргівлі. Тоді ж виникають процеси "гуманітарного втручання". У 1827 р. Великобританія, Росія і Франція спільно втрутилися у внутрішні справи Османської імперії з метою відновлення порушених прав грецького населення. Це привело, в підсумку, до відновлення незалежності Греції. У 1860 р. група європейських держав втрутилася у внутрішні справи Сирії, щоб запобігти геноциду християнського населення. Балканська війна 1878 р. велася також з метою захисту прав не мусульманського населення на Балканах. А наприкінці XIX – початку XX століть Сполучені Штати зробили ряд представлень уряду Російської імперії у зв'язку з переслідуванням євреїв.

З кінця XIX ст. багато уваги стало приділятися міжнародній кодифікації в області соціального і трудового законодавства. Цьому питанню була присвячена конференція європейських держав у Берліні в 1890 р.

У 1906 р. у Берні були прийняті перші міжнародні акти про захист праці. А Гаазькими конвенціями 1889 і 1907 рр. передбачався захист людини у випадку військових конфліктів.

11 листопада 1918 р. закінчилася Перша світова війна, що забрала понад 10 млн. людських життів. У Росії відбулася революція. Світ розколовся на два табори. Європа розділилася на 38 держав.

Відповідно до норм, що регулюють відносини між державами, уряди, у принципі, не мають права втручатися в справи іншої держави. Але після Першої світової війни зросла впевненість у тому, що силами одних урядів права людини не можуть бути належним чином захищені і що для цього необхідні міжнародні гарантії. Для можливості врегулювання майбутніх військових конфліктів у 1919 р. була створена перша міжнародна організація – Ліга Націй.

Ліга Націй, незважаючи на те, що в її повноваження не включалися питання, прямо пов'язані з правами людини, робила спроби забезпечити такі права шляхом залучення міжнародних засобів. Правда, це мало відношення лише до певних умов для захисту меншостей в деяких країнах. Взагалі діяльність Ліги Націй була не в змозі скоординувати демократичні зусилля, тому перед початком Другої світовій війною вона закінчила своє існування.

1.1.2. Права людини у міжнародних документах

Вперше термін "права людини" з'явився в міжнародній політичній лексиці після американської війни за незалежність і Великої французької революції. У той час у відповідних внутрішньодержавних документах говорилося про "права людини і громадянина".

З позицій сучасних міжнародних документів права людини – це соціальні домагання і можливості людини, об'єктивно обумовлені системою суспільних відносин, передовими ідеалами і т. д., що є важливими для правового становище людини в будь-якому сучасному суспільстві [68, с. 36-37].

Протягом XX ст. міжнародне співтовариство сильно змінилося, і насамперед у результаті Другої світової війни. У цю війну було втягнуто 61 державу з населенням 1700

мільйонів чоловік, що становило близько 80 відсотків усього людства. Закінчилася вона загибеллю понад 50 мільйонів осіб і матеріальними втратами, розмір яких у грошовому еквіваленті складає 316 млрд. доларів [83, с. 29-31]. Страшне світове потрясіння спонукало створити форум пошуку шляхів запобігання таких жахливих подій у майбутньому.

Організація Об'єднаних Націй (далі – ООН) була утворена у 1945 р., яка у Статуті, від імені всіх народів, що вступили в неї, затвердила прихильність ідеї захисту прав людини [87, с. 35-36]. Одна з основних цілей ООН – розробка міжнародних принципів для забезпечення прав людини у країнах світу, тому що історія прав людини – у всіх світових подіях. Без дотримання прав людини є неможливим економічний і соціальний прогрес та міжнародне співробітництво.

Статут ООН застосовує поняття "права людини і свободи" [80, с. 9]. Заради стислості і те й інше позначають терміном "права людини", оскільки мова йде про явища одного порядку. І право, і свобода – гарантована законом міра можливого поводження особи чи групи осіб. Порядок реалізації права тією чи іншою мірою регламентується. Свободу іноді розглядають як область людського поводження, у яку держава зобов'язується не втручатися.

У першій статті Статуту ООН прямо зазначається про "заохочення і розвиток поваги до прав людини і основоположних свобод для всіх". Проте, принципи, закладені в Статуті ООН, мають узагальнений зміст, тому виникла потреба установити більш конкретні критерії визначення прав людини і свобод та створення відповідної системи захисту.

10 грудня 1948 р. Резолюцією Генеральної Асамблеї ООН № 217 А(III) була прийнята Загальна декларація прав людини [81, с. 22-25]. Її поява дійсно стала поворотним пунктом у житті людства й, імовірно, перевершує за своєю значимістю усі відомі найбільші історичні події.

Загальна декларація вперше проголосила про наявність інформаційних прав людини, які були сформульовані у статтях 2, 11, 12, 19, 27 та 30.

Так згідно зі статтею 12: *"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. Кожна людина має право на захист від такого втручання або таких посягань"*. На основі цієї статті та у зв'язку з необхідністю детального упорядкування відносин з'явилося національне законодавство про захист даних, яке потребувало створення міжнародних стандартів на рівні європейських інституцій.

Згідно зі статтею 19 Загальної декларації: *"Кожна людина має право на свободу переконань і на вільне їх вираження; 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"*. Ця стаття є базою для пошуків балансу прав людини, суспільства і держави та створення законодавства про доступ до інформації.

У загальному плані зазначені в Загальній декларації прав людини інформаційні права можна вважати юридичним базисом та основою нової галузі права, яка сьогодні в Україні формується та отримала назву "Інформаційне право" [39, с. 86-87].

Найбільше у Другій світовій війні постраждали європейські народи, вся економіка Європи була практично зруйнована. Світова трагедія привела до розуміння необхідності будувати об'єднану Європу, у якій би поважались інтереси усіх. У 1949 р. була створена Рада Європи як оплот проти гноблення і погрози диктатури [81, с. 26-33].

Однією з головних цілей Ради Європи є захист і забезпечення прав людини та демократії в інтересах розвитку справедливості, рівності і достоїнства чоловіків, жінок і дітей.

Для того щоб бути членом Ради Європи, держава повинна поважати Демократію, Права Людини і Верховенство Права. Ці цінності є принципами справедливого суспільства.

Для захисту принципів справедливості 4 листопада 1950 р. Рада Європи прийняла Конвенцію Ради Європи "Про захист прав людини і основоположних свобод" [81, с. 34-61]. Ця Конвенція не тільки конкретизує ряд прав і свобод для всіх людей, що живуть у державах-членах Ради Європи, а й вперше гарантує їх захист Європейським судом з прав людини. Конвенція також юридично зобов'язує усі держави, що її ратифікують, приймати закони, які відповідають європейським стандартам.

У міждержавних стосунках захист прав людини здійснюється на основі таких принципів і норм міжнародного права, як неподільність і повага прав людини, загальноприйнятих відносин держав із власним населенням, співробітництво держав на базі міжнародних стандартів [68, с. 38-43].

Принцип неподільності прав людини передбачає, що усі права людини неподільні, однаково важливі, становлять єдиний комплекс. Неприпустиме протиставлення якого-небудь одного права чи свободи іншим. Інакше прагнення домогтися дотримання прав і свобод однієї групи може бути використане для обмеження прав іншої.

Визнання принципу неподільності прав людини не виключає їх градації, пріоритетів. На перше місце завжди ставлять право на життя, без забезпечення якого стає безглуздим дотримання інших прав. Однак дотримання лише одного права на життя недостатньо для повноцінного існування і розвитку особистості в суспільстві. Для цього необхідна повага і дотримання й інших прав і свобод, таких як, зокрема, право на особисту недоторканність, на справедливий публічний розгляд, на повагу особистого і сімейного життя, недоторканність житла і таємниці кореспонденції, право на свободу вираження своєї думки, одержання і поширення інформації й ідей без втручання з боку державних органів і незалежно від державних кордонів.

Принцип поваги прав людини як один з основних принципів сучасного міжнародного права не протистоїть іншим його принципам, а гармонійно з ним поєднується. Тому ніякі посилання на необхідність захисту прав людини не можуть виправдати спроб порушити такі принципи, як повага державного суверенітету, невтручання держав у внутрішні справи один одного, заборона погрози чи силоміць її застосування в міжнародних відносинах і т. д. Права людини і свободи не повинні застосовуватися як привід для зазіхань на мир і безпеку, незалежність і рівноправність держав, тобто на ті основи, на яких базується сама ідея міжнародного співробітництва.

Становлення принципу загальної поваги прав людини і свобод для усіх у якості одного з основних міжнародно-правових принципів відбувається у післявоєнний час і пов'язано безпосередньо з прийняттям Статуту ООН.

Преамбула Статуту ООН підтверджує "віру в основні права людини..., у рівноправність чоловіків і жінок". У статті 1 як мета членів ООН зазначене співробітництво між ними "у заохоченні і розвитку поваги до прав людини і свобод для усіх, незалежно від раси, статі, мови і релігії". Важливіше значення має стаття 55 Статуту, згідно з якою "Організація Об'єднаних Націй сприяє: а) підвищенню рівня життя, повної зайнятості населення й умовам економічного і соціального прогресу і розвитку; ...с) загальній повазі і дотриманню прав людини і свобод для всіх". Стаття 56 передбачає, що "всі учасники Організації зобов'язуються починати спільні і самостійні дії в співробітництві з Організацією для досягнення цілей, зазначених у статті 55".

Неважко помітити, що зобов'язання держав викладені тут у загальній формі, тому з моменту прийняття Статуту і дотепер держави прагнуть конкретизувати нормативний зміст принципу загальної поваги прав людини. З найбільшою повнотою й універсальні-

стю це зроблено в Загальній декларації прав людини 1948 р. і двох пактах, прийнятих у 1966 р. – "Міжнародному пакті про цивільні і політичні права" і "Міжнародному пакті про економічні, соціальні і культурні права", що виходять з визнання права народів на самовизначення. При цьому метою міжнародного співробітництва є не уніфікація національних законодавств, а розробка стандартів (моделей), що служать для держав своєрідною відправною точкою для вироблення власного національного законодавства. Безпосередня регламентація і захист прав людини і свобод, як і раніше, залишаються внутрішньою справою кожної держави.

Міжнародні норми в області прав людини в переважній більшості не можуть застосовуватися безпосередньо на території держави і вимагають від неї визначених кроків з імплементації, тобто привнесення міжнародних норм у національне законодавство. Наприклад, положення пактів про права людини прямо вказують на необхідність держав вживати заходи, зокрема законодавчі, із забезпечення людині прав, які нині передбачені. Як правило, міжнародні документи не визначають, яким чином держава буде виконувати взяті на себе зобов'язання. Але стандарти поводження, що містяться в міжнародних документах, певною мірою зв'язують свободу поводження держав у сфері національного законодавства.

Загальноприйняті відносини держав із власним населенням. Права людини і свободи як невід'ємні фактори демократії не безмежні [68, с. 41-43]. Одночасно з визначенням їх законодавчих обмежень модель правової держави припускає обмеження прерогатив державної влади при її втручанні в приватне чи громадське життя. Це зовсім не применшує ролі державних установ у житті суспільства. Навпаки, їх регулююча роль стає усе більш конструктивною.

У червні 1815 р. Наполеон, виступаючи перед депутатами, говорив: *"Люди не в змозі забезпечити своє майбутнє; тільки державні інститути вершать долі націй"*. У 1985 р. на колоквіумі, присвяченому проблемам модернізації держави, Президент Французької Республіки Ф. Міттеран заявив: *"Немає демократії без держави. Держава надає ресурси для виконання демократичних рішень у формі законів чи підзаконних актів; це забезпечує підтримку правопорядку – основне зусилля, необхідне для здійснення демократії, це захищає і забезпечує життєвість публічних свобод"*.

Із суверенітету держави випливає, що усі відносини з власним населенням – питання внутрішні, регульовані на національному рівні. На цьому заснована сформована в практиці ООН думка про те, що під порушенням принципу поваги прав людини варто розуміти загальну політичну і правову ситуацію в державі, що свідчить про те, що держава ігнорує своє зобов'язання поважати права людини, роблячи масові й грубі порушення основоположних прав, що є, наприклад, результатом апартеїду, колоніалізму, іноземної окупації і т. п.

Багато років вважалося, що окремі порушення прав фізичних осіб (індивідуальні випадки) відносяться до внутрішньої компетенції держави і тому не можуть бути предметом розгляду в ООН чи в інших міжнародних організаціях. Самі по собі вони можуть і не бути ознакою того, що в державі склалася обстановка, яка дозволяє говорити про порушення нею своїх зобов'язань за Статутом ООН. Але погляди на такий підхід змінилися. Та обставина, що держава самостійно регулює взаємовідносини з власним населенням не означає її "право" на свавілля. У процесі державного регулювання мають враховуватися міжнародні принципи, насамперед принцип обговорення окремих питань на міжнародному рівні. Ніщо не перешкоджає державам добровільно передавати на обговорення міжнародних органів питання, що стосуються порушень прав окремих осіб. Це робиться на основі міжнародних договорів. Відповідні положення є в першому

"Факультативному протоколі до Міжнародного пакту про цивільні і політичні права" 1966 р. і Конвенції Ради Європи "Про захист прав людини і основоположних свобод" 1950 р. Ці договори передбачають можливість розгляду в міжнародних органах приватних скарг щодо інформаційних прав (згідно зі статями 8 та 10).

У наш час визнається, що деякі індивідуальні випадки можуть бути предметом розгляду на міжнародному рівні і без договору, причому навіть без згоди зацікавленої держави. Однак точні критерії допустимості розгляду таких випадків не вироблені.

Міждержавне співробітництво з питань прав людини має бути деідеологізоване і деполітизовано. Це означає, що на рівні офіційних міждержавних контактів з гуманітарних питань необхідно виключати полеміку ідеологічного змісту, використання обговорюваних питань у пропагандистських цілях. Під час обговорення питань держави повинні прагнути до об'єктивності, а не керуватися виняткова політичними інтересами, зменшуючи масштаби порушень чи прав, навіть зовсім їх замовчуючи і, навпаки, перебільшуючи їх у тих випадках, коли мова йде про державу, відносини з якою з певних причин погіршилися. Співробітництво держав з гуманітарних питань не може не бути політичним саме тому, що це частина міждержавного співробітництва, яке не повинно бути ідеологізованим.

Міжнародні стандарти в сфері захисту прав людини. Статут ООН, не конкретизуючи поняття прав людини, містить кілька принципів, певною мірою цьому сприятливих. Так, у Статуті ООН говориться про рівноправність націй, чоловіків і жінок, про достоїнство і цінність особистості (тобто право на життя), про неприпустимість дискримінації за ознаками раси, статі, мови, релігії (тобто свобода совісті, переконань і т. п.). Можна вважати, що преамбула Статуту містить посилання на основні демократичні свободи в тій її частині, де говориться про прагнення учасників організації "сприяти соціальному прогресу ...при більшій свободі".

З урахуванням насамперед цих положень розроблялися і розробляються відповідні міжнародні стандарти. Основна робота велася і ведеться в рамках ООН та її спеціалізованих установ, насамперед ЮНЕСКО. Частина згаданих документів – резолюції міжнародних організацій – має рекомендаційний зміст. До них відносяться "Декларація про ліквідацію усіх форм нетерпимості і дискримінації на основі релігії чи переконань" 1981 р., "Декларація про права осіб, що належать до національних чи етнічних, релігійних і мовних меншин" 1992 р.

Резолюції мають важливе значення у формуванні нових стандартів в області прав людини й уточненні існуючих. Морально-політичний авторитет багатьох з них дуже високий, і держави з ними рахуються, хоча вони не накладають на них юридичних зобов'язань.

Інша частина документів в області прав людини – міжнародні договори, мають зобов'язуючий зміст для їх учасників. До них відносяться міжнародна Конвенція РС "Про ліквідацію усіх форм расової дискримінації" 1965 р., "Міжнародний пакт про економічні, соціальні і культурні права" 1966 р., Конвенція Ради Європи "Щодо катувань і інших жорстоких, нелюдських чи принижуючих достоїнство видів поводження і покарання" 1984 р. та інші договори. Ці договори закріплюють стандарти в області прав людини.

Пакти про права людини – одне зі значних досягнень ООН у сфері співробітництва з забезпечення прав людини. Ці договори покликані створити універсальну міжнародно-правову базу для міждержавного співробітництва з питань, що стосується прав людини. В даний час особливо актуальними постало питання про надання їм більшої ефективності, що припускає їх універсалізацію, тобто максимальне збільшення кола

учасників. Проте у них беруть участь навіть не всі постійні учасники Ради Безпеки ООН. Так, Китай не підписав обидва пакти про права людини 1966 р. США не беруть участі в Пакті про економічні, соціальні і культурні права. Останнє пояснюється тим, що американські конституційні норми, що випливають з політичної традиції захисту свободи, передбачають підвищений захист приватного підприємництва і приватної власності, а також недопущення обмежень свободи слова навіть з метою порушення суспільного порядку. Американські законодавці вважають, що міжнародним правом ці цінності захищаються недостатньо.

Своєрідний зміст мають документи ОБСЄ, прийняті в рамках загальноєвропейського процесу. Документи ОБСЄ мають політичну спрямованість, а їх положення часто іменують домовленостями. Оскільки керівники держав-членів ОБСЄ неодноразово заявляли про те, що домовленості підлягають безумовному впровадженню в життя, вони мають і юридичний відтінок. Положення документів ОБСС, що відносяться до прав людини, розглядаються як регіональні стандарти в області прав людини.

Загальний аналіз щодо ставлення з повагою до прав людини свідчить про те, що індивід поступово стає безпосереднім суб'єктом міжнародного права. Насамперед мова йде про грубі і масові порушення прав людини. Такі явища, як геноцид, апартеїд, расова дискримінація і т. п. уже кваліфіковані міжнародним співтовариством як міжнародні злочини й тому не можуть розглядатися як справи, що входять до внутрішньої компетенції держави.

1.1.3. Інформаційні права у класифікації прав людини

Інформаційні права людини закріплені у статтях 8, 10, 13, 17 Конвенції Ради Європи "Про захист прав людини і основоположних свобод" 1950 р. [55].

Стаття 8 визначає наступне: *"Кожна людина має право на поважання її особистого і сімейного життя, житла і таємниці листування. Держава не може втручатися в здійснення цього права інакше, як згідно з законом..."*.

Згідно зі статтею 10: *"Кожна людина має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і поширювати інформацію та ідеї без втручання держави і незалежно від кордонів. Ця стаття не перешкоджає державам вимагати ліцензування діяльності радіо-, теле- або кінопідприємств"*.

Підсумовуючи, можна зазначити, що різні суспільства мають різні соціальні можливості для забезпечення прав людини і свобод. Але в принципі для держав притаманні певні погляди на те, які права повинні бути надані індивідам і закріплені в національних законах. Реальне забезпечення цих прав і свобод може бути різним. Воно грунтується на рівні розвитку відповідного суспільства, на нього впливають національні, релігійні, етнічні й інші особливості. Разом з цим, є деяке загальне розуміння змісту і ролі прав та обов'язків людини у суспільстві, з чого й випливає їх класифікація.

Відповідно до прийнятої в міжнародних документах класифікації права людини поділяються на громадянські, політичні, економічні, соціальні і культурні. Можливі й інші варіанти класифікації. З початку 1970-х р. у міжнародній практиці одержала поширення концепція "трьох поколінь" прав людини [80, с. 9-15], до якої у наступному було приєднано ще одне "покоління" – інформаційне.

Перше покоління прав. Було породжено, головним чином, Великою французькою революцією, коли вперше держава задекларувала гарантії щодо громадянських та політичних прав людини – право на життя, свободу й безпеку, вільний вибір місця проживання і пересування, право на притулок від переслідування, свобода думки та її висловлення, мирних зборів, неприпустимість катування й інших жорстоких, негуманних форм поводження, свобода від втручання в особисту кореспонденцію і таємність, право на участь в управлінні державними справами, право не бути позбавленим власності, право мати власність тощо.

До другого покоління прав та свобод належить група соціально-економічних і культурних прав – право на працю та захист проти безробіття, соціальне та медичне забезпечення, доступ до публічної служби, відпочинок, освіту, достатній рівень життя, захист результатів літературної, художньої та наукової творчості тощо. Реалізація зазначених прав потребує сприяння з боку держави. Ці права і свободи легалізовано наприкінці XIX – на початку XX ст. в результаті класової боротьби за поліпшення добробуту та створення безпечних умов праці.

Третє покоління прав (права "солідарності") – права на солідарність, політичне, економічне, національне і культурне самовизначення, соціальний та економічний розвиток, на гуманітарну допомогу, на мир, безпечне навколишнє середовище, права соціальних та професійних груп тощо. Визнання цієї групи прав і свобод обумовлено процесами боротьби за національну незалежність народами колонізованих країн (Африки, Латинської Америки) після Другої світової війни. У прийнятій у 1981 р. Організацією африканської єдності "Африканській хартії прав людини і народів" закріплено ряд прав народів (право на самовизначення, право на вільне розпорядження своїми природними багатствами і ресурсами, право на розвиток і т. д.). Перелік прав третього покоління намагалися продовжити на неурядовому рівні. Але головна проблема, що виникла і потребує обговорення на міждержавному і науковому рівнях, – це проблема зв'язку прав людини і прав народів. Очевидно, не можна відокремлювати права людини від прав народів. Права народів також можуть розглядатися як права людини. Ці права – колективні права людини, але їх поняття не вичерпується правами третього покоління. Вони ширші. Наприклад, права професіпок також можуть вважатися колективними. У деяких випадках сполучення різних індивідуальних прав утворить нове, синтетичне право, що належить уже колективу. У такому плані можна розглядати право на проведення мирних зборів.

Дискусії про третє покоління прав людини, що продовжуються, свідчать про те, що перелік прав людини не є чимось сталим і може бути продовжений.

Четверте покоління прав. З розвитком інформаційного суспільства виникла думка про нове покоління прав і свобод – *прав людини в інформаційному суспільстві (комунікаційні права)* [69; 87]. Т. Корнєєва у [87, с. 503] аргументує пропозицію щодо запровадження четвертого покоління прав та свобод наступним чином – "оскільки інформаційне суспільство стає реальною дійсністю з розширенням інформаційних технологій, електронних комунікацій, які стали невід'ємними потребами людського життя, то і на місцевому, і на глобальному рівнях виникає необхідність гарантування прав людини в інформаційному суспільстві.

По-перше, різні здобутки технологій (Інтернет) є засобом підтримки реалізації прав людини, їх інформаційного поширення. По-друге, у структурі сучасного громадянського суспільства є значна група прав людини, пов'язаних з участю в інформаційних відносинах".

Із зазначеною вище пропозицією погоджується О.В. Аиілогов, який у [69, с. 14] пише: "...у наш час перед державою постає низка проблем, пов'язаних із забезпеченням доступу громадянина до інформації за допомогою мережі Інтернет, охороною конфіденційності індивідуальних (приватних) електронних баз даних, електронних відправлень тощо. ...В разі бездіяльності органів державної влади, місцевого самовря-

дування чи перевищення ними наданих законом повноважень щодо управління інформаційно-комунікаційною сферою може складати предмет адміністративного судового процесу в Україні. Права людини і свободи громадянина в галузі інформаційних технологій від їх порушень суб'єктами владних повноважень утворюють об'єкт забезпечення національною адміністративною юстицією".

1.2. Інформаційна політика

1.2.1. Інформаційна політика розвинених країн

Сучасна інформаційна політика розвинених країн світу розглядається як сукупність напрямів і способів діяльності компетентних органів держави з контролю, регулювання та планування процесів в інформаційній сфері щодо одержання, зберігання, обробки, використання та поширення інформації. Держава регулює відповідний розподіл інформаційних ресурсів, загальні принципи інформаційної діяльності, встановлює пріоритети для забезпечення національних інтересів.

Сьогодні розвинені країни світу йдуть шляхом цілеспрямованого правового упорядкування відносин в національному інформаційному просторі, що визначається юрисдикцією відповідної держави, приймають необхідні законодавчі акти, перебудовують діяльність органів державної влади, які відповідають за формування і реалізацію інформаційної політики. Огляд та аналіз концепцій інформаційної політики дає можливість побачити здобутки і перспективи країн, які мають спільну мету у становленні інформаційного суспільства. Наведемо деякі відправні моменти щодо інформаційної політики за кордоном, які визначені, зокрема, у [83, с. 117-122].

Головними напрямами європейської інформаційної політики є [84, с. 56]:

- розвиток інформаційної інфраструктури;
- створення національного інформаційного потенціалу;
- забезпечення доступу до інформації;
- використання інформаційних ресурсів в національних інтересах;
- створення загальної системи охорони інформації (та захисту даних – *від авт.*);
- сприяння міжнародному співробітництву у галузі комунікацій та інформації;
- гарантування інформаційного суверенітету держави;

Велика Британія. Конституції в традиційному розумінні як основного законодавчого акта, який закріплює основи державного ладу, у Великій Британії не існує. У країні діє неписана конституція, складена з норм статутного права, загального права і норм, що представляють собою конституційно закріплені звичаї. Найбільш важливими з них вважаються Білль про права 1689 р. [81, с. 21], Білль про успадкування престолу 1701 р., Закон "Про парламент" 1911 р. і 1949 р. Основним джерелом англійського права є судові прецеденти, тобто рішення судів, що мають обов'язкову силу для них самих і нижчих судів, статути – законодавчі акти британського парламенту і, нарешті, акти, що видаються виконавчими органами так званого делегованого законодавства.

Пройшовши етап послідовного перетворення, у Великій Британії були видані законодавчі акти, що консолідують правові норми по найбільш значних інститутах цивільного і кримінального права. При виданні цих актів не ставилася задача кодифікації цілих галузей права – вони вбирали в себе в упорядкованому вигляді застосовані лише до окремих правових інститутів норми, з численних раніше виданих законодавчих актів, а також найбільш важливі положення, сформульовані в нормах прецедентного права. У результаті цього законодавчим регулюванням була охоплена більшість галузей англійського права, що у багатьох відносинах стало важливішим джерелом права, ніж норми, сформульовані в прецедентах.

За останні десятиліття англійське законодавство стало ще більшої систематизованим. У перспективі передбачено через консолідацію законодавчих актів у різних галузях права провести реформу усього права Англії до його кодифікації.

Сучасна інформаційна політика Великої Британії формується в плані участі у створенні глобальної системи міжнародних відносин і побудови інформаційного суспільства. Ціль інформаційної стратегії Великої Британії – удосконалення умов конкуренції на інформаційному ринку, підвищення ефективності інформаційних послуг і впровадження інформаційно-комп'ютерних технологій у державне управління. Основні завдання британського уряду у сфері інформаційно-комп'ютерних технологій та мереж передбачають:

- реалізацію проекту британської інформаційної супермагістралі (Super Janet) щодо розвитку телекомунікаційних мереж;
- створення сприятливих умов для здійснення бізнесу і підприємництва завдяки застосуванню інформаційно-комп'ютерних технологій та мереж.

Пріоритетами британської інформаційної політики щодо поширення інформаційно-комп'ютерних технологій визначені: освіта, охорона здоров'я, приватний бізнес.

В 1997 р. в урядовій програмі "Відродження нової, молодої Британії" на основі "інформаційного збагачення" були сформульовані принципи інформаційної політики, що передбачають: технологічну нейтральність законів; сприяння міжнародному співробітництву; захист інтересів споживача в комп'ютерних системах і мережах.

Німеччина. Концепція інформаційної політики передбачає: вільний транскордонний обмін інформацією і свободу на вільне висловлення своїх поглядів і переконань; розвиток інформаційно-комп'ютерних технологій та мереж; свободу конкуренції в інформаційній сфері; створення відповідно до нових політичних, економічних та інформаційних змін певних норм і принципів правового регулювання інформаційної діяльності у німецькому суспільстві.

Уряд Німеччини з огляду на політичну та економічну роль інформаційних процесів і технологій прийняв чотири програми, кожна з яких має відповідні цілі.

Перша програма (1974 – 1977 рр.) ставила за мету забезпечити громадськості доступ до інформаційних систем, накопичення знань з інформаційних процесів, проведення політичних дискусій із проблем інформаційного розвитку суспільства.

Друга програма (1985 р.) передбачала переорієнтацію федеральної інформаційної політики з обмеження регуляції урядом і розвиток приватної ініціативи щодо:

- ринку інформаційних ресурсів та інформаційного бізнесу, лібералізації у відношенні інформаційної діяльності приватного сектору;
- гарантій вільного обігу інформації і посилення міжнародної позиції Німеччини в області міжнародного інформаційного обміну;
- забезпечення доступу до міжнародних інформаційних систем і мереж німецьких підприємств, орієнтованих на застосування інформаційно-комп'ютерних технологій, сприяння приватному інформаційному бізнесу;
- створення телекомунікаційних мереж у напрямах: охорона здоров'я, біологія, сільське господарство, наука, патенти, технології і бізнес, юриспруденція.

Третя програма (1994 р.) "Федеральна підтримка нових комп'ютерних та інформаційних технологій". Вона передбачала запровадження контролю з боку міністерств за здійсненням фінансування нових напрямів діяльності державних установ і приватних підприємств, інформаційних центрів і служб.

Четверта програма "Info-2000: німецький шлях до інформаційного суспільства" передбачає формування інформаційного суспільства в країні, що має на меті:

• створення інформаційної економіки, розвиток інформаційних мереж, інформатизацію державного управління;

• лібералізацію телекомунікацій, підтримку національного виробника електронних продуктів, одночасний розвиток державного і приватного бізнесу;

• активізацію розширення обміну інформацією між урядами Земель та суб'єктами інформаційної діяльності, а також посилення відповідальності Земель щодо контролю за змістом інформації. Федеральний Закон про телекомунікації (1991 р.) надає Землям право на стимулювання розвитку нових інформаційних послуг та ліцензування інформаційної діяльності щодо обмеження поширення інформації забороненого змісту (насильство, агресія, порнографія, злочини). Політичні аспекти Закону про Інтернет 1997 р. стосуються прав і обмежень на свободу поглядів, змісту інформації, що призводить до політичної нестабільності;

• сприяння розвитку національних мереж у країнах Західної і Центральної Європи, СНД, країнах "третього світу". Інформаційна політика Німеччини спрямована на сприяння реформуванню державного управління в цих країнах, їх участі у вільному транскордонному обміні інформацією, пропаганду ідеалів європейської демократії, створення правової бази, технічного оснащення інформаційного сектору і підготовку кваліфікованих фахівців для національних і приватних корпорацій, організацій, фондів та ін.

Франція. Мета інформаційної політики Франції – розвиток інформаційних магістралей, електронного ринку і банківської сфери, лібералізація регулювання відносин щодо комунікацій, реформування інформаційного законодавства, стимулювання наукових досліджень в області інформаційних продуктів, створення систем інформаційної безпеки і попередження комп'ютерних злочинів.

Різні погляди політичної еліти на стратегію створення інформаційного суспільства стримують прогресивний рух країни в плані глобального співробітництва. Високий інформаційний потенціал країни, зокрема, власна космічна індустрія, електронне виробництво, програмне забезпечення, великий спектр інформаційних послуг і політика обмеження для закордонних компаній (8 % присутності у французькому інформаційному середовищі, обов'язковий переклад французькою аудіо-, відео-, кінопродукції або титри французькою мовою, державний контроль інформаційної діяльності і монополія держави в застосуванні інформаційно-комп'ютерних технологій та мереж), недостатньою мірою сприяють лідерству країни в європейському регіоні.

У 1998 р. Франція в Програмі побудови інформаційного суспільства визначила пріоритетні напрями міжнародного співробітництва. В Програмі зазначено, що формування нових інформаційно-комп'ютерних технологій вимагає цілісної системи в підходах до правових, науково-дослідних, прикладних і зовнішньоекономічних аспектів глобальної комунікації і викликає необхідність проведення міжнародних консультацій із проблем універсалізації мереж, охорони приватного життя, вільного обміну даними та ін. На базі Програми був розроблений план дій щодо поліпшення міжнародного інформаційного обміну і підкреслена важливість ринку електронного бізнесу та інформаційних послуг.

Стратегія інформаційної політики Франції стосується також франкомовних країн Африки, Азії, Латинської Америки. У контексті цієї глобалізації комунікацій і просування національних інтересів у треті країни уряд створив Фонд допомоги і співробітництва для підтримки впровадження нових французьких інформаційних технологій.

Сполучені Штати Америки. За доктриною США, право виконує роль буфера між інтересами держави і фізичної особи.

Інформаційна політика здійснюється в руслі загальної юрисдикції, відповідно до якої з 1820-х рр. ведеться систематизація норм загального законодавства з одночасним залишенням за судами широких повноважень його тлумачення. Причому, відмінність американської правової системи від англійської – визначальне місце Конституції як джерела права.

Протягом XIX століття в штатах починалися спроби кодифікації законів за окремими галузями права, що далеко не відразу і не у всіх випадках приводило до їх офіційного видання. У наш час законодавство США набуло вигляд і продовжує удосконалюватися значною мірою в плані кодифікованого, а не просто консолідованого змісту. Федеральне законодавство нині публікується в систематизованому вигляді як Зведення законів США, що складає 50 розділів, кожний з яких присвячений певній галузі права, наприклад, розділ 40 – "Патенти", розділ 7 – "Сільське господарство", розділ 50 – "Війна і національна оборона". Деякі його розділи – це просто зведення близьких за змістом актів, виданих у різний час і мало пов'язаних між собою. Інші, навпаки, містять у собі кодекси законів відповідної галузі права, складені за певною схемою. Зведення законів перевидається кожні 6 років. Приймаючи черговий закон, Конгрес вказує, яке місце він має зайняти у Зведенні законів і які зміни у зв'язку з цим треба внести в розділи, глави, параграфи чинного Зведення.

Наприкінці 1980-х рр. у структурі світового ринку виникли процеси інтенсифікації в організації бізнесу. Це було викликано тим, що, по-перше, інформаційно-комп'ютерні технології дають можливість "перебудувати" світовий ринок значно простіше і швидше, ніж суто організаційні заходи. По-друге, Інтернет став перетворювати бізнес на процес організації глобальних комунікацій без національних кордонів. Для збереження лідерства і регулювання процесів інтенсифікації бізнесу США в 1993 р. прийняли державну програму під назвою "Національна інформаційна інфраструктура" (NII), яка базується на потенційних можливостях Інтернету [83, с. 186-188], що трохи відрізняється від європейського підходу до побудови інформаційного суспільства [83, с. 189-192].

Метою національної інформаційної політики США є впорядкування інформаційних потоків у політичній, економічній, науковій і військовій галузях в інтересах забезпечення збалансованості між державним контролем і свободою підприємницької діяльності. Інформація розцінюється як один з основних національних ресурсів, а системи, що забезпечують її створення, обробку і поширення, розглядаються як головний стратегічний фактор розвитку індустрії інформації і побудови інформаційної інфраструктури. Концепція національної інформаційної політики США передбачає необхідність розширення й удосконалення інформаційного середовища під своєю егідою, посилення впливу на такі регіони, як країни Латинської Америки, Центральної і Західної Європи, Азійсько-Тихоокеанського регіону.

Інформаційна політика США визначається як комплекс нормативно-правових актів державного сектору, покликаних заохочувати і регулювати створення, використання, збереження, передачу і поширення інформації. Її пріоритетами є:

• підтримка наукових досліджень і розробок у сфері інформатизації і телекомунікацій, сприяння обміну технологіями між університетами і фірмами;

• створення й удосконалення інформаційної інфраструктури, у тому числі глобальної інформаційної інфраструктури;

• забезпечення збалансованості між основними інформаційними цінностями, яку може бути порушено в результаті введення нових інформаційних технологій, а саме –

конфіденційністю інформації, інформацією як суспільним надбанням і благом, інформацією як товаром, інформацією як невід'ємним елементом функціонування держави;

• недоторканність приватного життя і захист персональних даних у різних областях державного управління і приватного сектору;

• удосконалення державної політики у сфері телекомунікацій.

Основні принципи інформаційної політики надають громадянам США невід'ємні права: на свободу інформації (зокрема, у засобах масової інформації), на публічні (відкриті) судові процеси, на обвинувачувальну інформацію, інтелектуальну власність, на ознайомлення з урядовою інформацією, на охорону і безпеку інформації та ін.

Доступ до інформаційних матеріалів, що зберігаються в державних органах США, визначений законами "Про свободу інформації" 1966 р. і "Про охорону особистої таємниці" 1974 р. Закони встановили правило, за яким всі особи, які бажають отримати інформацію з державних органів, можуть офіційно її запросити. Відомості з будь-якого федерального відомства повинні безперешкодно надаватися будь-якому бажаючому їх одержати, якщо вони не входять до кола визначених законом винятків.

Згідно із Законом 1974 р. усім громадянам США забезпечується право на ознайомлення з персональними даними, зібраними про них владою. Певні відомості не підлягають розголосу згідно із Законом 1966 р., що забороняє доступ сторонніх особам "до суто особистих, медичних і подібних досьє, оскільки це було б явно невиправданим вторгненням у приватне життя людини". Іншими словами, інформація, на яку поширюється чинність Закону 1966 р., доступна всім, а відомості, захищені Законом 1974 р., надають тільки тим, кого вони стосуються. Дія законів не поширюється на правоохоронні органи.

Варто також звернути увагу на такий важливий аспект. Згідно з принципами європейського права охорона інформації виходить з положень авторського права, а в США – із права, що визначає інтереси споживача інформації.

У вересні 1976 р. Конгрес США прийняв Закон "Про висвітлення діяльності уряду", який розширював права громадян на одержання інформації про діяльність адміністративних органів. Законом передбачається, що всі засідання колегіальних органів адміністративних агентств, що складаються з осіб, призначених Президентом, стосовно яких приймаються рішення, повинні бути відкритими для широкої публіки. Обмеження встановлені лише відносно інформації, яка:

• стосується питань національної безпеки і зовнішньополітичної діяльності уряду, а також того, що має бути у таємниці із погляду на інтереси бізнесу;

• стосується внутрішньої діяльності адміністративних органів;

• розкриває відомості, отримані в ході проведення розслідувань;

• торкається таких питань, що у відповідності до спеціальних нормативних актів не повинні розголошуватися.

Рішення про те, яка інформація має бути закритою, приймається більшістю голосів членів відповідного компетентного органу. Законодавством передбачена можливість оскарження рішення стосовно тлумачення інформації.

Японія. За попередніми даними, Японія відстає від США більше ніж на 5 років у сфері розповсюдження персональних комп'ютерів, кабельного телебачення, електронної телефонії та в інших аспектах інформаційної політики.

З ініціативи Ради з телекомунікацій при Міністерстві пошти і комунікації Японії розроблена національна програма під назвою "Бачення інформаційних комунікацій XXI століття". Головна мета – створення ефективного інформаційного суспільства, цілі якого близькі до цілей створення Національної інформаційної інфраструктури США.

Особливе значення ця програма надає, з одного боку, зростанню економіки, створенню нових видів інформаційного бізнесу і робочих місць, а з іншого – соціальному розвитку країни.

Японська версія побудови інформаційної супермагістралі базується на засобах волоконно-оптичного зв'язку, що надає урядовим інститутам, державним організаціям і приватним підприємствам доступ до програмного забезпечення, що дістають найбільшого поширення. Японія має намір увійти до Глобальної інформаційної інфраструктури і надає великого значення міжнародній кооперації з питань електронної економіки.

Кабінетом Міністрів Японії заснований центр сприяння становленню інтелектуального інформаційно-комунікаційного суспільства, призначений для інтеграційних заходів щодо створення Національної інформаційної інфраструктури і кооперації зусиль з входження до Глобальної інформаційної інфраструктури. Уряд сприяє розробці нових інформаційно-комп'ютерних технологій, особливо тих, що стосуються органів влади, е-медицини, інтелектуально-інформаційних систем (створення штучного інтелекту), урядових довідкових послуг, системи управління ліквідацією наслідків стихійних лих і кризових ситуацій. Через суспільні інститути уряд заохочує виконання програми "Інформаційна грамотність населення".

Росія. Інформаційна політика Росії забезпечується законодавством країни, зокрема Концепцією правової інформатизації Росії (1993 р.), Законом "Про інформацію, інформатизацію і захист інформації" (1995 р.), Законом "Про участь у міжнародному інформаційному обміні" (1996 р.), Концепцією формування і розвитку єдиного інформаційного середовища Росії і державних інформаційних ресурсів (1998 р.) та ін.

У концепції і законах визначаються першочергові завдання інформаційної політики і становлення демократичних інститутів, а саме:

• інтеграція країни в міжнародне інформаційне середовище;

• демонополізація інформаційних служб і структур;

• розвиток ринку інформаційних ресурсів разом з державним регулюванням інформаційної діяльності;

• створення умов для підприємництва в інформаційній сфері і захисту інформації;

• забезпечення конституційних гарантій свободи слова, вільного функціонування засобів масової інформації та ін.

З метою вироблення стратегії інформаційної політики робочою групою Експертної ради з інформаційних технологій при Адміністрації Президента Російської Федерації в 2001 р. розроблений проект програми інформатизації Росії "Біла Книга інформаційних технологій". Програма містить попередні рекомендації з участі Росії в міжнародних ініціативах відповідно до Окінавської Хартії глобального інформаційного суспільства [2, с. 193-196], підписаної лідерами країн "великої вісімки" під час зустрічі в 2000 р.

На підставі рекомендацій і після їх широкого обговорення передбачалося вироблення базового документа, що міг би лягти в основу:

• загальної термінологічної і понятійної бази в сфері інформаційних технологій;

• бачення місця Росії у глобальному інформаційному суспільстві;

• виявлення критичних точок впливу інформаційно-комп'ютерних технологій на розвиток економіки і соціальної сфери;

• позиції стосовно міжнародних ініціатив із подолання інформаційної нерівності.

Вищезазначене тісно пов'язане з дослідженням регуляції інформаційних відносин, кодифікації інформаційного законодавства та формування інформаційного права в Росії. У роботі [90] визначається, що у юридичній літературі термін "інформація" у сполученні з терміном "право" уперше було використано наприкінці 1970-х рр., але трохи

в іншій інтерпретації. А.Б. Венгеров запропонував поняття "інформаційного права" як сукупності норм про роботу з інформацією в управлінні при автоматизації.

Приблизно через 10 років І.Е. Маміофа розробив концепцію "програмного права", що обслуговує відносини в сфері індустрії інформатики.

І.З. Карась, Ю.М. Городецький і В.П. Тихомиров висловилися за використання поняття "право інформатики", де мова йде про право, яке регулює відносини, що стосуються створення алгоритмів перетворення інформації, функціонування інформаційних систем, створення штучного інтелекту, експертних систем, баз знань.

Практично в той же час І.Н. Грязіним пропонується поняття "інформаційно-комп'ютерне право", покликане регулювати відносини, пов'язані з інформацією і програмними засобами.

На початку 1990-х рр. Ю.М. Батуріним досить детально розроблялася ідея "комп'ютерного права", що забезпечує регулювання інформаційних відносин, пов'язаних зі створенням і використанням електронно-обчислювальних машин. До цієї ідеї у 1997 р. звертається І.Л. Бачило, який підтримує думку щодо гіперсистемного правового утворення в інформаційній сфері, але розглядає її в обсязі терміна "інформаційно-комп'ютерне право".

У 1995 р. А.Б. Агаповим висувається пропозиція про "інформаційне право" як відокремлену сукупність інформаційних законодавчих актів, що інкорпоруються у структуру федерального права.

У 1997 р. В.А. Копилов у [91, с. 16] відстоює поняття "інформаційного права" як системи норм і відносин, що виникають в інформаційній сфері, та визначає, що в основі "програмного права" лежать відносини, що виникають із створення, поширення та використання програмних продуктів; в основі "права інформатики" – відносини, які існують в області інформатики – науки, яка вивчає проблеми створення, поширення та використання інформації; в основі "комп'ютерного права" – відносини, які існують у зв'язку із створенням, поширенням та використанням комп'ютерів. Щодо терміна "інформаційно-комп'ютерне право", то В.А. Копилов вважає, що у широкому розумінні – це об'єднання множин відносин щодо інформації та відносин щодо комп'ютерів, а у вузькому розумінні – це добуток цих двох множин. Він також зазначає, що "правову інформатику" слід розглядати як науку про створення, перетворення та споживання правової інформації.

Всі зазначені терміни визначають складові частини інформаційного права у комплексному його розумінні. Цю тезу В.А. Копилов розвиває та конкретизує у 2002 р. у наступній роботі під назвою "Інформаційне право" [92]. Зазначимо також, що дещо раніше його думку підтримав М.М. Рассолов, який у [94] висловив важливі питання нової комплексної галузі права. Зазначений погляд на перспективи розвитку правового регулювання в інформаційній сфері одержав підтримку в жовтні 1999 р. на першій Всеросійській конференції з проблем становлення інформаційного суспільства в Росії.

На початку 2009 р. у Кремлі відбулося перше засідання Ради з розвитку інформаційного суспільства при Президентові Росії (указ про її створення був підписаний в листопаді 2008 р.) [246]. На засіданні Президент Росії різко розкритикував повільний розвиток в Росії інформаційного суспільства. Він підкреслив, що ніякий прогрес і модернізація неможливі без інформаційних технологій: *"Это касается и научно-технической сферы, и собственно вопросов управления, и даже вопросов укрепления демократии в стране"*. За останні роки, за словами Президента, інформаційні технології і інформаційні послуги стали достатньо істотною статтею російського несировинного експорту, досягнувши рівня приблизно в $1 млрд. Проте, як заявив Д. Медведєв, *"все это нас не*

устраивает, потому что по ключевым показателям мы еще страшно далеки от большинства развитых государств". Незважаючи на те, що у Росії високий *"інтелектуальний потенціал і маса програмістів"*, відставання від країн-лідерів не зменшується, а, навпаки, наростає. *"По индексу развития электронного правительства мы были в 2005 г. на 56-м месте, а в 2007 г. достигли 92-го. О чем это говорит? Это говорит о том, что у нас никакого электронного правительства нет, все это – химера. В рейтинге готовности стран к сетевому миру мы тоже на "почетном" 72-м месте"*.

Зокрема, Д. Медведєв зазначив, що весь документообіг в органах державної влади дотепер ведеться на папері, а *"компьютеры в основном используются как пишущие машинки"*. Відсутні сучасні системи планування і сучасні системи фінансово-управлінської звітності. Для громадян нема можливості відправити з особистого комп'ютера заяви або прослідити за проходженням свого запиту в тому або іншому відомстві, одержати електронну довідку за системою електронного єдиного вікна: *"Мы должны были создать единый портал государственных и муниципальных услуг, он должен был заработать с 1 января наступившего года. Этого тоже не произошло"*. Кажучи про розвиток інформаційних технологій в соціальній сфері, Президент Росії підкреслив, що потрібно починати масове навчання вчителів новим технологіям.

На закінчення засідання Ради було схвалено створення спеціальних робочих груп для контролю за інформатизацією в різних сферах. У регіонах за цим напрямом повинні бути призначені відповідальні на посаді віце-губернаторів.

1.2.2. Інформаційна політика в Україні

Інформаційна політика України визначається Конституцією України (1996 р.), законами України "Про наукову і науково-технічну діяльність (1991 р.), "Про інформацію" (1992 р.), "Про науково-технічну інформацію" (1993 р.), "Про захист інформації в автоматизованих системах" (1994 р.), "Про друковані засоби масової інформації" (1992 р.), "Про авторське право та суміжні права" (1993 р.), "Про національний архівний фонд і архівні установи" (1993 р.), "Про телебачення і радіомовлення" (1995 р.), "Про Концепцію Національної програми інформатизації" (1998 р.), "Про Національну програму інформатизації" (1998 р.), "Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" (2007 р.), а також іншими чинними нормативними актами загального і спеціального змісту, в яких визначені співвідношення верховенства міжнародних норм і національні пріоритети. Здійснений нами аналіз законодавства України в сфері інформації та інформатизації, коротку анотацію базових законів, які регулюють найбільш загальні аспекти відносин, а також можливі напрями удосконалення інформаційного законодавства надано у [95].

Закон України "Про інформацію" від 02.10.1992 р. № 2657-XII [5] – перший в Україні закон, який заклав правові основи інформаційної діяльності, визначив головні напрями і способи державної інформаційної політики, закріпив право громадян України на інформацію і визначив правові форми міжнародного співробітництва в галузі інформації. Значною заслугою розробників закону є те, що вони вперше запропонували і визначили право власності на інформацію (ст. 38), надали інформації статус товару та вказали порядок її ціноутворення (ст. 39). Також важливою новацією у законі є те, що вперше у ньому були означені правові формули щодо захисту персональних даних людини (у законі застосований термін "інформація про особу" (ст. 23), хоча на той час у стандартах європейського законодавства вказана інформація визначалась як "персональні дані").

Сьогодні розвиток інформаційного середовища визначається комплексом нових

досягнень прогресу, серед яких:

- швидка зміна інформаційно-комп'ютерних технологій;
- переведення інформації в цифровий формат (дигіталізація);
- формування транснаціональних інформаційних потоків;
- переміщення капіталів у цю сферу як найбільш прибуткову;
- висока конкуренція серед провідних виробників, їх об'єднання і дезінтеграція.

Обов'язковою частиною підготовчих заходів для приєднання до ЄС є створення в країнах-кандидатах умов для побудови інформаційного суспільства. Тому у рамках Національної програми інтеграції України в ЄС передбачається вирішення ряду загальнодержавних проблем, зокрема:

- гармонізація чинних і розробка нових законодавчих актів з інформатизації в Україні відповідно до вимог ЄС та імплементації положень європейських нормативних актів, що регулюють відносини в сфері інформації та інформатизації;
- формування стратегії й основ державної політики підтримки українського сегменту мережі Інтернет, сприяння розповсюдженню різноманітної і достовірної інформації про Україну за допомогою мережі Інтернет, забезпечення інформаційної відкритості суспільства;
- сприяння доступу фізичних і юридичних осіб до світових інформаційних ресурсів тощо.

Законом України "Про Концепцію Національної програми інформатизації" від 04.02.1998 р. № 75/98-ВР [29] окреслено принципи державної політики в сфері інформатизації, здійснивши досить глибокий аналіз процесу інформатизації в Україні. Державна політика інформатизації розглядається "як складова частина соціально-економічної політики держави в цілому і спрямовується на раціональне використання промислового та науково-технічного потенціалу, матеріально-технічних і фінансових ресурсів для створення сучасної інформаційної інфраструктури в інтересах вирішення комплексу поточних та перспективних завдань розвитку України як незалежної демократичної держави з ринковою економікою". До загальних принципів державного регулювання зазначеної сфери Закон відносить принципи "централізації і децентралізації, саморозвитку, самофінансування та самоокупності, державної підтримки через систему пільг, кредитів, прямого бюджетного фінансування".

Закон України "Про Національну програму інформатизації" від 04.02.1998 р. № 74/98-ВР [30], який включає зазначену вище Концепцію, сукупність державних, галузевих, регіональних програм та проектів стосовно місцевого самоврядування у цій сфері, став своєрідним імпульсом щодо початкових дій, позначивши механізми їх реалізації.

21 вересня 2005 р. на парламентських слуханнях з питань розвитку інформаційного суспільства в Україні (відповідно до Постанови Верховної Ради України від 17.03.2005 р. № 2488-IV) зазначалося, що "в розбудові інформаційного суспільства в Україні є певні досягнення, але й існує багато невизначеностей. Практично не сформульована дієва національна політика щодо побудови інформаційного суспільства в Україні...". В інформаційно-аналітичних матеріалах до парламентських слухань відповідні проблеми зокрема, що стосується стану інформаційного законодавства, інформаційних ресурсів, надання послуг, науки та освіти, були висвітлені наступним чином:

- *стратегія розвитку інформаційного суспільства*: недосконалість національної стратегії розвитку інформаційного суспільства; непослідовність і неузгодженість реалізації державної стратегії виконавчими органами; слабка консолідація зусиль державного, бізнесового і суспільного секторів щодо реалізації національної стратегії; наявність значної кількості неузгоджених загальнодержавних, галузевих, регіональних, бізнесових програм і проектів у сфері розвитку і використання ІКТ;
- *законодавча база*: різноплановість нормативно-правового регулювання суспільних відносин в інформаційній сфері; відсутність, неузгодженість, суперечливість, неповнота законодавчих і підзаконних актів у сфері телекомунікації, використання Інтернет-технологій, створення і використання електронних інформаційних ресурсів і продуктів, використання електронного документообігу і електронного підпису, інформаційної безпеки тощо;
- *електронні інформаційні ресурси*: недостатня кількість необхідних технічних стандартів, загальнодержавних, галузевих класифікаторів і довідників із створення і використання електронних інформаційних ресурсів; неузгодженість мережі центрів, що надають послуги щодо збереження і захисту даних, створення віртуальних серверів, веб-хостингу;
- *електронні інформаційні ресурси органів державної влади та місцевого самоврядування*: недостатні повнота, актуальність і достовірність інформації, що представлена на веб-сайтах; низький рівень підготовки фахівців, які займаються підготовкою і розміщенням інформаційно-довідкових та аналітичних матеріалів на відповідних веб-сайтах; недостатній рівень інтерактивності; низька ергономічна культура і невисокий дизайнерський рівень веб-сайтів;
- *електронні інформаційні ресурси освіти*: гальмування створення єдиного інформаційного освітнього простору; відсутність державних методичних рекомендацій щодо створення системи електронних інформаційних ресурсів у галузі освіти; не розроблено заходів щодо стимулювання створення спеціальних шкільних порталів;
- *електронні інформаційні ресурси сфери відпочинку і розваг, культури та спорту*: відсутність дієвої державної політики підтримки створення електронних інформаційних ресурсів в архівах, бібліотеках і музеях; неузгодженість в них технічної і технологічної інфраструктури; невисокий рівень підготовки персоналу для роботи з інформаційними технологіями; відсутність дієвої державної політики з консолідації зусиль бізнесу зі створення електронних інформаційних ресурсів у різних областях відпочинку, спорту;
- *електронні інформаційні ресурси засобів масової інформації*: відсутність державного протекціонізму щодо створення електронних інформаційних ресурсів невеликих по тиражах ЗМІ, особливо регіональних; юридична невизначеність статусу засобів масової інформації, що створюють виключно електронні інформаційні ресурси; не визначено юридичний статус самого електронного інформаційного продукту, що продукується легальними ЗМІ;
- *надання електронних послуг населенню і бізнесу органами державної влади та місцевого самоврядування*: відсутність чітко визначеної урядової концепції організації надання електронних послуг населенню і бізнесу; недостатня організація міжвідомчої спільної роботи для реалізації принципу "єдиного вікна"; юридична невизначеність статусу і переліку урядових е-послуг для органів державної влади всіх рівнів; недостатня інформатизація внутрішніх управлінських і зовнішніх міжвідомчих процесів державних органів влади; низький рівень використання комп'ютерних аналітичних методів обробки даних у державних органах влади;
- *електронна торгівля*: нерозвиненість карткових систем безготівкових платежів; аморфність державної політики по відношенню до ініціатив різних соціальних проектів, заснованих на використанні карткових систем безготівкових розрахунків;
- *наукові дослідження і система освіти в сфері ІКТ*: недостатній розвиток фундаментальних досліджень у сфері ІКТ; безсистемність і фрагментарність прикладних

наукових досліджень у сфері розвитку і використання ІКТ; практично повна відсутність вітчизняних прогнозів розвитку ІКТ, рекомендацій щодо впровадження ІКТ у різні сфері діяльності країни;

• *дистанційне навчання*: юридична невизначеність системи дистанційної освіти; недостатнє методичне опрацювання проблем впровадження; невизначеність системи дистанційної освіти (в цілому та із викладання окремих дисциплін); слабкий організаційний і технологічний рівень підтримки дистанційної освіти; невисока готовність професорсько-викладацького складу до роботи в умовах дистанційного навчання;

• *комп'ютерна грамотність населення:* неоднозначність в реалізації державної політики в області комп'ютеризації шкіл; відсутність широкого методологічного опрацювання використання комп'ютерних мультимедійних технологій при викладанні всіх шкільних предметів; нерозвиненість системи навчання студентів та перепідготовки вчителів особливостям роботи з технологіями; відсутність загальнодержавної програми підвищення комп'ютерної грамотності населення; відсутність інфраструктури її підвищення; не сформована державна політика із перепідготовки фахівців бізнесу з урахуванням специфіки їх діяльності й особливостей використання ІКТ у конкретній предметній області; відсутність мережі спеціалізованих центрів перепідготовки фахівців різних галузей народного господарства; нескоординована та несистемна реалізація державної політики перепідготовки державних службовців щодо використання ІКТ; практична відсутність технічної та технологічної інфраструктури перепідготовки державних службовців.

У січні 2007 р. Верховною Радою України прийнятий Закон України № 537-V "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" [37]. У Загальних положеннях Закону зазначено, що "одним з головних пріоритетів України є прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвиткові та підвищуючи якість життя".

У Загальних положеннях Закону визначається, зокрема: "ступінь розбудови інформаційного суспільства в Україні порівняно із світовими тенденціями є недостатнім і не відповідає потенціалу та можливостям України, оскільки:

• розвиток нормативно-правової бази інформаційної сфери недостатній;

• рівень інформатизації окремих галузей економіки, деяких регіонів держави є низьким;

• відсутня координація зусиль державного і приватного секторів економіки з метою ефективного використання наявних ресурсів;

• створення інфраструктури для надання органами державної влади та органами місцевого самоврядування юридичним і фізичним особам інформаційних послуг з використанням мережі Інтернет відбувається повільно;

• ефективність використання фінансових, матеріальних, кадрових ресурсів, спрямованих на інформатизацію, впровадження ІКТ у соціально-економічну сферу, зокрема в сільське господарство, є низькою;

• наявне відставання у впровадженні технологій електронних бізнесу, бірж та аукціонів, електронних депозитаріїв, використанні безготівкових розрахунків за товари і послуги тощо;

• рівень комп'ютерної та інформаційної грамотності населення є недостатнім, впровадження нових методів навчання із застосуванням сучасних ІКТ – повільним;

• спостерігається поглиблення "інформаційної нерівності" між окремими регіонами, галузями економіки та різними верствами населення".

Основним завданням розвитку інформаційного суспільства в Україні Закон декларує "сприяння кожній людині на засадах широкого використання сучасних ІКТ – можливостей створювати інформацію і знання, користуватися та обмінюватися ними, виробляти товари та надавати послуги, повною мірою реалізовуючи свій потенціал, підвищуючи якість свого життя і сприяючи сталому розвитку країни на основі цілей і принципів, проголошених Організацією Об'єднаних Націй, Декларації принципів та Плану дій, напрацьованих на Всесвітніх зустрічах на вищому рівні з питань інформаційного суспільства (Женева, грудень 2003 року; Туніс, листопад 2005 року) та Постанови Верховної Ради України від 1 грудня 2005 року "Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні".

Законом визначено основні засади – концептуальна основа для завдань щодо розвитку інформаційного суспільства в Україні як одного з пріоритетних напрямів державної політики, що, зокрема, передбачає вдосконалення законодавства з регулювання інформаційних відносин.

Згідно із Законом, національна політика розвитку інформаційного суспільства в Україні ґрунтується на засадах: пріоритетності науково-технічного та інноваційного розвитку держави; формування необхідних для цього законодавчих і сприятливих економічних умов; всебічного розвитку загальнодоступної інформаційної інфраструктури, інформаційних ресурсів та забезпечення повсюдного доступу до телекомунікаційних послуг та ІКТ; сприяння збільшенню різноманітності та кількості електронних послуг, забезпеченню створення загальнодоступних електронних інформаційних ресурсів; поліпшення кадрового потенціалу; посилення мотивації щодо використання ІКТ; широкого впровадження ІКТ в науку, освіту, культуру, охорону здоров'я, охорону навколишнього середовища; забезпечення інформаційної безпеки.

Законодавче забезпечення розвитку інформаційного суспільства передбачає створення цілісної системи законодавства, гармонізованої з нормами міжнародного права з питань розвитку інформаційного суспільства, зокрема здійснення кодифікації інформаційного законодавства. Кодифікаційний акт має включати в себе розділи, зокрема про засади електронної торгівлі, правову охорону прав на зміст комп'ютерних програм, удосконалення захисту прав інтелектуальної власності, в тому числі авторського права при розміщенні та використанні творів у мережі Інтернет, про охорону баз даних, дистанційне навчання, телемедицину, надання органами державної влади та органами місцевого самоврядування юридичним і фізичним особам інформаційних послуг з використанням Інтернету тощо.

1.3. Рефлексивне управління суспільною думкою

1.3.1. Ретроспективний аналіз маніпулювання свідомістю

У соціальних науках поширеним є метод звертання до ретроспективного аналізу подій для того, щоб виявити певні аналогії в закономірностях суспільного розвитку, отримати ті уроки, які дозволять врахувати позитивні і негативні тенденції, у тому числі ті, що супроводжують періоди кризових соціально-політичних і економічних змін. Проте історія вчить, що вона нічому не вчить. Більш того, усі знають, що мозок народжує думку, але ніхто не знає, як вона народжується.

У 1930-ті рр. Е. Фромм досліджував особливості індивідуальних, групових і масових психологічних явищ в періоди соціальних криз [96]. В результаті аналізу ним були виявлені закономірні історичні аналогії в особливостях психології людей в періоди кризових суспільних змін. Він зіставив сучасні йому реалії з даними епох Відродження і Реформації, оскільки саме в ці історичні періоди в ряді країн здійснювався перехід до якісно нових суспільних форм життя людей, відбувалася ломка відповідних економічних структур, соціальних інститутів і суспільних відносин, різко змінювалася державна ідеологія, індивідуальна і суспільна психологія.

Інтерес до цього аналізу пояснюється тим, що розглянуті Е. Фроммом соціальні процеси за силою і спрямованістю дії на суспільну та індивідуальну психологію мають багато спільного з тим, що відбувається в Україні, Росії й інших країнах СНД. Окрім цього, багато одержаних ним результатів цілком можуть бути застосовані як відправні моменти для розуміння людиною суті тих соціальних явищ, які звалилися на неї сьогодні, а також для визначення основних напрямів формування інформаційно-психологічного захисту від них.

У проведеному порівняльному аналізі Е. Фромм показав, що середньовічне суспільство, з одного боку, було жорстко структуроване і обмежувало свободу людини як особистості, але з другого – психологічно давало йому відчуття більшої упевненості.

Розглядаючи епоху Відродження і відзначаючи її прогресивність, Е. Фромм, разом з тим, показує наскільки проник в неї маніпулятивний підхід у взаємостосунках між людьми. Наскільки глибоко він уразив і вищий клас, і тим більше низи суспільства. Звернемо увагу і на наступний висновок, тобто на те, що сам перехід до епохи Відродження і її розквіт були пов'язані як з втратою "середньовічних кайданів", так і з переходом до нових форм дії на людей – психологічних маніпуляцій. *"Возрождение*, – пише він, – *было культурой богатого и сильного класса, который оказался на гребне волны, поднятой штормом новых экономических сил. Простой народ, которому не досталось ни нового богатства, ни новой власти, превратился в безликую массу, которая потеряла уверенность своего прежнего положения; этой массе льстили или угрожали, но власть имущие всегда манипулировали ею и эксплуатировали ее".*

Іншими словами, Відродження було культурою не для дрібних торговців або ремісників, а для багатих аристократів і бюргерів. Їх економічна діяльність, їх багатство давали їм відчуття свободи і усвідомлення індивідуальності. Але і вони теж зазнали втрат: втратили ту упевненість і відчуття приналежності, які забезпечувала їм середньовічна соціальна структура. Вони стали вільніші, але і більш самотні. Вони користувалися своєю владою і багатством, щоб вичавити з життя всі радощі до останньої краплі; але при цьому їм доводилося застосовувати всі засоби – від психологічних маніпуляцій до фізичних тортур, щоб управляти масами і стримувати конкурентів усередині власного класу.

Всі людські відносини були отруєні цією смертельною боротьбою за збереження та примноження багатства завдяки можливостям влади. Солідарність з побратимами або випадкові з членами свого класу змінилася цинічним відособленням; інші люди розглядалися як "об'єкти" використання і маніпуляцій або безжально знищувалися, якщо це сприяло досягненню власних цілей. Індивід був охоплений пристрасним егоцентризмом, ненаситною жагою багатства і влади. В результаті було отруєне і ставлення процвітаючого індивіда до своєї власної особи, його відчуття упевненості в собі і відчуття безпеки. Він сам перетворився на такий самий об'єкт власних маніпуляцій, на який раніше були перетворені ним інші. І є всі підстави сумніватися в тому, що повновладні господарі епохи Відродження були такі щасливі і упевнені в собі, як це часто

зображають. Виходить, що перехід від "середньовічних оков" до епохи Відродження привів до змін у взаємостосунках і психології людей, деякі аспекти чого визначались у наступному.

По-перше, до безпрецедентного за масштабами і активністю застосування маніпуляцій свідомістю людини. Особистість, об'єднання людей, соціальні групи стали цілком цілеспрямовано розглядатися як об'єкти маніпуляцій, як засоби досягнення цілей одними людьми за рахунок маніпулювання іншими.

По-друге, самі маніпулятори перетворилися на об'єкти власних маніпуляцій, тобто, перетворюючи інших на об'єкти маніпуляцій, людина стає таким самим об'єктом маніпулювання.

По-третє, зникли відчуття упевненості і безпеки, які змінилися відчуттями нікчемності і беззахисності у більшості людей, що не одержали ні влади, ні багатства.

По-четверте, люди зуміли правдою-неправдою дістати багатство і владу, продовжили в демагогічній та цинічній формі їх примножувати, удаючи з себе поборників чесності та справедливості завдяки, зокрема різних дрібних подачок та обіцянок.

Відмова від жорстких суспільних зв'язків у державі, перехід від детально регламентованої поведінки людей за допомогою цілої системи соціальних інститутів примушення (монопольної ідеології), за допомогою яких і здійснювалося соціальне управління, породжують нові форми маніпуляцій, по-суті більш витончених, пов'язаних не із зовнішнім примушенням, а з масованою дією на суспільну й індивідуальну психіку особи в обхід свідомого контролю, через сферу неусвідомлюваних, нечітко усвідомлюваних і несвідомих реакцій психіки людини [97].

Розглядаючи причини внутрішнього конфлікту людини, відомий американський психоаналітик К. Хорні виказала вельми цікаву думку, яку можна вважати однією з важливих істин: *"Противоречие в том, что, с одной стороны, мы ценим и превозносим концепцию конкуренции как двигателя прогресса, а с другой – не устаем пропагандировать братскую любовь и смирение"* [98, с. 128].

За прогнозами учених, завдяки сучасним можливостям поширення інформації деструктивні маніпуляції людиною, громадською думкою і масовою свідомістю можуть разом з національними конфліктами, екологічними катастрофами і демографічними бідами перетворитися на ще одну глобальну світову проблему [99].

Висунення маніпуляцій як суспільно-психологічного явища на провідне місце в системі загроз інформаційно безпеки особи визначається наступними чинниками:

- масовим впровадженням маніпуляцій свідомістю в інформаційно-комунікативні процеси, ефект дії яких набагато посилюється широкомасштабним і стихійним розповсюдженням новітніх інформаційних технологій, засобів комунікації, телекомунікаційної техніки;
- різким збільшенням кількості суб'єктів маніпулятивної дії (політичні, релігійні, громадські організації, рекламні агентства, комерційні структури, окремі особи і т. д.), що мають доступ до сучасних маніпулятивних технологій і засобів поширення інформації та даних;
- відсутністю дієвої системи психологічного захисту особи в масштабах суспільства в цілому, оскільки традиційні захисні механізми зруйновані або просто неадекватні сучасним умовам, а нові не поспішають формуватися в плані їх відповідності міжнародним стандартам;
- стихійним і масовим розповсюдженням новітніх маніпулятивних технологій (наприклад, нейролінгвістичне програмування тощо) [100];

• слабкою сформованістю у громадян індивідуального психологічного захисту від маніпулятивної дії, оскільки порівняно з багатьма іншими країнами, де процес застосування маніпуляцій свідомістю і відповідно формування захисних механізмів здійснювався протягом довгого часу, населення виявилося не готовим до адекватної соціальної активності в принципово новій суспільно-психологічній ситуації і інформаційному середовищі, що якісно змінилося;

• підвищеною схильністю значної частини населення підпадати під маніпулятивні дії у зв'язку з тривалим знаходженням у кризових умовах кардинальної зміни суспільства (зокрема, трансформація правової системи, системи державного управління тощо), що різко знижує опір маніпулятивній дії.

Зазначені вище складові маніпулювання перешкоджають формуванню адекватної інформаційно-орієнтованої основи соціальної поведінки і в цілому життєдіяльності особи, пригнічують її емоційно-вольову сферу. Це в свою чергу робить неможливим формування стійкої системи суб'єктивних відносин, стимулює не прогнозовану рухливість і різкі коливання соціально-політичних орієнтацій, оцінок, установок у значної частини населення, що трансформується в нестабільність соціальних і політичних процесів та соціально-політичної ситуації в цілому в країні, виступаючи як одна із загроз інформаційній та національній безпеці в політичній, соціальній і економічній сферах.

Людина – істота соціальна. Як говорив Аристотель, тільки боги і звірі можуть жити поза суспільством. Індивідуум – це ідеальне уявлення про ізольовану людину, яке склалося в XVII столітті при виникненні сучасного західного суспільства. Саме латинське слово "індивідуум" – це переклад грецького слова "атом", що означає "неподільний". Людина виникає і існує тільки у взаємодії з іншими людьми і під їх впливом. Закладена в нас природою програма поведінки недостатня для того, щоб ми були людьми. Вона доповнюється програмою, записаною у знаках духовності, моралі, а також у системі правових норм, встановлених державою. Наші уявлення і поведінка завжди знаходяться під дією і впливом інших людей та громадської думки. Причому, уявлення і поведінка кожній людини можуть піддаватися так званій "маніпуляції".

Західна цивілізація розглядається суспільством вільних індивідуумів, що живуть на основі права. Закон і громадянські права, що охороняються державою, поставили в цивілізовані рамки довічну *"войну всех против всех"*, боротьбу за існування. Один з головних філософів громадянського суспільства Т. Гоббс (1588 – 1679 рр.) [166] називав державу, здатну цивілізувати цю війну, Левіафаном (на ім'я могутнього біблійного чудовиська) та вважав, що кінець війни може бути покладено в результаті укладення договору між людьми [75, с. 234-242]. Проте ця війна стала всеосяжною конкуренцією, а суспільне життя – ринком.

Англійський філософ, засновник лібералізму Д. Локк (1632 – 1670 рр.), соціально-політична концепція якого базується на природному праві та теорії суспільного договору, усвідомлював, що прагнення до вигоди роз'єднує людей, бо *"никто не может разбогатеть, не нанося убытка другому"* [75, с. 257-264]. Свободу індивідуума розуміють перш за все як роз'єднання через конкуренцію. У політичній сфері цьому відповідає демократія, яка передбачає наявність конкуренції, що не може існувати без, зокрема, "інформаційної війни". Головним у підтримці порядку є свобода індивідуума, що дозволяє йому в кожному акті війни робити усвідомлений раціональний вибір і укладати вільний контракт. Не важливо, чи йде мова про купівлю або продаж робочої сили, тієї або іншої жувальної гумки або партійної програми (на виборах). Це – ідеал. У чистому вигляді він не досягається. Питання в тому, на якому шляху розвитку суспільство наближається, а на якому віддаляється від ідеалу.

Сьогодні значна частина мислителів вважає, що, зробивши маніпуляцію свідомістю головною технологією панування, Захід зробив фатальну помилку і зайшов у безвихідь. Причина в тому, що маніпуляція свідомістю здійснюється завжди приховано, й це позбавляє індивідуума свободи значно більше, ніж пряме примушення. Жертва маніпуляції повністю втрачає можливість раціонального вибору, бо її бажання програмуються ззовні. Таким чином, її становище в конкуренції, у "війні всіх проти всіх" різко погіршується. Фактично, це – ліквідація духовності та громадянських прав, а значить, ліквідація найпринциповішої основи західної цивілізації. На її місці виникає нова, гірша форма тоталітаризму, що замінила батіг набагато ефективнішим і більш антигуманним інструментом – "індустрією масової культури", що перетворює людину на програмованого робота. Як сказав німецький філософ Краус про нинішню правлячу верхівку Заходу: *"У них пресса, у них биржа, а теперь у них еще и наше подсознание"* [101, с. 27].

Корінням слово "маніпуляція" є латинське manus – "рука" ("manipulus" – "жменя", від "manus" і "ple" – "наповнювати"). У словниках європейських мов слово тлумачиться як поводження з об'єктами з певними намірами, цілями (наприклад, ручне управління, огляд пацієнта лікарем за допомогою рук і т. д.). Мається на увазі, що для таких дій потрібна спритність і вправність. У техніці ті пристосування для управління механізмами, які ніби є продовженням рук (важелі, рукоятки), називаються маніпуляторами. Звідси з'явилося сучасне переносне значення слова – спритне поводження з людьми як з об'єктами, речами.

Виданий в 1969 р. в Нью-Йорку "Сучасний словник соціології" визначає маніпуляцію як "вид застосування влади, за якого володіючий нею впливає на поведінку інших, не розкриваючи особливість поведінки, яку він від них чекає" [101, с. 11]. Таким чином, це поняття означає набір способів прихованого управління.

У сучасному значенні маніпуляція – це частина технології влади, спрямованої на програмування думок і уявлень людей, їх настроїв і навіть психічного стану з метою забезпечити таку їх поведінку, яка потрібна тим, хто володіє засобами маніпуляції. Французький письменник Л. Вовенарг писав: *"Искусство нравиться – это искусство обманывать"*. Генріх Гейне зауважив: *"Тот, кто хочет влиять на толпу, нуждается в шарлатанской приправе"*. Відомий фахівець з управління С. Паркінсон, предметом дослідження якого є бюрократизм державної адміністрації, зазначає: *"В динамичном обществе искусство управления сводится к умению направлять по нужному руслу человеческие желания. Те, кто в совершенстве овладел этим искусством, смогут добиться небывалых успехов"* [102].

Якщо узагальнити визначення, які дають авторитетні зарубіжні дослідники явища маніпуляції, то можна виділити її головні, родові ознаки.

По-перше, це вид інформаційно-психологічної дії (не фізичне насильство, але може передбачати загрозу насильства). Мішенню дій маніпулятора є свідомість, психіка людини та колективів людей.

По-друге, маніпуляція – це прихована дія, факт якої не повинен бути усвідомлений об'єктом маніпуляції. Успіх маніпуляції гарантований, коли той, хто піддається маніпуляції, вірить, що все те, що все відбувається, природне і неминуче. Коротше кажучи, для маніпуляції потрібна фальшива дійсність, в якій її присутність не відчуватиметься.

Коли спроба маніпуляції розкривається і це стає достатньо широко відомим, акція звичайно припиняється, оскільки розкритий факт такої спроби завдає маніпулятору збитку.

Ще ретельніше ховається головна мета – так, щоб навіть викриття самого факту спроби маніпуляції не призвело до з'ясування подальших намірів. Тому приховування

інформації – обов'язкова ознака, хоча деякі прийоми маніпуляції включають гру в щирість і в правдивість відомостей, що надаються.

По-третє, маніпуляція – це дія, яка вимагає значної майстерності і знань. Зустрічаються, звичайно, талановиті самородки з могутньою інтуїцією, здібні до маніпуляції свідомістю оточуючих за допомогою доморослих засобів. Але розмах їхніх дій невеликий, обмежується особистою дією – в сім'ї, в бригаді, в роті або банді. Якщо ж ідеться про суспільну свідомість, про політику, хоча б місцевого масштабу, то, як правило, до розробки акції притягуються фахівці або хоча б спеціальні знання, що беруться з літератури або інструкцій. Оскільки маніпуляція суспільною свідомістю стала технологією, з'явилися професійні працівники, що володіють цією технологією (або її частинами). Виникла система підготовки кадрів, установи, наукова і популярна література, див., зокрема [103 – 106].

Ще важлива, хоча і не така очевидна ознака: до людей, свідомістю яких маніпулюють, ставляться не як до осіб, а як до об'єктів, особливого роду речей. Маніпуляція – це частина технології задля коштів та влади, за якою ховається бажання використати об'єкта маніпуляції тільки на свою користь.

Як правило, в поняття маніпуляції не включається поняття "етикет" – дія на поведінку оточуючих за допомогою алегорій і умовчань, мови знаків, зрозумілих, можливо, у певному середовищі. Коли людина звертається до іншого, використовуючи прийоми етикету (наприклад, витончено ввічливо), вона, звичайно, прагне видинути на поведінку партнера на свою користь. Але це не маніпуляція, оскільки тут не приховуються ні факт дії, ні наміри. Навпаки, знакова мова повинна бути зрозумілою, інакше спроба дії не може бути вдалою. Без етикету жити в суспільстві не є можливим. Застосовуючи правила етикету, ми не поводимося з людиною як з річчю, ми поважаємо її як особистість (хоча може бути й по-іншому: говорять "здрастуйте", а в підсвідомості – "щоб тебе біс забрав").

Обман, будучи одним з важливих прийомів у всіх технологіях маніпуляції, сам по собі не завжди має маніпулятивну дію. Помилкова інформація, впливаючи на поведінку людини, аніскільки не зачіпає її дух, наміри й установки. Тому, наприклад, поняття маніпуляції не стосується немовлят, оскільки вони не можуть ухвалювати самостійних рішень і відчувати себе відповідальним суб'єктом.

Будь-яка маніпуляція свідомістю є взаємодією. Жертвою маніпуляції людина може стати лише в тому випадку, якщо вона виступає як її співучасник. Тільки якщо людина під впливом одержаних сигналів або відомостей перебудовує свої переконання, думки, настрої, цілі і починає діяти за новою програмою – маніпуляція відбулася. А якщо вона засумнівалася, захистила свою духовну програму, вона жертвою не стає. Маніпуляція – це не насильство, а спокуса. Кожній людині дана свобода духу і свобода волі. Значить, вона навантажена відповідальністю – встояти, не впасти в спокусу. Одна з головних ознак того, що в якийсь момент здійснюється програма маніпуляції свідомістю, полягає у тому, що люди раптом перестають слухати розумні переконання – вони неначе бажають бути обдуреними.

Головні труднощі створює той бік маніпуляції, який позначається як "прихованість", та ще за наявності майстерності й спритності. Професійні маніпулятори, як і фокусники, своїх секретів не розкривають. Навіть мемуари, в яких вони хваляться досягненнями в цій царині, покликані швидше напустити туману, ніж просвітити і попередити нащадків.

Таким чином, дійсне значення слів і справ авторів та виконавців акцій з маніпуляції свідомістю завжди ретельно приховане, і потрібна серйозна розумова робота щодо

їх виявлення. Виявлення реального значення в словах і діях людей, які прагнули це значення приховати, є інтерпретацією, тлумаченням. Вони можуть допомогти людині, яка хоче по можливості захистити свою особисту свідомість від маніпуляції.

Підходячи до висловів або фактів як до об'єкта розуміння (або розслідування), необхідно із самого початку усвідомлювати, що зміст слів та дії, до яких вони закликають, є лише одна з можливих версій. І на цьому першому етапі вони не мають ніяких переваг перед іншими можливими версіями, які ми зобов'язані побудувати самі, без підказки, без емоцій. Тобто до будь-яких слів і справ політиків і їх ідеологів треба підходити, як слідчий, що вислуховує перше пояснення підозрюваного. У цьому немає порушення презумпції невинуватості – ні слідчий, ні ми не відкидаємо можливості, що надана версія істинна, не називаємо її автора брехуном або злочинцем. Але і не приймаємо її відразу за істину. Ми хочемо встановити істину.

Перша (і, ймовірно, головна) умова успішної маніпуляції полягає в тому, що в переважній більшості випадків нема бажання витрачати душевні і розумові сили, час на те, щоб просто засумніватися. Багато в чому це відбувається тому, що пасивно зануритися в потік інформації набагато легше, ніж критично переробляти кожен сигнал. На це ніяких сил не вистачить, якщо людина не оволоділа до автоматизму деяким набором контролюючих "розумових інструментів", які самі собою, без зусиль свідомості й волі, аналізують інформацію за однією ознакою: чи є в ній симптоми маніпуляції.

Приховане значення є у всіх словах і всіх діях. Людина, що "набила руку" в тому, щоб шукати різні значення слів і дій, відразу помічає повідомлення, в яких є симптоми наявності прихованого значення. При цьому має бути відчуття міри.

Наука створила інтелектуальні інструменти, корисні для людини, які будують захист від маніпуляцій. І навіть не просто інструменти, а цілий методологічний підхід, який називається "герменевтика". У початковому значенні герменевтика (від грецького слова "роз'ясню") – наука про тлумачення текстів [101].

Герменевтика виникла вже в епоху еллінізму для вивчення і тлумачення старих текстів (наприклад, Гомера). До речі, вже тоді у зв'язку із сліпотою Гомера було сказано про труднощі правильно тлумачити слова, якщо немає можливості самому побачити, про що йде мова.

У Середньовіччі головним предметом герменевтики стало Священне Писання. Європа наповнилася богословами, які вели нескінченні диспути і породжували єретичні тлумачення. В епоху Відродження герменевтика стала важливим прийомом у суспільних наукових пошуках. Її активно застосовував Ніколо Макіавеллі – політик, що заклав основи нового вчення про державу. Він першим заявив, що влада тримається на силі і злагоді. Звідси витікає, що "монарх" має безперервно вести особливу роботу щодо завоювання і утримання влади [107]. Тому саме явище маніпуляції довго позначалося словом "макіавеллізм". Вважається, що політична філософія Макіавеллі передбачила діяльність якобінців у Великій французькій революції, які здійснили грандіозну за своїми масштабами маніпуляцію масовою свідомістю.

Нинішні дослідження показали, що праці Макіавеллі про державу, які сприймалися як виключно оригінальні, є плід його досліджень "герменевтики" старих авторів. Він по-новому інтерпретував деякі роботи Платона, Теренція, Лівія і Данте, а також свої власні уявлення. У нашому столітті Антоніо Грамши обдумував грандіозний план – "переписати" книгу Макіавеллі "Монарх" з висоти досвіду XX ст. У своїх одкровеннях Макіавеллі висловив думку, важливу безпосередньо для теми: слова політиків завжди потребують тлумачення. Він загострив це питання до межі, зізнавшись в листі від 17 травня 1521 р.: *"Долгое время не говорил я того, во что верю, никогда не верю я и в то,*

что говорю, и если иногда случается так, что я и в самом деле говорю правду, я закутываю ее такой ложью, что ее тяжело найти".

У XIX столітті герменевтика стала загально філософським методом і дуже розширила коло об'єктів. З її допомогою історики намагалися відновити, реконструювати духовність і культурне значення подій минулих епох. Підходом герменевтики користувалися і користуються найбільші філософи нашого часу (Хайдегер, Хабермас, Фуко).

Сьогодні сфера дії герменевтики як наукового підходу значно розширилася. Слово (і текст) стали розглядати лише як приватний вираз ширшого поняття – знака. Всі ми знаємо, що поширення інформація може втілюватися в найрізноманітніших знакових системах. Одяг, поза, жест можуть бути красномовнішими за слова, це – "невербальні тексти". За оцінками американських психологів (Дж. Руш), мова жестів налічує 700 тисяч чітко помітних сигналів, тоді як найповніші словники англійської мови містять не більш як 600 тисяч слів. Адже, крім жестів, є безліч інших знакових систем. Тому завжди є необхідність інтерпретувати, тлумачити будь-яке повідомлення, якій знаковій системі воно б не належало.

Будь-який жест, вчинок має, окрім очевидного, видимого значення, безліч підтекстів, у яких виражають себе різні іпостасі, різні "маски" людини. Спілкування людей – безперервний театр, а іноді й карнавал цих масок-персон (звідси з'явилося поняття "персональні дані"). Латинське слово "персона" походить від назви білої маски в античному театрі і буквально означає "те, через що проходить звук" ("per" – "через", "sonus" – "звук"). У цих масок рот робився з розтрубом, щоб підсилювати звук.

Дуже важко правильно зрозуміти значення повідомлень, що "вдягнуті" в слова і дії людей. Навіть в рамках однієї культури тлумачення слів і вчинків людей іншого кола, іншого положення (духовності) – непроста задача.

Який же головний принцип герменевтики, на чому засноване тлумачення текстів або подій? На тому, що слово або жест вбудовуються в їх контекст. Вже текст – від латинського "тканина", "зв'язок" (звідси поняття – "текстура") – є спільність думок і слів, скріплена безліччю зв'язків, частина з яких прихована. А контекст – набагато ширша спільність, в яку вплетений текст, і вплетений зв'язками вже в основному прихованими. І рівень розуміння тексту залежить від того, як глибоко і широко ми змогли ці зв'язки уловити, тобто тлумачити.

Інтерпретація, тлумачення – це відновлення неявних або спеціально прихованих зв'язків з контекстом. Успіх цієї справи визначається знанням, умінням, волею і творчими здібностями читача або спостерігача. Знання можна придбати, уміння виробити. Ми на маленькій фотографії відразу впізнаємо людей і навіть уявляємо їх образ "як живий". А дикун у джунглях, коли йому показують фотографію навіть знайомих предметів і людей, дивиться на неї абсолютно байдуже і нічого не бачить – він не навчений сприймати ці образи.

Але знання і уміння мало. Без роботи розуму, духу і уяви нічого не вийде. Коли ми дивимося на пейзаж талановитого художника, ми так живо відтворюємо в нашій уяві картину, що здається, ніби художник виписав всі деталі, кожен листочок на дереві. Але ж це неможливо. Листочків він виписав дуже мало, і вони непропорційно великі. Якби художник зобразив деталі точно, ми б просто не впізнали б образ. Він, знаючи закони сприйняття, тільки натякнув нам, дав знак, а картину ми створили (разом з ним, з його умілими знаками) в нашій уяві. Ми – співавтори картини.

Яку ж мету переслідує той, хто бажає маніпулювати свідомістю людини, коли посилає повідомлення у вигляді текстів або вчинків? Його мета – дати такі знаки, щоб ми, вбудувавши ці знаки в контекст, змінили образ цього контексту в нашому сприйнятті.

Він підказує такі зв'язки свого тексту або вчинку з реальністю, нав'язує такс їх тлумачення, щоб наше уявлення про дійсність було спрямоване в бажаному для маніпулятора напрямі. А значить, це вплине і на нашу поведінку, причому ми будемо упевнені, що вчиняємо в повній відповідності з нашими власними бажаннями.

Сказати слово або зробити дію, які б так торкнулися струн душі, щоб ми раптом побачили дійсність в спотвореному вигляді саме усупереч нашим інтересам – велике мистецтво. Таке слово і такий вчинок не можуть бути ясними, світлими, зрозумілими, вони обов'язково звернені до чогось прихованого від розуму.

Яка задача людини, що, не бажаючи бути пасивною жертвою маніпуляції, робить маленьке дослідження у дусі герменевтики – намагається дати свою інтерпретацію словам і вчинкам? Вона полягає в тому, щоб відтворити в думці (можливо, повніше) реальний контекст повідомлення і різними способами вбудувати в нього почуте або побачене. Зрозуміло, абсолютно повно відтворити дійсність неможливо, потрібно провести відбір істотних її ознак.

Особливо важливо і важко відтворити спеціально приховувані сторони дійсності і їх зв'язок з повідомленням. Потрібно шукати інтерес. Ще стародавні римляни говорили "шукай, кому вигідно". Проте ця рекомендація може застосовуватися для того, щоб направити пошук у помилковому напрямі. Пошук прихованого значення – психологічно важкий процес. Він вимагає інтелекту, мужності і свободи волі, адже потрібно на час скинути тягар авторитету, яким часто володіє відправник повідомлення.

Вважається, що люди в своєму підході до інтерпретації поділяються на два основні типи. Одні починають з того, що прагнуть в міру можливості чітко відновити логіку автора повідомлення, до нори відставляючи убік свої власні версії. Якщо вони знаходять в цій логіці вади і в автора повідомлення "кінці з кінцями не в'яжуться", тут вони і починають "копати". Інші не витрачають часу на те, щоб реконструювати "інтелектуальні інструменти" авторів повідомлення. Вони приймають готовий висновок повідомлення як одну з допустимих версій, але лише одну з декількох можливих, і приступають до вироблення набору своїх версій. Вони конструюють контексти, приміряючи до них запропоновану версію.

На практиці обидва підходи застосовуються в тій або іншій комбінації. Як вважає П. Рікер, важливо засвоїти головне: *"Множественность интерпретаций и даже конфликт интерпретаций является не недостатком или изъяном, а достоинством понимания, образовывающего суть интерпретации"*. Справа не в тому, щоб скласти з декількох версій одну "усереднену". Тільки аналізуючи різні версії можна наблизитися до істини, особливо коли деякі фігуранти зацікавлені в її приховуванні.

На жаль, дуже часто ми спостерігаємо звуження свідомості: одержавши повідомлення, ми відразу ж з упевненістю приймаємо для себе одне-єдине його тлумачення. І воно служить для нас керівництвом до дії. Часто це відбувається тому, що ми з "економії мислення" слідуємо думки "авторитету", ажіотажу мітингу, укоріненим забобонам. Знаходячись під впливом якогось одного стереотипу, ми на практиці робимо великі помилки. І навіть неважливо, чи беззастережно віримо брехливому повідомленню, чи вибудовуємо власну помилкову його інтерпретацію – в обох випадках поведінка неадекватна реальності, і людину може чекати невдача.

При цьому врятуватися від маніпуляції за допомогою упертості, просто слідуючи своїй думці, неможливо. Можна лише протриматися якийсь час, поки зацікавлені особи не підберуть інші докази, зіграють на емоціях або в інший спосіб вплинуть на свідомість і вчинки.

1.3.2. Основні поняття та головні чинники маніпуляції

Поняття, що визначають прояв маніпулювання та приховане примушення людини, можна умовно поділити на дві основні групи, згідно з якими вони застосовуються у повсякденній мові та у практиці управління й науки.

До першої групи можна віднести наступні поняття: "афера", "блеф", "демагогія", "інтрига", "махінація", "обман", "хитрість", "шахрайство" (рос. мов. – жульничество, мошенничество, плутовство).

Афера – несумлінна, протизаконна або сумнівна з погляду законності справа, сумнівна операція, "темна" справа, махінація [108, с. 65; 109, с. 354].

Блеф – 1) обман із метою створення перебільшеного уявлення про свої сили, можливості, значимість і т. ін.; 2) прийом у карточній грі в покер [110].

У переносному значенні: вигадка, обман, що має на меті залякати, вселити перебільшене уявлення про себе; вигадка, обман через хвалібу або розрахований на залякування, введення в оману будь-кого; вигадка, брехня з метою залякати або вселити іншому перебільшене уявлення про будь-що [108, с. 204; 109, с. 93; 111, с. 98].

Брехня (рос. – ложь) – невідповідність істині, те, чого немає насправді.

Дезінформація (фран. "desinformation" від "des…" – префікс, що означає "знищення", "відсутність" чи "спотворення" інформації) – 1) свідоме неправдиве повідомлення, відомості, що перекручуються і поширюються з метою уведення в оману; 2) введення в оману невірними відомостями, брехнею [144]. Це поняття включає і передбачає підробку документальних доказів з тим, щоб викликати у відповідь дію з боку скомпрометованих осіб або організацій.

В Україні згідно з ДСТУ 3396.2-97 "Технічний захист інформації. Терміни та визначення" під дезінформуванням розуміють спосіб технічного захисту інформації, який полягає у формуванні свідомо хибної інформації для унеможливлення несанкціонованого доступу до істинної інформації.

За допомогою дезінформації певні сили, органи, організації, особи прагнуть ослабити позиції опонентів, конкурентів, приховати власні прорахунки і провали. Дезінформація нерідко застосовується державно-владними органами задля досягнення політичних, військових, пропагандистських та інших цілей, щоб позбавити населення, окремі соціальні групи орієнтації у подіях життя (див. підрозділ 2.4.3).

Демагогія (від грец. "народ" і "вести") – маніпулювання інформацією, спекулятивне спотворення фактів, свідоме застосування у корисливих цілях неправдивих, нереальних для практичного втілення обіцянок [144]. У побуті це поняття є синонімом слів "базікання", "балаканина", а в суспільно-політичної практиці розглядається як оціночна особливість публічних промов, виступів, заяв, котрі не містять у собі конструктивної ідеї, пропозицій, заплутують певну проблему, відвертають увагу від складних, першочергових питань і завдань.

Демагогія розглядається не тільки як негативне явище, а й потужний і небезпечний засіб маніпуляції масовою та індивідуальною свідомістю. Теза нацистської пропаганди у фашистській Німеччині цинічно проголошувала: "Брехня, для того щоб у неї повірили маси, повинна бути абсолютною".

Демагогія – один з засобів політичної конкуренції і боротьби за владу. Її "майстрами" виявляють себе політики, змушені маскувати своє справжнє обличчя і політичні цілі.

Зовнішніми ознаками демагогії є говірливість з будь-яких питань, фальшивий пафос, гасла, надмірне пишномовство; спотворення фактів, підміна аргументів, применшення потенцій противників; загравання з публікою та апеляція до низьких інстинктів аудиторії, натовпу.

Внутрішніми ознаками демагогії є спекуляція реальними проблемами, сподіваннями людей з метою забезпечення прихованих соціальних, політичних, групових, особистих цілей (досягнення перемоги на виборах та ін.); популістське прагнення зажити авторитету, реалізувати свої цілі за будь-яку ціну; корисливість, авантюризм, гіпертрофоване честолюбство.

Основними гарантами боротьби з демагогією є порядність з плюралізмом думок, розвинене громадянське суспільство, культура толерантності, критичне ставлення до політиків.

Інтрига – 1) приховані зловмисні дії, до яких удаються для досягнення будь-якої мети; 2) підступні, приховані дії, звично непристойні для досягнення будь-чого, направлені проти будь-кого. У літературі інтрига означає схему розвитку подій, що розкриває боротьбу дійових осіб між собою в драматичному або епічному творі [108, с. 204; 110, с. 354; 111, с. 673].

Махінація (від лат. "хитрість", "прийом") – несумлінний спосіб досягнення мети; нечесна, хитра витівка [111, с. 239].

Облуда – удавання, лицемірство з метою обдурювання; фальш, неправда.

Обман – неправдиві слова, дії тощо, що навмисно вводять інших в оману [111, с. 543].

Омана – хибне сприйняття дійсності, зумовлене неправильним, викривленим відображенням її органами чуття; уявний образ чого-небудь, що помилково сприймається як дійсний.

Ошуканство – обман, обдурювання.

Ошукувати – 1) вводити будь-кого в оману діями або словами; обманювати, обдурювати; 2) діяти нечесно, вдаючись до обману, шахрайства.

Хитрість – удавання з будь-яким наміром; що-небудь неясне, незрозуміле, приховане значення будь-чого [111, с. 599]. Хитрий – який приховує свої істинні наміри, йде непрямими, обманними шляхами до досягнення будь-чого; лукавий.

Шахрайство – 1) нечесний, спритний вчинок, обман [111, с. 146]; 2) злочин, що полягає в заволодінні чужим майном або правом на нього, а також в отриманні інших благ шляхом обману, зловживання довірою тощо.

У кримінальному праві Російської Федерації шахрайство – злочин у сфері економіки, направлений проти власності, розкрадання чужого майна або придбання права на чуже майно незаконним шляхом.

В американському законодавстві шахрайство - навмисне спотворення правди з тим, щоб, використовуючи помилкову версію або обман чи зловживаючи довірою, заволодіти цінним майном особи або організації [112, с. 175].

В Україні шахрайство вважається видом майнового злочину, вчиненого за допомогою обману та зловживання довірою (стаття 190 КК України). При шахрайстві потерпілий передає майно або право на нього винному добровільно. Але така добровільність має уявний зміст, оскільки вона викликана обманом. Будучи введеним в оману щодо певних обставин, потерпілий помилково вважає, що особа, якій він передає майно, має право на його отримання. Хоча насправді вона такого права не має. Приблизно за такою ж схемою шахрай заволодіває чужим майном і при зловживанні довірою, коли він, користуючись такою довірою, одержує майно, не маючи при цьому наміру його повернути.

"Шахрайство в Інтернеті". Цей термін стосується махінацій будь-якого виду, де використовуються один або декілька елементів Інтернету – такі як кімнати в чатах,

електронна пошта, дошки оголошень або веб-сайти – для залучення потенційних жертв, проведення шахрайських операцій або для передачі надходжень від шахрайства до фінансових установ або іншим особам, що беруть участь в таких махінаціях.

Якщо достатньо часто користуватися Інтернетом, можна помітити, що події і операції у віртуальному світі звичайно відбуваються в режимі реального часу. Для більшості людей це означає тільки те, що в Інтернеті все, як уявляється, робиться швидше – ділові рішення, пошук інформації, особиста взаємодія і багато що іншого.

Шахраї в Інтернеті теж діють в режимі реального часу. Вони прагнуть максимально застосовувати унікальні можливості Інтернету – такі як розсилка електронних повідомлень за декілька секунд по всьому світу або розміщення інформації на веб-сайті так, щоб вона стала доступна всьому світу, – для проведення різного роду махінацій набагато швидше, ніж раніше.

Перші ознаки того, що вас хочуть обдурити:

- лист-пропозиція прийшов вам як снам;
- вам обіцяють високі прибуток/заробіток/зарплату
- при цьому нічого особливого робити не треба;
- іноді у вас навіть не питають підтвердження кваліфікації;
- вас просять вислати N-у суму грошей за докладну інформацію або за ніби-то поштові витрати;
- на сайті працедавця не вказані контактні дані, в кращому разі вказаний e-mail на безкоштовному хостингу;
- виставлені для перегляду сертифікати неможливо роздивитися;
- вам пропонують роботу, що добре оплачується (від кількох сотень у.о.) з сайта на безкоштовному хостингу (тобто у працедавця немає і 20 доларів на власний домен).

Види шахрайства в Інтернеті. В цілому, всі ті старі схеми махінацій, що переслідували споживачів та інвесторів протягом багатьох років до створення Інтернету, нині з'являються у віртуальному просторі (іноді їм властива певна тонкість, викликана Інтернет-технологіями). При стрімкому зростанні Інтернету, особливо е-комерції, віртуальні злочинці прагнуть представити свої злочинні схеми так, щоб вони якомога більше були схожі на товари і послуги, пропоновані більшістю добросовісних електронних торгівців. При цьому вони не тільки завдають збитків споживачам та інвесторам, але й підривають довіру споживача до законної е-комерції і Інтернету.

Ось кілька видів шахрайства в Інтернеті:

- схеми проведення аукціонів і роздрібної торгівлі в режимі "он-лайн";
- ділові можливості/надомна робота;
- крадіжка особистих даних і шахрайство;
- інвестиційні схеми "он-лайн";
- схеми з використанням кредитних карток.

Нещодавно викрито новий вид шахрайства в Інтернеті. Завзятий бізнесмен Даррен Моргенстерн зумів "поставити на гроші" як мінімум 27 тис. власників сайтів. Всі вони заплатили йому по 70 дол. за позбавлення від мережних шахраїв. Не знаючи, що єдиним шахраєм, який працює проти них, був сам Моргенстерн.

Схема, за якою працював Д. Моргенстерн, була проста і дієва. Чергова жертва (наприклад, власники сайта //www.reuters.com) одержувала лист від якоїсь служби моніторингу доменних імен. У листі указувалося, що якісь зловмисники хочуть зареєструвати домен під назвою, дуже схожою на ім'я домена адресата, наприклад, //www.reuters.net. Пильна служба відзначала, що, на її думку, "новий домен реєструється з непристойною метою", і повідомляла про свою можливість перешкодити реєстраціям, якщо її послуги (всього 70 дол.) будуть сплачені.

Аналіз змісту виділених в першу групу понять дозволяє зробити деякі висновки.

При розкритті їх сутності в описі даних понять застосовується ряд загальних ознак, що виступають як їх особливості. Часто це призводить до того, що значення одного з них визначається через значення іншого. Так, наприклад, маніпуляція визначається як махінація, шахрайство чи омана та ін. У зазначених поняттях можна виділити їх загальний гносеологічний зміст, який передбачає:

- маскування істинних цілей, дій, суть яких полягає, як правило, в отриманні односторонньої або більшої вигоди для ініціатора цих дій;
- застосування методів, що маскують істинні цілі і спонукають скоювати дії, вигідні для ініціатора їх застосування (аферіста, шахрая, махінатора, обманщика тощо).

Ступінь впливу маніпуляцій різний. Від слабко вираженого (хитрість) до найвищого, який перетворює їх на кримінальне суспільно небезпечне діяння (шахрайство, що має кваліфікацію злочину з відповідним складом і запобіжним заходом).

У сутності понять відображаються особливості умов їх застосування (афера – справа, оборудка), сфера застосування (шахрайство – отримання майнової або іншої, переважно матеріальної вигоди), основні прийоми (блеф), механізми (інтрига) тощо.

До другої групи можна віднести поняття: макіавеллізм, стратагеми (стратагемна політика), спеціальні і таємні операції, політичні ігри й інтриги, лобізм.

У поняттях цієї групи, як і попередньої, містяться основні ознаки, що відображають суть прихованого примушення людей до певної поведінки:

- маскування істинних цілей дій, суть яких полягає, як правило, в отриманні односторонньої або більшої вигоди для ініціатора цих дій;
- застосування методів, що маскують істинні цілі й спонукають скоювати дії, вигідні для ініціатора їх застосування;
- небезпека дій, що позначаються даними поняттями, яка полягає в їх загальній негативній моральній оцінці.

У той же час слід зазначити, що відбувається певна трансформація моральної оцінки способів таємного примушення, що використовують у сфері управління. Моральне несхвалення сприяє появі такого прийому, як публічне звинувачення опонентів в їх застосуванні і, таким чином, в порушенні загальноприйнятої етики соціальних відносин.

Насправді ж застосування таких способів у міжнародних відносинах, політичній і економічній боротьбі, протиборстві спецслужб, військовому мистецтві і дипломатії є правилом і, відповідно, впливає на моральну оцінку.

Таким чином, разом із загальною публічною морально негативною оцінкою застосування цих способів, у вказаних сферах соціальної взаємодії оцінка їх застосування визначається такими двома основними принципами, як "мета виправдовує засоби" і "подвійний стандарт". Іншими словами, застосування способів таємного примушення з власного боку виправдане і морально допустиме, а з протилежного – ні, оскільки цілі опонентів нібито не є такими високими і корисними, як свої. Досягнення власних цілей визначає допустимість застосування будь-яких способів і засобів.

Під *макіавеллізмом* розуміють політичну діяльність, що не нехтує будь-якими засобами заради досягнення поставленої мети.

Суть *стратагемної політики* полягає в забезпеченні реалізації підготовленої стратагеми, використовуючи при цьому засоби і методи не з норм і звичаїв міжнародного права, а з теорії військового мистецтва, і ґрунтується на принципі – мета виправдовує

засоби. Змістовна модель стратагеми є синтезом результатів оцінки ситуації і специфічного прийому, виробленого теорією для аналогічної обстановки.

Стратагема, зокрема зовнішньополітична, в інтерпретації фахівців – це, як правило, добре розроблений стратегічний план, націлений на вирішення однієї або кількох найважливіших стратегічних задач зовнішньої політики держави, що передбачає застосування обманних дій (хитрощів, пасток), які вводять противника в оману щодо істинних цілей і спонукають його діяти певним чином, вигідним для протилежної сторони [113, с. 18-47].

Спеціальні і таємні операції є поняттями, що відображають стійкі організаційні форми комплексного застосування різних способів і засобів прихованого примушення людей. Про їх законність як певних норм соціальної взаємодії можуть, зокрема, свідчити наступні факти. Дані поняття введені в офіційне вживання, і їх зміст розкривається у відповідних нормативних і методичних матеріалах та літературних джерелах. Так, наприклад, в законодавстві США наводяться наступні визначення таємних операцій і психологічної війни.

Таємна операція передбачає:

• діяльність зі збору розвідувальної, контррозвідувальної й іншої інформації, таємну політичну або економічну пропаганду і напіввійськову діяльність, що ведеться такими способами, які забезпечують секретність операцій;

• операції проти іноземних урядів, установ і осіб здійснюються так, щоб приховати справжніх організаторів або дозволити їм у разі провалу заперечувати причетність до даних операцій;

• операції негласного розслідування, в яких використовують секретних агентів.

Комплексне застосування різних способів прихованого примушення людей у вигляді системи психологічних операцій і різноманітних пропагандистських акцій та рекламних кампаній виступає як поширений засіб політичної боротьби не тільки в зовнішньополітичній діяльності і в умовах міжнародних конфліктів, але й у внутрішньополітичній діяльності. І в цьому полягає ще одна особливість.

Політичні ігри, інтриги. Мета будь-якої політики – здобуття і утримання влади. У внутрішній політиці інформаційна війна офіційно визначається пропагандистським протистоянням політичних опонентів і агітацією, хоча нерідко набуває складнішою комплексно-маніпулятивного змісту ігор та інтриг, коли в хід ідуть будь-які доводи, звинувачення, компромат (зі скандалами), приховування від громадськості закулісних операцій тощо. Тут війна виступає як дії, направлені на ослаблення морального духу політичних опонентів, на підрив авторитету їх керівників, на дискредитацію їх дій, врешті-решт, на здійснення тиску на погляди окремих людей і громадську думку в цілому для досягнення конкретних цілей [114, с. 323-324].

Лобізм (англ. "lobbysm" від "lobbi" – "приймальна", "кулуари") – специфічний інститут політичної системи, потужний механізм впливу певних соціальних груп і громадських об'єднань ("груп тиску") на процес прийняття рішення органами державної влади з питань політики. Лобіювання – спроба окремих громадян або їх груп впливати не тільки на прийняття, відхилення чи зміну законів у парламенті, а й на адміністративні рішення уряду, спираючись на підтримку як обраних депутатів, так і різних політичних партій, державних і недержавних установ, громадських організацій, ЗМІ. До лобіювання вдаються представники таких соціальних структур, як бізнес, торгівля, освіта, наука, мистецтво тощо.

Мета лобіювання в тому, щоб домогтися від парламенту, президента держави, уряду ухвалення чи відхилення тих або інших законодавчих чи підзаконних актів.

Практично всі великі корпорації та спілки мають у своєму складі особливі підрозділи, що займаються лише цією діяльністю. Заінтересовані групи активно користуються послугами найманих лобістів, якими виступають впливові особи, юридичні, пропагандистські та консультативні фірми. Для досягнення своєї мети застосовуються різні засоби і методи:

• готують і пропонують проекти законів, стратегію та тактику їх просування;
• виступають у комітетах, комісіях парламенту з критикою опонентів;
• представляють інформацію з акцентом на вигідних для себе аспектах;
• координують та контролюють лобістські дії;
• організують кампанії – "тиск з місць" (потоки листів, телеграм, дзвінків);
• фінансують виборчі кампанії;
• вдаються до прямого підкупу посадових осіб.

У 1995 р. Конгресом США прийнятий "Акт про лобіювання", який вимагає реєстрацію лобістів, оприлюднення ними регулярних звітів про свою діяльність. Організаціям, що звільнені від оподаткування та отримують субсидії, забороняється займатися лобіюванням.

В Україні лобізм фактично існує, хоч він не врегульований у законодавчому порядку.

Серед вказаних організаційних форм комплексного застосування способів прихованого примушення людей можна виділити дві основні категорії.

До першої відносяться ті з них, які мають специфічну сферу застосування, обмежену колом об'єктів дії, і не зачіпають безпосередньо в масовому порядку значні групи населення. Це, зокрема, спеціальні й таємні операції, оперативні та політичні ігри, лобіювання. Такі ж організаційні форми, як психологічні операції в політичній боротьбі, інформаційно-пропагандистські і рекламні кампанії направлені, як правило, на більшість населення, тобто для них практично кожна людина є об'єктом дії і прихованого психологічного примушення.

До *головних чинників маніпуляції свідомістю* більшість дослідників відносить брехню, обман та дезінформацію.

Ще античні філософи, починаючи з Аристотеля і Платона, намагалися розібратися не тільки в суті брехні і обману, але й в морально-психологічних аспектах цих явищ, а також виробити рекомендації, що перешкоджатимуть поширенню брехні. Так, займаючись викриттям софістів і їх прийомів у ході різного роду обговорень, Аристотель дійшов формулювань основних законів формальної логіки. У Середньовіччі і у новітній час Монтень, Макіавеллі, Монтеськ'є, Шопенгауер, Дюпра, російські філософи Соловйов, Бердяєв і ряд інших дослідників приділяли аналізу феномена брехні достатньо багато уваги [104].

У наш час у визначення поняття "брехня" вкладають різний зміст. У буденній свідомості вона звичайно асоціюється з негативною, соціально не схваленою дією – обманом, який визначають або як синонім брехні, або як процес, який породжує брехню. Проте, в словниках брехня трактується не тільки як неправда, обман і спотворення істини, але й як вигадка, фантазія і навіть жарт, розиграш. Разом з тим, відомо, що істину можна спотворити ненавмисно, і це буде не брехня, а помилка. Що стосується вигадки, фантазії або жарту, то при їх правильному застосуванні немає наміру завдання збитків об'єкту застосування. *"С психологической стороны,* – пише Т.В. Сахнова, – *обман характеризуется сознательным созданием ложного представления о тех или иных обстоятельствах действительности в сознании другого субъекта. Обманывающий действует умышленно, то есть не только передает ложную информацию (или умалчивает о чем-либо), но и скрывает свои истинные намерения"* [115, с. 80].

У психологічній літературі справедливо підкреслюється те, що стратегією брехні може бути як досягнення, так і уникнення яких-небудь наслідків. *"Лживость – форма поведения, заключающаяся в намеренном искажении действительности ради достижения желаемой цели или стремления избежать нежелательных последствий. В тех случаях, когда лживость становится привычной формой поведения, она закрепляется и превращается в качество личности"* [116, с. 175].

Аналізуючи поведінку дітей, В.В. Зеньковський пише: *"Под ложью мы должны разуметь заведомо лживые высказывания с целью кого-либо ввести в заблуждение: мы имеем здесь три основных момента, одинаково необходимых для того, чтобы была возможность говорить о лжи, – ложное (в объективном смысле) высказывание, сознание того, что это высказывание ложно, и, наконец, стремление придать заведомо ложной мысли вид истины, стремление ввести кого-либо в заблуждение"* [117, с. 215].

Французький дослідник Ж. Дюпра, що займався проблемою брехні в минулому столітті, вважав, що це психо-соціологічний, словесний акт навіювання, за допомогою якого намагаються умисно посіяти в думці іншого яке-небудь позитивне або негативне сприяння, хоче сам той, хто навіює, розуміє, що це не відповідає істині. Ж. Дюпра, також як і сучасні дослідники, вважав, що брехня як навіювана дія може здійснюватися не тільки як словесний акт, а також і за допомогою невербальних засобів спілкування [118]. Відомо багато людей які ефективніше за слова вводять в оману за допомогою жесту, пози, міміки або косметики, гриму, одягу й інших засобів перевтілення і маскування, створюючи помилковий образ або доповнюючи зміст спотвореної інформації невербальними компонентами спілкування.

Із стародавніх часів визначилися два основних підходи до допустимості брехні. Платон, Гегель, Макіавеллі вважали брехню на благо суспільства допустимою і навіть необхідною. "*Уж кому-кому*, – писав Платон, – *а правителям государства надлежит применять ложь как против неприятеля, так и ради своих граждан – для пользы своего государства, но всем остальным к ней нельзя прибегать*". У книзі "Республіка", слідуючи принципу *"стремления к наибольшей выгоде государства"*, Платон надає ще двом соціальним групам – лікарям і суддям – право застосовувати спотворення істини для блага громадян. Платон вважав, *"что судьи имеют право лгать, чтобы обманывать неприятеля или граждан в целях общего интереса, подобно докторам, которые имеют право лгать в интересах своих пациентов"* [74].

Ще категоричніше про допустимість брехні писав Вольтер в XVIII ст., але вважав, що брехня є вищою чеснотою, якщо вона творить добро, причому потрібно брехати, як *"черт, не боясь, не время от времени, а смело и всегда"*. А. Шопенгауер називав заперечення необхідної брехні *"жалкой заплатой на одежде убогой морали"* [119].

Протилежна думка випливає з християнської моралі і розглядає брехню з погляду шкоди, що завдається, а тому не приймається як форма поведінки людини. Єпископ Аврелій Августин заперечував будь-яку форму брехні, вважаючи, що вона підриває довіру між людьми. І. Кант не допускав права суб'єкта на брехню навіть тоді, коли треба дати відповідь на питання зловмисника, чи "удома той, кого він задумав убити". Разом з тим, Фома Аквінський намагався пов'язати виправданість видів брехні з моральним чинником, вважаючи, що гріх брехні загострюється, якщо суб'єкт має намір брехнею заподіяти шкоду іншому, і це називається шкідливою брехнею. Гріх брехні зменшується, якщо вона направлена на добро або розвагу, і тоді ми маємо справу з жартівливою брехнею, або – на користь, й тоді це послужлива брехня, за допомогою якої суб'єкт прагне допомогти іншій людині або врятувати її від шкоди. Російський філософ В.С. Соловйов також вважав за можливе етичну брехню "у порятунок".

Таким чином, думки щодо цієї проблеми достатньо різноманітні, і сучасні дослідження показують, що існує великий діапазон оцінок людьми допустимості брехні в різних сферах життєдіяльності. Можна без перебільшення сказати, що маємо безліч форм людської поведінки, складовою яких є спотворення інформації і введення в оману іншої людини з найрізноманітніших мотивів. У повсякденному житті людина нерідко стикається з ситуацією, коли вирішує дилему – сказати те, що вона дійсно думає чи ні, і його зовнішня поведінка не завжди відповідає суб'єктивному ставлення до дійсності. Але коли і в якій мірі ця брехня, як розглядати подібну дію з моральної точки зору? Навіть умисне умовчання у якихось ситуаціях, наприклад, щодо думки про іншу людину, може мати ті ж наслідки, що і брехня, але, залежно від обставин, це може називатися тактом, дипломатичністю, а може кваліфікуватися як хитрість і лицемірство.

Недостатньо визначати тільки критерій навмисного (свідомого) введення в оману іншої людини, щоб обов'язково говорити про брехню в негативному значенні. Або, як писав Фома Аквінський про "шкідливу брехню" – дружній розиграш або жарт не припускають заподіяння збитків об'єкту їх призначення. Хоча за критерієм свідомості дії і методами дії на об'єкт у багатьох випадках вони подібні з брехнею і обманом. Таким чином, визначення брехні і омани в негативному значенні може включати наступні компоненти: навмисність дії; спотворення реальності (дійсності, фактів, інформації); соціально не схвалювану, неблагородну, перш за все корисну мету, в результаті досягнення якої отримується перевага однієї людини або групи осіб над іншою людиною або групою осіб, яким завдаються збитки.

Виділення як критерію оцінки соціального схвалення (несхвалення) цілей суб'єкта, що вдається до брехні як форми поведінки, є достатньо уразливим моментом. Разом з тим, феномен брехні практично завжди розглядається в контексті соціального середовища. Компонент, що створює сенс, кінцевий результат і мета суб'єкта, якій діє за допомогою брехні, оцінюється з позицій конкретного соціуму. Існує цілий ряд видів професійної діяльності: дипломатія, політика, лікарська практика, військове мистецтво, операції спецслужб, деякі експерименти в психології тощо, в ході яких суб'єкти діяльності приховують свої наміри, цілі, застосовують різні прийоми і маніпулюють людьми, як об'єктами дії. При цьому обман противника на війні – це "військова хитрість", приховування інформації лікарем від пацієнта – "обман у порятунок", таємна операція спецслужб – "оперативна комбінація", приховування планів державними діячами від інших правителів або навіть від власного народу – дипломатія, політика тощо.

Справа не тільки в благозвучності термінів. Передбачається, що суб'єкти названих структур на відміну, наприклад, від шахраїв діють не у власних інтересах, а виконують певне соціальне замовлення і опираються на моральні і етичні норми соціуму, заради інтересів якого здійснюється маніпулювання об'єктом дії, включаючи прийоми і методи обманного змісту. Це психологічна кваліфікація суб'єктивного ставлення до дій за формальними ознаками, цілком відповідними брехні і маніпуляціям.

Що стосується логіки, то істинність або помилковість конкретної думки розглядається незалежно від того, як до цього ставиться той суб'єкт, який виказує брехню. Російський логік С. Поварнін писав: *"...истина будет оставаться истиною, хотя бы ее произносили преступнейшие уста в мире; и правильное доказательство останется правильным доказательством, хотя бы его построил сам отец лжи"* [120, с. 73].

З позицій логіки при оцінці істини не має значення психологічна оцінка щирості суб'єктів спілкування, і навпаки, – людина, говорячи нещиро, може, навіть сама того не бажаючи, висловлювати істинні речі. Це на перший погляд парадоксальне твердження не буде суперечливим, якщо взяти до уваги семантичні відтінки категорій "правда" та "іс-

тина". Перший термін включає суб'єктивний відтінок, тобто елемент особистого ставлення до інформації, що передається. Термін "істина" як категорія логіки і юриспруденції відображає реальний стан явищ. Тому людина, що бажає ввести в оману іншу і повідомляє явно помилкову інформацію (але при цьому сама не має правильного уявлення про те, що повідомляється), може, бажаючи збрехати, говорити істину або бути близькою до неї. Наприклад, підслідний, будучи переконаним у повній непричетності іншої людини, хоче звести наклеп на неї, але при цьому не здогадується, що потрапив якраз у ціль. Або навпаки, через будь-які причини людина приховує від слідства власну думку, що свідчить про злочинну поведінку іншого, таким чином "вигороджує" його, не припускаючи, що насправді приховувана оцінка не відповідає фактам дійсності і він сам помиляється, вважаючи поведінку підозрюваного злочинною. У даних випадках присутній обман як поведінковий акт, але "язовні" висловлюється істина. Подібні сюжети часто стають основою детективних, гумористичних і драматичних історій.

Існують певні відмінності в розмежуванні брехні й обману. Коли ми говоримо про обман, то перш за все маємо на увазі процес, дію. Що стосується понять "брехня", "неправда", то вони перш за все використовуються як оцінка інформації, що не викликає довіри. Критикуючи одне з визначень "обману" зарубіжних дослідників, які вважають, що "обман" може бути визначений як вчинок або твердження, мета якого – приховати істину від іншого або ввести його в оману, В.В. Знаков вважає обман витонченішою формою брехні. Він визначає обман як *"полуправду, сообщенную партнеру с расчетом на то, что он сделает из нее ошибочные, не соответствующие намерениям обманывающего выводы"* [121]. Проте, як він також зазначає, в обмані може і не бути помилкових фактів, достатньо свідомо втаїти частину інформації, що спричинить спотворення об'єктивної дійсності. Можна ввести в оману людину, навіть надаючи йому достовірну інформацію, але подаючи її певним чином, враховуючи психічний стан об'єкта, особові якості, обмежуючи можливості отримання додаткової або уточнюючої інформації. Тому ключовим моментом визначення обману не може бути кількість і якість використаної інформації. Що ж до методів, що дозволяють дезорієнтувати об'єкт дії, то вони можуть бути різними, включаючи і напівправду.

Про витоки схильності до брехні і маніпулювання. Більшість психологів вважають, що найважливіші спонукальні чинники, що роблять вплив на появу схильності до брехні і маніпулювання іншими людьми, слід шукати в соціалізації індивіда, у витоках формування особи, тобто в тому, як протікає її дитинство, як поводиться його оточення, як відбувається подальший розвиток людини, а також у яких умовах він здійснює свою життєдіяльність. Фахівці в області психології, аналізуючи мотиви і умови дитячої брехні, в першу чергу звертають увагу на відчуття страху і боязнь покарання у дітей, які з'являються через дуже жорстоке поводження з ними або природну слабкість і невпевненість, які відчуває дитина, стикаючись зі скрутними ситуаціями.

Відомо, що людина вже на ранніх етапах розвитку проявляє здатність уникати неприємні емоцій з боку агресивного оточення за допомогою маскування і пристосування. Недоброзичливі інтонації, крик, агресивна міміка й інші невербальні компоненти спілкування сприймаються дитиною як акти ворожості з перших тижнів життя, і тому достатньо швидко в нього розвиваються захисні механізми. Згодом, коли дитина прагне приховати непристойні вчинки, вона починає вдаватися до умовчання факту їх скоєння або до прямого заперечення зроблено, тобто починає застосовувати брехню або маніпуляцію стосовно до дорослих.

Крім страху, "пусковим механізмом" застосування брехні дитиною є усвідомлення того, що до нещирості як форми впливу на саму дитину і як способу ефективної психологічної дії на оточуючих вдаються батьки або інші представники його референтних груп. Включення обману в структуру звичної поведінки настає тим швидше, чим менш благополучні умови життя і виховання. Причому розуміння того, що брехня яка є нормою для поведінки дорослих, у певних ситуаціях є шоком для дитини, сприяє переосмисленню стратегій власної поведінки. Формування маніпулятивних тенденцій поведінки, починаючи з дитячого віку, достатньо повно описано американською дослідницею Е. Шостром у книзі "Людина-маніпулятор" [98], а також щодо їх звичайних проявів у подальшому житті в іронічно-саркастичних книгах Сіріла Паркинсона "Закони Паркинсона" [102] та Лоуренса Питера "Принцип Питера, или Почему дела идут вкривь и вкось" [122].

В.В. Знаков зазначає, що *"обращаясь к анализу психологических механизмов вранья, нередко его нужно рассматривать как внешнее проявление защитных механизмов личности, направленных на устранение чувства тревоги, дискомфорта, вызванного неудовлетворенностью субъекта своими взаимоотношениями с окружающими"* [121, с. 251]. Він наводить показовий приклад (цитуючи В. Соловйова) впливу на детермінацію нечесної поведінки обставин іншого рівня, пов'язаних з соціальними умовами життя людей. Ще в 1855 році К.С. Аксаков писав у доповідній записці царю: *"Современное состояние России представляет внутренний разлад, прикрываемый бессовестной ложью... При потере взаимной искренности и доверенности все объяла ложь, везде обман. Правительство не может при всей своей неограниченности добиться правды и честности; без свободы общественного мнения это и невозможно. Все лгут друг другу, видят это, продолжают лгать, и неизвестно, до чего еще дойдут"* [121, с. 216].

Деякі дослідники пов'язують схильність до брехні з національно-психологічними особливостями певних етнічних груп. Ж. Дюпра вважав, що для деяких рас і країн брехня є неминучим явищем. Гасконці відомі своєю схильністю до вигадок, що спонукають їх брехати через хвальбу, що не має, втім, серйозного змісту; нормандців вважають дуже скритними і такими, що виявляють достатнє мистецтво в цьому; італійці відрізняються шахрайством; англійці – лицемірством; греки – нещирістю; турки – невірністю даному слову; азіати негідні довіри; нарешті більшість інших рас вважаються нездатними до правдивості [118, с. 91]. Подібна точка зору грішить надмірно різким узагальненням, проте не можна повністю заперечувати той факт, що виховання і національні традиції впливають на особливості міжособового спілкування. Узяти хоча б норму поведінки, прийняту рядом релігій, згідно з якою брехня одновірцям вважається злочином, а обдурити "неправедного" цілком допустимо.

Взагалі, питання про принципи дії груп і організацій, включаючи релігійні, політичні, фінансові, – таємні і відкриті, – об'єднані за найрізноманітнішими ознаками, потребує докладнішого розгляду з погляду впливу корпоративності на норми поведінки їх членів. Солідарність всередині припускає чесність і довірливість, зовнішні контакти, навпаки, передбачають обмеження інформації, допускають брехню для захисту інтересів конкретної структури.

У цілому в суспільстві існує безліч передумов, починаючи з функціонування сім'ї і закінчуючи соціальними структурами, вплив яких упродовж всього життя людини сприяє формуванню особистих якостей, що обумовлюються застосуванням брехні і маніпуляцій при вирішенні життєво важливих проблем.

Не випадково конкретні особливості індивіда, пов'язані з тенденціями до маніпулювання іншими людьми і застосуванням різноманітних форм брехні в буденному житті і ділових відносинах, одержали назву "макіавеллізм" – реабілітація будь-яких засобів для досягнення поставленої мети. Люди з такою вдачею вважають за краще об-

межувати інформацію, з легкістю спотворюють її, маніпулюють іншими людьми для досягнення власних цілей. Як це не парадоксально, самі такі особи не завжди можуть добре визначати брехню. Їх віра в те, що людьми можна управляти, допомагає "майстерно" брехати, не відчуваючи при цьому розкаянь і мук совісті.

Проблема виявлення нещирості, дезінформації і маніпуляцій в процесі спілкування є актуальною для різних сфер діяльності людини. Перш за все це пов'язано з необхідністю встановлення і підтримки контактів, у тому числі з такими категоріями людей, чию інформацію через наявність певних особливостей, життєвих обставин та інших причин не завжди можна вважати достовірною.

Для виявлення нещирості, дезінформації і маніпулятивних прийомів спілкування вдаються до різних способів контролю і перевірки одержуваної інформації: уточнення відомостей через не залежні один від одного джерела, застосування технічних засобів контролю, створення перевірочних ситуацій, вивчення реакцій об'єкта за допомогою поліграфа або, як його ще називають, "детектора брехні". Крім того, для виявлення нещирості необхідно приділяти увагу аналізу поведінки в ході безпосереднього спілкування. Це пов'язано з тим, що в багатьох ситуаціях способи перевірки одержуваної інформації утруднені або вимагають деякого часу. Аналіз поведінки партнера в ході безпосереднього спілкування дозволяє також внести корективи в тактику бесіди, відзначати, що викликає зовнішні реакції (або не викликає), і з'ясувати причини цього.

Стан навмисного приховування будь-чого спричиняє виникнення у свідомості людини суперечності між інформацією та реальністю. Такий стан кожна людина переживає по-різному. Він залежить від індивідуальних психічних якостей та ситуативної небезпеки через можливість бути обдуреним. Глибина переживань з приводу брехні також пов'язана з наявністю самовиправдувальної позиції, коли людина підводить певну базу під необхідність удатися до обману.

І все-таки обдурити не завжди легко. Наприклад, тому, що, окрім очей, на які традиційно звертають увагу, у людини є ще голос, міміка й інші "слабкі місця", які свідчать про її психічний стан та справжні інтереси. Аналізу в ході безпосереднього спілкування або після нього піддається зміст інформації та слів, техніка їх передачі іншій особі. Успішність виявлення приховуваних обставин, прийомів маніпуляцій багато в чому залежить від досвіду і підготовки людини, яка намагається це робити.

Для експертів, перед якими стоїть задача оцінити ступінь щирості тієї або іншої особи, представляють інтерес роботи зарубіжних і вітчизняних дослідників, у яких здійснюються спроби виділити значущі ознаки брехні за допомогою спостереження за партнером у ході спілкування. Дослідження психологів показують, що в хороших "лайкекспертів", – людей що ефективно визначають брехню, виражені соціальна активність, контактність, налаштованість на спілкування з іншими, діяльність серед різних соціальних груп, готовність до взаємодії. Ці люди прямо говорять, що хочуть, і чекають подібної поведінки від інших, а тому вельми чутливі до брехні.

Враховуючи складність оцінки і зіставлення вербальних та невербальних сигналів для визначення нещирості, важливо звертати увагу на суб'єктивний бік поведінки людини в різних ситуаціях. Просте заперечення, висловлене "ні" на поставлене запитання істотно відрізняється від мовчазного протесту, коли людину в чомусь обвинувачують, або від мовчання підсудного, що ставиться індиферентно до звинувачення, а також від мовчазного спокою людини, яка не допускає навіть можливості підозр щодо себе. Комплекс вербальних і невербальних відтінків поведінки людини в ході складних комунікативних ситуацій вимагає прояви професійної психологічної якості від людини, якій доводиться займатися оцінкою висловів і дій іншої людини на предмет їх істинності.

Багатоманітні і форми прояву брехні та нещирості. Вони починаються від більш прямолінійних і грубих форм та закінчуються створенням будь-яких уявлень, що не відповідають правді, за допомогою прикрашання, перебільшення або спрямованих на навіювання, приховування фактів, заперечень, умовчань, спотворень тощо.

Слід підкреслити умовність тих ознак, які виділяються як "індикатори брехні". Не існує засобів, що дозволяють розшифровувати "мову мозку" до такого ступеня, щоб прочитувати думки і точно дізнаватися, що людина думає. Тому при спостереженні висновки про можливість присутності брехні робляться на основі наявності більш-менш виражених психофізіологічних зрушень в організмі, які піддаються зовнішньому контролю, а також за допомогою аналізу змісту інформації та слів, що надходить від людини. Проте необхідність обережності при інтерпретації проявів супутньої брехні не означає того, що від подібного аналізу поведінки слід відмовлятися. Розуміючи непрямий вплив ознак, що виділяються, слід лише не поспішати з кінцевими висновками.

Про ознаки нещирості. Вивчення літератури за проблематикою дозволяє виділити наступні ознаки нещирості, зокрема хвилювання, що виявляється в голосі і мові при передачі помилкової інформації:

- мимовільна зміна інтонації;
- зміна темпу мови;
- зміна тембру голосу;
- поява тремтіння в голосі;
- поява пауз при відповідях на запитання, які не повинні викликати утруднення;
- дуже швидкі відповіді на запитання, які повинні примусити задуматися;
- поява в мові виразів, нетипових для даної людини в звичному спілкуванні, або зникнення типових для нього слів і оборотів;
- демонстративне підкреслення (виділення) за допомогою мовних засобів — інтонацією, паузами тощо, яких-небудь фрагментів інформації, маскуючи або спотворюючи істинне ставлення до неї [104].

Остання ознака відноситься до групи прийомів, що свідомо застосовуються тим, хто бреше, для дезорієнтації іншої людини і може служити як індикатор брехні при зіставленні з іншими даними. У буденній практиці, коли вдається переконатися, що це саме прийом, про такі випадки говорять, що людина "перегнала", намагаючись будь-що "впарити" іншим.

На відміну від голосу людині краще вдається контролювати своє обличчя. Орієнтуватися тільки на обличчя не варто, оскільки особа має дуже багато параметрів, що вимагають аналізу при індикації брехні. Різноманітна міміка, рухи очей, напрям погляду, зміна рис обличчя людини в ході спілкування, а головне — неоднозначність проявів різних станів людини "зовні" часто призводять до неправильних висновків про ступінь щирості людини.

Таким чином, шляхом самоконтролю і управління зовнішніми проявами психічних реакцій, емоцій, відчуттів за допомогою міміки, погляду й інших "параметрів" особи можна достатньо успішно вводити в оману іншу людину. З другого боку, визначити брехню вдається у багатьох випадках саме завдяки аналізу виразу обличчя.

Орієнтуючись на обличчя партнера по спілкуванню для індикації брехні, частіше увага спостерігача звертається на наступні параметри:

- "бігаючий" погляд. Це ознака, яка традиційно відзначається, пов'язана з тим, що людина, не звикла до брехні або така, що хвилюється з інших причин в ході помилкової заяви, насилу "тримає погляд" партнера по спілкуванню і відводить очі убік;
- легка усмішка. Вона часто супроводжує помилковий вислів, хоча може бути лише формою прояву індивідуального стилю спілкування. Усмішка, що супроводжує

брехню, дозволяє приховувати внутрішню напругу, проте не завжди виглядає достатньо природною;

• мікронапруга лицьових м'язів. У момент помилкового повідомлення по обличчю немов "пробігає" тінь. Відеозйомка дозволяє зафіксувати при цьому короткочасну напругу у виразі обличчя, що триває менше секунди;

• контроль партнера у момент помилкового вислову. Повідомляючи брехню, деякі учасники на короткий час концентрували свою увагу на обличчі партнера, нібито намагаючись оцінити, наскільки успішно їм вдалося ввести його в оману;

• рух зіниць очей. Згідно з даними фахівців з нейролінгвістичного програмування (НЛП), є певні зони (дві з дев'яти), в які мимоволі потрапляє зіниця ока при так званому конструюванні інформації, що в ряді випадків є різновидом нещирості, оскільки йдеться про свідоме спотворення при виконанні завдань, відповідях на запитання і т. д. Частіше "спрацьовувало" не стільки спостереження за зоною конструювання, скільки аналіз розбіжностей рухів зіниці ока за змістом інформації. Наприклад, коли обговорення торкалося яких-небудь образів, зіниця знаходилася не у візуальній, а в аудіальній зоні. Подальше обговорення підтверджувало, що той учасник, у якого це фіксувалося, дійсно не прагнув представити образ, а був зайнятий іншими думками [124, с. 18];

• вегетативні реакції. Почервоніння обличчя або його окремих частин, тремтіння губ, розширення зіниць очей, прискорене моргання та інші зміни, притаманні для відчуття сорому, страху й інших емоцій, що супроводжують нещирість на підсвідомому рівні у людей, які не звикли брехати і почуваються незручно.

При аналізі міміки й інших параметрів, пов'язаних з реакціями людини на предмет виявлення можливості присутності нещирості, важливо застосовувати індивідуальний підхід до визначення так званого "фонового" стану людини. Відомо, що при процедурі дослідження на поліграфі оператор заздалегідь заміряє загальний фон нормальної реакції випробовуваного, ставлячи йому запитання нейтрального змісту. Окрім них ставляться також контрольні запитання, що викликають стан тривоги, і, нарешті, значущі запитання, що безпосередньо стосуються дослідження. Саме зіставлення результатів відповідей на різні типи запитань дає можливість зробити певні висновки. Щось подібне може відбуватися і при безпосередньому спілкуванні. Свідомо або підсвідомо партнери відзначають індивідуальні особливості природної поведінки один одного і роблять для себе висновки про конкретні особливості і стан іншого, відзначаючи відхилення від звичного стилю спілкування. Таким чином, практично будь-яка реакція партнера у спілкуванні може інтерпретуватися по-різному залежно від того, чи є вона природним проявом індивідуального стилю спілкування і можлива для даної людини в даній ситуації або ж ця реакція викликана іншими причинами, зокрема, бажанням приховати істинне ставлення до обговорюваного питання.

Проблема фіксації природності поведінки, зіставлення її з іншими елементами спостереження виникає і при аналізі жестикуляції та поз людини. Дослідження напряму, що одержав за кордоном назву "Мова тіла", підкреслюють, що інтерпретація жестів, міміки, поз та інших невербальних компонентів спілкування повинні здійснюватися в контексті аналізу всієї ситуації. Саме на невідповідності змісту вислову зовнішнім проявам ставлення до даного вислову часто будується припущенням про присутність нещирості. Так, заява типу "мені це дуже цікаво" в поєднанні з "відсутнім", не сфокусованим на партнері поглядом, перехрещеними руками і ногами або іронічною усмішкою дозволяє думати про можливість присутності нещирості.

Фахівці виділяють ряд жестів, які можуть супроводжувати брехню, обман, сумнів і шахрайство. До них відноситься такі:

• рука до обличчя – спостерігалося, що медсестри, які брешуть пацієнтам про стан здоров'я, частіше підносили руку до обличчя, ніж сестри, які говорили правду;

• прикриття рота – прикриття рота долонею, пальцями або кулаком, а також покашлювання з прикриттям рота. У разі якщо подібний жест пов'язаний із зазначеними позиціями, зімкнута долоня лежить на щоці, а вказівний палець часто показує вгору;

• дотик до носа – легке потирання носа або швидкий дотик до нього, які на відміну від дійсного чухання носа виглядають не так явно;

• потирання ока – при великій брехні чоловіки схильні відводити очі й потирають їх, а жінки – легко торкатися ока і потирати під ним. Цей жест може поєднуватися із щіпленими зубами і фальшивою усмішкою;

• відтягування коміра – пов'язується з роздратуванням у чутливих тканинах обличчя і шиї, що виникає під час неправдивої заяви через виділення поту [125, с. 68-74].

Проте, напряму пов'язувати жести або пози з нещирістю дуже ризиковано, так як національні культури відрізняються. Інша справа – намагатися співставляти їх з рештою спостережуваних параметрів і змістом інформації.

Що стосується аналізу змісту інформації на предмет виявлення "симптомів брехні", то в роботі [126, с. 128-130] визначаються деякі з їх основних ознак:

• суперечність висловів іншій інформації, зібраній з даного питання, а також суперечність усередині самої інформації. Брехню важко продумати у всіх деталях, тому брехун прагне запам'ятати те, що вважає найважливішим серед осмислених ним обставин. Ряд обставин в процесі підготовки до брехні взагалі ним не осмислюється.

Часто брехня має ланцюговий зміст – одна брехня породжує іншу, одна спотворена обставина змушує вносити корективи і в інші. Все це вимагає серйозних зусиль і часу, що часто не дозволяє брехуну продумати і все це запам'ятати. Основний прийом виявлення – уточнюючі питання з упором на деталізацію фактів;

• невизначеність, неконкретність відомостей. Причина – виклад того, що не було пережито і тому лише поверхнево закріпилося в пам'яті або швидко було ним забуто (хоча і обдумувалося при підготовці брехні). Відсутність реальної діяльності, яка б включала так чи інакше описувані події і факти, робить виклад брехні позбавленим активного компоненту (у тому числі й на граматичному рівні);

• надмірна, нарочита точність опису подій (особливо віддалених за часом) – наслідок заучування наперед підготовленої помилкової інформації;

• збіг у найдрібніших деталях повідомлень декількох опитуваних. Звичайно декілька чоловік, які спостерігали одну і ту ж подію, не дають їй однакових описів. Це має декілька причин: індивідуально-психологічні відмінності, відмінності в психічному стані у момент розгортання подій, відмінності в мірі активного включення в події, що відбуваються, відмінності в точках спостереження за подіями, селективність уваги і сприйняття. Як наслідок цього – увагу кожного з учасників більш-менш однаково привертають найяскравіші і найбільші ознаки, деталі ж ними сприймаються максимально індивідуально, що впливає на зміст інформації;

• відсутність в описі неістотних подробиць і деталей. Вигадане минуле пасивне, штучне, не пережите суб'єктом. Єдина мета конструювання такого "минулого" – введення в оману, що і призводить до однобічного опису і селекції деталей. Зникають неістотні "добавки", типові для даної людини при реальному переживанні схожих подій.

• різне пояснення одних і тих же подій на різних етапах спілкування. Часто трансформація пояснень викликана тим, що людина забуває деталі своїх минулих вигаданих пояснень, і це змушує її давати нові тлумачення подіям;

• виключно позитивна інформація про самого себе і відсутність щонайменших сумнівів у трактуванні подій (не обумовлена відповідними конкретними особливостями). Правдивість людини не змушує її зупинятися і перед викладом того, що може його невигідно характеризувати (можливе часткове маскування "негативу"). Правдиві люди звичайно не приховують і виникаючі у них сумніви в поясненні деяких фактів, що не властиво брехуну;

• настирне, неодноразове (нав'язливе) повторення будь-яких тверджень (не обумовлене нейтральними причинами). Східне прислів'я – ти сказав мені вперше, і я повірив. Ти повторив – і я засумнівався. Ти сказав утретє – і я зрозумів, що ти брешеш;

• "проговори" (обмовки) в ході спілкування, тобто мимовільне повідомлення достовірної інформації як наслідок конфліктного суперництва в свідомості людини правдивих і помилкових варіантів пояснення або опису події;

• нетипові для даної людини (з урахуванням рівня інтелекту й освіти) терміни і фразеологізми – результат заучування інформації (можливо, підготовленої іншим);

• слабкість емоційного фону висловів – як наслідок відсутності реальних емоцій у момент розгортання "реальної" події. Правильніше говорити про неадекватність емоційного фону особистому ставленню до події, оскільки, окрім схемної безликості і емоційної блідості, може, хоча і рідше, зустрічатися утрирувана і нарочита емоційність;

• недоречні, неодноразові посилання на свою доброчесність і незацікавленість. Зайве афішування подібних чеснот викликає сумнів у правдивості інформації;

• ухилення від відповіді на пряме запитання, спроби створити враження, що це запитання незрозуміле або "забуте";

• приховування того, що не може бути не відоме, або забудькуватість щодо особливо значущих подій.

Наявність у людини схильності до маніпулювання іншими за допомогою брехні формується за відповідних передумов виховання і розвитку упродовж довгого часу. Тому і прийоми, якими користуються люди подібного складу, дуже індивідуальні. Можливі випадки, коли людина випереджає події. Знаючи, що його можуть запідозрити в нещирості, він починає розповідати свою версію того, що відбулося, щоб сформувати у партнера психологічну установку на подальше сприйняття невигідної для себе інформації. Діагностичним елементом виявлення цього прийому служить аналіз доцільності розповіді на тему, достовірність викладу якої може братися під сумнів.

Психологи з'ясували деякі можливі типові прийоми, до яких вдаються особи для введення в оману партнера у спілкуванні:

• розказували про події, які добре знали, але які відбулися з іншими людьми;

• передавали реальні події, але переносили їх в іншу обстановку або змінювали в часі;

• відомості розбивали на окремі блоки, які передавали стислими фразами;

• використовували очевидну інформацію для брехні, яку легко перевірити ще раз, чекаючи, що саме тому в достовірності не засумніваються;

• деталізували помилкову інформацію, щоб представити її реальнішою;

• помилкову інформацію по змісту і логіці пов'язували з достовірною;

• прагнули поводитися спокійно, не стежили уважно за поведінкою співбесідника, не відводили погляд при уточнюючих запитаннях, прагнули говорити рівним голосом, швидко і упевнено відповідати на додаткові запитання.

Проблема виявлення нещирості є надзвичайно складною через числені чинники, які підлягають аналізу. Досвідчена людина може визначити брехню, але затрудниться відповісти, якщо запитати, як вона це зробила. Спроба систематизації ознак, що свідчать про можливість присутності нещирості, дозволяє більш цілеспрямовано підійти до

розвитку комунікативної компетентності людей, які займаються політикою, підприємницькою діяльністю, працюють у системі державного управління.

Враховуючи сказане вище про неприхований зміст багатьох з наведених ознак, необхідно при виявленні нещирості й маніпулятивних прийомів підходити до оцінки одержуваної інформації з урахуванням:

• повторної перевірки відомостей. Звернувши увагу на ту або іншу обставину, що свідчить про можливість нещирості, не слід відразу робити однозначні висновки, треба постаратися перевірити інформацію, в достовірності якої засумнівалися;

• комплексності в оцінці спостережуваних параметрів. Збільшити точність в оцінці поведінки партнера у спілкуванні можна, якщо орієнтуватися не тільки, скажімо, на зміст його інформації, а й на все, що можна контролювати в даній ситуації;

• контексту ситуації. Обстановка, в якій відбувається спілкування, зміст обговорюваних питань та інші обставини вимагають внесення відповідних корективів до оцінки поведінки партнера у спілкуванні;

• особистих чинників, і перш за все ступеня вираженості "макіавеллізму". Брехня з вираженими маніпулятивними здібностями важче піддається розшифровці, ніж брехня людини, не звиклої до маніпулювання іншими за допомогою спотворення інформації.

1.3.3. Види маніпулювання

У сучасних умовах основними видами маніпулювання свідомістю людини є пропаганда, агітація, реклама та так званий "зв'язок з громадськістю" (від англ. "паблік рілейшнз"), які у більшості випадків здійснюються за допомогою ЗМІ.

Пропаганда. Це поняття (від лат. "предмет поширення") передбачає діяльність (усну або за допомогою засобів масової інформації) з поширення, популяризації ідей в громадській свідомості. Під політичною пропагандою розуміється систематично здійснювані зусилля вплинути на свідомість індивідів, груп, суспільства для досягнення визначеного, наперед наміченого результату в політичній діяльності [114, с. 320].

Цей вид масової комунікації є основним засобом дії на свідомість. На відміну від реклами, пропаганда не обмежена жорсткими тимчасовими рамками і її не просто виявити. Більшість людей піддаються їй щодня, але не завжди ми це помічаємо.

Пропаганда, як правило, не здійснюється на користь лише однієї людини. Вона відображає світогляд правлячої в суспільстві влади, партії тощо. Мета маніпулятивної, негативної пропаганди – перетворити аудиторію на слухняний, керований натовп.

Саме слово "пропаганда" несе в собі негативний відтінок. Потужність цієї інформаційної зброї була дійсно велика. Так Гітлер у "Майн кампф" писав: *"С помощью умелого и длительного применения пропаганды... можно представить народу даже небо адом и, напротив, самую убогую жизнь представить как рай"* [127, с. 233].

У демократичному суспільстві все відбувається трохи по-іншому. В. Амелін зазначає: *"И пропаганда, и манипулирование допускают наличие массовой аудитории, крепко ориентированной на определенные стереотипы. Пропаганда, как и манипулирование, неэффективная в аудитории, настроенной критически, или когда они охватывают одну часть аудитории, а другая остается вне их влияния"* [128, с. 62].

Звичайно, політична свідомість не є чимось застиглим. Подолати критичний настрій аудиторії можливо. В цьому випадку створення нових стереотипів, штампів є відмінною рисою агресивної, наступальної пропаганди.

Пропаганду не можна порівнювати з рекламою, оскільки *"пропаганда стремится вызывать более быстрое коллективное, чем только индивидуальное действие. В этом*

значении ее следует отличать от рекламы, поскольку реклама стремится влиять на индивидуальное действие. В пропаганде, напротив, в наличии попытка создать какое-то убеждение и добиться действия в соответствии с этим убеждением... Ясно, что пропаганда, владея таким содержанием, действует для того, чтобы положить конец дискуссии и рассуждению... При пропаганде цель доминирует, а средства подчинены этой цели" [129, с. 562].

Відомі *три основні способи*, за допомогою яких пропаганда досягає своїх цілей:

- підтасовування фактів і надання помилкової інформації;
- застосування внутрішньогрупових і позагрупових установок. Це дозволяє втілити, наприклад, технологію створення "образу ворога";
- застосування емоційних установок і стереотипів, якими люди вже володіють, шляхом вибудовування асоціацій між цими установками і задачею пропагандиста.

Типи пропаганди. У певному значенні пропаганда приречена на існування в сучасному суспільстві. Вона перш за все впливає на емоції людей, які бувають різні. Є емоції негативні, руйнівні, а є емоції позитивні, творчі. Ісус Христос був пропагандистом. Він переконував людей любити один одного, а не ненавидіти, творити, а не руйнувати. Чи завдавав він такою пропагандою шкоди оточуючим, своїм послідовникам? Мабуть, ні, швидше, навпаки. Тому коли йдеться про шкоду або користь пропаганди, то потрібно насамперед розібратися, які емоції викликає ця пропаганда. В основі нашої поведінки лежать певні переконання. Тому якщо люди засвоюють руйнівні переконання, то і дії, що робляться ними, будуть відповідними. Якщо не розпізнати істинних цілей пропагандиста спочатку, то потім може бути вже пізно. Отже, сама природа пропаганди така, що вона досягає своїх цілей, впливаючи перш за все на емоції людей. Але дуже важливо, на які саме емоції вона впливає.

Тут криється відмінність між позитивною і негативною пропагандою. Що ж до методів переконання, якими хвалилися ідеологи соціалістичної пропаганди, то вони теж мають місце як один з технічних прийомів пропагандистської дії, але не більше того. Врешті-решт, за допомогою раціональних аргументів можна заморочити людям голову не гірше, ніж за допомогою софістики. Позитивна пропаганда не допускає брехню і приховування фактів. У цьому її відмінність від негативної.

І, нарешті, найголовніше: у чиїх інтересах здійснюється пропагандистська дія, які цілі воно переслідує? Це питання, по суті справи, ключове. Всі суперечки навколо пропаганди і того, чиї ж інтереси вона виражає, підводять нас до проблеми співвідношення приватного (корпоративного) інтересу й інтересів суспільства. Коли ці інтереси збігаються, то ситуацію можна вважати ідеально позитивною.

Коли вектори інтересів направлені в протилежні боки, то, природно, пропаганда несе шкоду суспільству. Більше того, нерідко пропагандист вимушений йти на свідомий обман, щоб приховати реальні наслідки тих дій, до яких він закликає людей.

Проте на практиці вектори приватного і загального інтересу найчастіше знаходяться один до одного під якимсь "кутом". Описані вище крайнощі зустрічаються рідше. Чим більший цей "кут", тим ширше застосовуються маніпулятивні методи переконання, тим вірогідніша небезпека бути обдуреним. Звичайно, "зміряти" його на практиці досить проблематично. Мало того, його ще треба знайти. Але якщо маніпуляцію вдалося розкрити, то вона вже значною мірою втрачає свою силу. Маніпуляції припускають приховану дію. Вони, як вампіри, не терплять світла. Тому ледве не єдиний спосіб боротися з негативною пропагандою і маніпулятивними методами – це виявляти їх і виставляти на світло Боже.

Методи пропаганди. Прийомами пропаганди можна назвати: передування думок, що несуть оцінку, перед викладом, замовчування або спотворення фактів, упереджена інтерпретація фактів і т. д.

Серед основних способів дії на аудиторію виділяють твердження і повторення. Згадуючи радянське минуле, можемо навести масу прикладів однозначних, таких, що не підлягаючих обговоренню, тверджень, які упроваджувалися в масову свідомість: радянське суспільство – найсправедливіше, СРСР – оплот миру, марксизм – єдине вірне вчення і т. д.

Може виникнути питання – чому в 1970-ті рр. мало хто реагував на гасла? Як наголошується в [130], річ у тому, що задача пропаганди – перевести слова в дії, оскільки пропаганда виступає інструментом здійснення політичної волі будь-якої особи або групи осіб. У 1970-ті рр. радянська пропаганда вже не ставила перед собою таких задач. Якщо в 1930-ті рр. пропаганда закликала боротися з шкідниками та зрадниками і люди доносили один на одного, в 1960-ті рр. закликали освоювати цілину і люди їхали та за копійки працювали, то в 1970-ті рр. заклики і гасла партії перетворилися з керівництва у свого роду вивіски, за якими нічого не стояло. Пропаганда 1970-х рр. служила заспокоєнню самих можновладців, але втратила свій вплив на населення країни, оскільки перестала спонукати до дій.

Агітація (від лат. – "приведення до руху") – інформаційна діяльність з метою спонукання до політичної активності окремих осіб, груп або широких мас населення.

Відрізняється різноманітністю усних, друкованих і аудіовізуальних засобів і є поширеним інструментом політичної боротьби [114, с. 18].

Реклама. Технології, вживані в політичній і комерційній рекламі, на думку багатьох дослідників, практично ідентичні. Проте, політичну рекламу визначають дві принципові відмінності. Перше: час її обмежений. Друге: на виборах головна мета – перемога над конкурентами. Навіть відставання на один голос зведе нанівець всі зусилля рекламістів. Проте виборча кампанія не зводиться лише до однієї реклами. Вона включає агітаційні та пропагандистські заходи, особисті зустрічі кандидата з виборцями, заходи у зв'язках з громадськістю і т. д.

Під рекламою розуміють будь-яку дію, пов'язану із спробою продати щось, представити публіці той або інший товар. На Заході поняття "реклама" ("advertising") має чіткі рамки: *"реклама – любая платная форма представления и продвижения идей, товаров или услуг от имени известного спонсора"* [131, с. 482].

Такий підхід продиктований багато в чому чисто прагматичними міркуваннями, оскільки дозволяє уникати всіляких юридичних неув'язок.

Маніпуляції в політичній рекламі. Основний спосіб дії на виборців, що застосовується в політичній рекламі, – це експлуатація чинних в суспільстві стереотипів шляхом їх посилення, зіставлення, ослаблення і т. д.

Інший маніпулятивний прийом – вибудовування сприятливих для кандидата асоціацій. Часто в рекламному фільмі використовують добре відомі імена, що є гордістю нації, і в кінці вводять кандидата, майбутнього "слугу народу".

Як правило, політична реклама приречена бути маніпулятивною. Вона служить драматизації виборчого процесу, яка досягається роздуванням достоїнств одного кандидата і зменшенням таких у конкурентів. Один із способів зменшення цих перебільшень полягає в тому, щоб надавати кандидатам рівні можливості для ведення рекламної кампанії. У цьому значенні двопартійна система, що склалася в США і Великобританії, працює дуже продуктивно.

Реклама в системі комерційного маркетингу. Ф. Котлер визначає маркетинг як "вид человеческой деятельности, направленный на удовлетворение потребностей людей с помощью обмена" [131, с. 47]. Мета маркетингових зусиль – так добре пізнати і зрозуміти клієнта, щоб товар або послуга точно йому підходили.

Зусилля із збуту і його стимулюванню стають частиною "комплексного маркетингу", тобто набору маркетингових засобів, які необхідно гармонійно поєднати один з одним, щоб добитися максимального ефекту на ринку. Серед таких засобів важливу роль відіграє реклама.

Що є комплексним маркетингом? Це "набір змінних чинників маркетингу, що піддаються контролю, сукупність яких фірма використовує в прагненні викликати бажану у відповідь реакцію з боку цільового ринку" [131, с. 95]. У комплекс маркетингу входить все, що фірма може зробити для виникнення попиту на свій товар. Основними складовими комплексу маркетингу є: товар, ціна, методи розповсюдження товару і методи стимулювання попиту на нього. Діючи в обстановці кінцевої невизначеності, рекламіст повинен мати в своєму розпорядженні по можливості повне уявлення про споживача, структуру ринку, самий товар. Вивчення споживачів (збір персональних даних) допомагає виявити групи найвірогіднішних покупців, з'ясувати, як саме споживачі сприймають рекламований товар, зрозуміти, на який результат вони розраховують, ухвалюючи рішення про покупку. Тому планування реклами повинен передувати етап збору маркетингової інформації про стан ринку, позиції конкурентів, виявлення сильних і слабких сторін товару, що виводиться на ринок.

Після проведення роботи з позиціонування товару, за сегментацією ринку і визначення цільової аудиторії ухвалюється рішення про вибір рекламної стратегії, формулюється основна ідея рекламного обігу, вибираються носії реклами, формується бюджет рекламної кампанії, складається графік проходження реклами в засобах масової інформації. Таким чином, реклама, завершує зусилля маркетологів, доводячи до споживачів у доступній і привабливій формі ті переваги даного товару, які, як вважає продавець, задовольнять потреби покупців.

Політична реклама в системі політичного маркетингу. Політична реклама є складовою частиною політичного маркетингу. Їх ефективність, так само, як і у випадку з комерційною рекламою, залежить від того, наскільки точно вдалося визначити очікування виборців, як сформульована центральна ідея кампанії, чи вдало вона спланована і т. д. Проте, оскільки "специфікою маркетингового підходу є націленість не просто на вивчення ринку, але й на управління ним" [132, с. 88], то небезпека застосування маркетингових засобів в маніпулятивних цілях достатньо велика.

Якщо в комерційному маркетингу дослідники ринку намагаються визначити мотиви покупки, то в політичному маркетингу досліджуються мотиви голосування виборців. Існує декілька гіпотез, що пояснюють мотиви голосування виборців:

- "соціологічна": голосуючи, люди виявляють солідарність зі своєю соціальною групою (класовою, етнічною, релігійною, сусідською і т. д.);
- "соціопсихологічна": голосуючи, люди керуються укоріненими (наприклад, у сім'ї) політичними симпатіями, психологічним тяжінням до певної партії, лідера і т. д.;
- "политико-комунікаційна": люди голосують під впливом власне виборчої кампанії, зокрема, під впливом формованого ЗМІ, політичною рекламою іміджу політика, партії;
- "раціонального вибору": люди голосують (або не голосують) не як члени групи, а як індивіди, керуючись при цьому власним інтересом, розрахунком, вигодою [132, с. 124].

Суперечності між цими гіпотезами нема, оскільки вони пояснюють мотиви поведінки різних груп виборців. Виборці, що визначаються напередодні голосування, складаються з груп. Всі вони виправдовують комунікативну гіпотезу і є основною мішенню політичної реклами. Політична реклама апелює перш за все до "масової людини", людини, що позбавлена традиційного коріння і не має чітко усвідомлених політичних уподобань.

Рішення голосувати може ухвалюватися як на основі раціонального аргументування, так і під впливом емоційних чинників. У політичній рекламі раціональне аргументування "упаковується" в емоційну "обгортку". Оскільки в основі мотивів лежать певні незадоволені потреби, реклама має переконати виборця, що пропонований кандидат зможе розв'язати його проблеми. Це – головна задача рекламістів, і саме на цьому полі виростають ті самі маніпуляції, в яких обвинувачують творців реклами: від відвертого обману виборців до невиправданого перебільшення достоїнств кандидата і замовчування його недоліків.

Політично рекламна кампанія дещо нагадує бойові дії. Коли йдеться про вибори державного рівня, вона повинна, в ідеалі, охопити всю країну. Раціонально розподілити ресурси, бюджет кампанії – одна з основних задач рекламістів.

Методи політичної реклами і способи маніпулювання виборцями. Серед основних методів потрібно назвати: поштову розсилку, телевізійні ролики, радіоролики, наочну агітацію (плакати, розтяжки, щити тощо), сувенірну продукцію (значки, вимпели, бейсболки, прапори, футболки тощо), концерти та інші розважальні заходи.

Поштова розсилка. Дуже ефективна для створення ілюзії спілкування з кандидатом персонально. Політик демонструє увагу до конкретного виборця, указуючи в листі ім'я і по батькові одержувача. Підпис кандидата свідчить про те, що він особисто звертається до потенційного виборця. Технологи рекомендують, коли це можливо, ставити підпис, а не факсиміле. Підпис свідчить про інтерес політика до адресата. Звичайно, при масовій розсилці доводиться відмовлятися від "живих" підписів. Цей недолік компенсується кількістю листів.

Телевізійні ролики.. Це престижний вид реклами, який має широке поширення. Вважається при цьому, що телебачення – наймогутніший канал дії на виборця.

Політична телереклама – досить складний жанр. За рівнем досягнень в цій області вона значно відстає від комерційної реклами. Ефективність телереклами залежить не тільки від якості, але й від таких чинників, як частота показу, час показу, інтервали між показами, цикли показів, контекст показу (до фільму або програми, під час фільму або програми, після фільму або програми), популярність каналу, загальна спрямованість каналу (адресність реклами) і т. д.

Наочна агітація. В основному це плакати. Їх можна розділити на два види:

- із зображенням політика. На цих плакатах виборець бачить обличчя кандидата, яке повинне викликати довіру. Має значення ракурс зйомки, якість друку. Якщо плакат надрукований погано, зображення нечітке – позитивні емоції він може не викликати;
- без зображення політика. Як правило, такі плакати містять слогани кампанії. Головна увага надається тому, щоб: а) привернути увагу виборця; б) зафіксувати увагу, спонукати ознайомитися з плакатом; в) закласти в свідомість виборця ідею плаката.

Сувенірна продукція. Вона використовується для популяризації логотипів партії, зображень кандидата і основних гасел кампанії. Тут політична реклама пішла шляхом комерційної. Головна мета реклами – за допомогою розповсюдження сувенірної продукції забезпечити занам'ятання кандидата або партії, пов'язати у свідомості виборця рекламований образ з певними знаками і символами. Якщо виборець приймає символіку кандидата, він уже стає так би мовити, частиною його команди. Це свого роду мітки, нав'язувані виборцям. Якщо продукція привертає увагу, викликає емоційний відгук у виборців, значить, мета досягнута.

"Зв'язок з громадськістю". Вище наголошувалося, що термін "паблік рілейшнс" означає "зв'язки з громадськістю". Як зазначається в [133, с. 13] – "цель "паблик рилейшн" – установление двустороннего общения для выявления общих представлений или общих интересов и достижения взаимопонимания, основанного на правде, знании и полной информированности". ПР-менеджери повинні прокладати мости взаєморозуміння між певним суб'єктом і його аудиторією чи між двома або більше суб'єктами.

На Заході (як у діловому світі, так і в політиці) величезне значення надається підтримці хорошої репутації в суспільстві. ПР і тут приходить на допомогу.

Напрями застосування ПР наступні [133, с. 14-15]:

- консультування на основі законів поведінки людини;
- виявлення можливих тенденцій і прогноз їх наслідків;
- вивчення громадської думки, ставлення щодо вжиття необхідних заходів для задоволення очікувань громадськості;
- підтримка спілкування, заснованого на правді і повній інформованості;
- запобігання конфліктам і непорозумінню;
- гармонізація особистих і суспільних інтересів;
- сприяння доброзичливим відносинам;
- поліпшення виробничих відносин;
- реклама товарів і послуг;
- створення власного іміджу.

Чесність, відвертість, повна інформованість, встановлення гармонійних відносин – всі ці поняття лежать в основі діяльності ПР-менеджерів.

Виділяють наступні функції ПР:

- аналітико-прогностична (аналіз, прогнозування тенденцій);
- організаційно-управлінська (відпрацювання цільових заходів);
- комунікативно-інформаційна (щодо забезпечення інформацією);
- консультантивно-методична (виступає як радник керівника) [134, с. 92].

Найважливішою задачею ПР-команди є уміння адекватно реагувати на непередбачені ситуації, різкі випади конкурентів і т. д.

Більш того, зусиллями менеджерів з ПР створюється імідж політика, який транслюється на мільйонну аудиторію, тобто "создаваемый образ должен подменить реального человека при выполнении им властных функций, связанных с публичностью власти. В результате оказывается как бы два президента, поскольку реальный тоже никуда не исчезает окончательно" [135, с. 123].

Сьогодні великою популярністю у психологів і виборчих технологів користується техніка нейролінгвістичного програмування (НЛП). Подібне багато в чому іншим технологіям, НЛП може застосовуватися як для розпізнавання маніпуляцій, так і безпосередньо для маніпулювання. Один з лідерів цього напряму Р. Бендлер вважає, що *"большинство людей не пользуется собственным мозгом активно и продуманно"* [136, с. 11]. Можна стверджувати, що якщо людина не користується своїм мозком, то завжди знайдеться інша людина, яка це зробить за місто неї в своїх інтересах. Тобто наша "розумова безгосподарність" відкриває для маніпуляторів якнайширші можливості.

У НЛП розрізняють три види репрезентативних систем: візуальну, аудіальну і естетичну. Одна з цих систем у людей, як правило, буває переважаючою: одні люди краще бачать картину уявної мети, інші – чують, а треті – відчувають. За предикативними словами і зовнішніми ознаками можна визначити провідну репрезентативну систему людини. Якщо ви хочете її в чомусь переконати, то творці НЛП рекомендують копіювати поведінку співбесідника, розмовляти з ним на його "мові". Основне значення копіювання, підстроювання під співбесідника полягає в тому, щоб у певний момент непомітно перехопити ініціативу і тоді партнер, сам того не помічаючи, починає слідувати за вами. В результаті подібної витонченої маніпуляції людина потрапляє в підлегле положення, деколи сама того не відаючи.

Подібне "перехоплення ініціативи" намагаються здійснювати і політики. Оратор спочатку входить в контакт з аудиторією, зливається з нею, а вже потім починає заволодівати нею і направляти спілкування в потрібне йому русло.

У принципі "перехоплення ініціативи" не є новим відкриттям. Ним часто користувалися інтуїтивно вожді, оратори, полководці у всі часи. Але технології, подібні НЛП, дозволяють свідомо оволодіти цією технікою людям, які не володіють від природи необхідною для цього інтуїцією і т. д. Іншими словами, маніпулятивні прийоми стають доступні практично будь-якій людині, що відчуває необхідність в їх застосуванні. Відсутність таланту підміняється чітко відпрацьованими алгоритмами дій.

Маніпулювання свідомістю за допомогою засобів масової інформації. ЗМІ мають значні можливості щодо маніпулювання свідомістю та вчинками людини. Маніпуляційний арсенал ЗМІ передбачає: навмисне спотворення реального стану справ шляхом замовчування одних фактів і "випинання" інших, публікації помилкових повідомлень, пробудження в аудиторії відповідних емоцій за допомогою словесних образів або візуальних засобів (зокрема, жестів) впливу на свідомість. Всі ці прийоми спрямовані на створення певного емоційного настрою і психологічних установок.

Матеріалом у маніпуляціях є інформація, з якою можна виконати наступне:

- сфабрикувати, видаючи її за справжню;
- спотворити шляхом неповної, односторонньої її подачі;
- відредагувати, додавши різні домисли;
- інтерпретувати факти у вигідному для маніпулятора світлі;
- втаїти важливу інформацію, будь-які істотні деталі;
- проявляти вибіркову увагу до фактів відповідно до своєї позиції;
- супроводжувати матеріал заголовком, що не відповідає змісту;
- приписати будь-кому заяви, яких він ніколи не робив;
- опублікувати правдиву інформацію, коли вона втратила свою актуальність;
- неточно цитувати, коли приводиться частина фрази або виступу, яка у відриві від контексту набуває іншого, часом протилежного значення.

Всі ці маніпуляції сконюють з урахуванням конкретних цілей і задач, що стоять перед маніпуляторами. Повідомлення є лише будівельним матеріалом, зовнішньою оболонкою, упаковкою, в яку поміщається істинне "послання" маніпулятора. Адже маніпулятор прагне демонструвати приховану дію і завжди радий використовувати будь-які слушні підстави у своїх корисливих цілях. На жаль, журналіст не може бути абсолютно неупередженим. Існує два основні підходи до ролі журналістики в суспільстві.

Прихильники ліберального підходу вважають, що все, що відбувається цікавого і важливого для аудиторії ЗМІ, повинно бути відображено в новинах.

Інша журналістика має на увазі застосування ЗМІ для підтримки основ суспільства і виховання людей з метою удосконалення їх як соціальних суб'єктів. Такий підхід притаманний для суспільств, де ЗМІ монополізовано державою. Критики цього підходу вважають, що журналісти не можуть виступати арбітрами, які визначають соціальні цінності в суспільстві, в якому існують різні точки зору.

Прийоми маніпуляцій у ЗМІ.

Телебачення. Сьогодні воно є наймогутнішим технічним засобом маніпуляцій у країнах світу. Причому те, як виглядає політик по телебаченню, багато в чому залежить

від ставлення до нього журналістів, що готують матеріал. Перерахуємо ряд чинників, які дозволяють журналістам маніпулювати політиком або його висловами.

Ситуація, в якій береться інтерв'ю. Вони бувають стандартні (в студії, удома, в кабінеті), випадкові (журналісту вдається зловити політика, психологічно не налаштованого спілкуватися) і екстрені (катастрофи, захоплення заручників).

Зміст передачі.

А. Прямий ефір. У прямому ефірі політик гарантований від того, що його вислови можуть бути спотворені, але в той же час він повинен проявити себе умілим полеміст ом і не дозволити журналісту загнати себе в кут на очах у телеглядачів. Запитання телеглядачів можуть бути досить несподіваними, і політик повинен продемонструвати хорошу реакцію.

Б. Передача в записі. Якщо передача дається без купюр, то для політика це навіть краще, ніж прямий ефір, оскільки немає постійного тиску, людина більш розслаблена. З другого боку, журналіст може заднім числом додати свої коментарі, на які політик уже не в змозі реагувати. Якщо ж інтерв'ю дається окремими шматками упереміш з коментарями журналіста і різними додатковими сюжетними ходами, то тут політик повністю у владі телебачення.

В. Атмосфера інтерв'ю: формальна – неформальна, довірча – ворожа, агресивна – доброзичлива і т. д. Атмосфера задає тон дискусії. Тон зумовлює подальші оцінки глядачів. Якщо журналіст говорить – "а зараз подивіться інтерв'ю з лідером так званих патріотів N", – то глядачу задаються певні рамки, і він ще до інтерв'ю приймає той або інший бік, що позбавляє значення всю розмову. Коли журналіст подає якогось діяча, кажучи про нього щось позитивне, то вже цим дається сигнал доброзичливо поставитися до всього, що скаже цей суб'єкт. Розуміючи це, політики намагаються мати "свої" ЗМІ або, принаймні, "своїх" людей в ЗМІ. "Свої" журналісти виступають в ролі постановників шоу, репетиція якого проведена наперед, що зовсім не в'яжеться з образом журналіста як "сторожового пса демократії". Зате політика, якого доручено "ставити на місце", журналісти можуть, м'яко кажучи, закидати провокаційними запитаннями.

Газети і журнали. Перш за все читач звертає увагу на фотографії. Особливо якщо перед ним кольоровий журнал. Підбір фотографій залежить від тих цілей, які ставлять перед собою автори матеріалу. Підібрати невигрішне для того або іншого політика фото нічого не варто. Навіть у професійних фотомоделей є ракурс зйомки, якого вони уникають. Що ж говорити про політиків, які в більшості своїй далеко не Аполлони.

Взагалі, політики надають багатий матеріал журналістам для маніпулювання. Головним чином це вислови. При умілому підході цитата, що вирвана з контексту і супроводжується коментарем автора, може тлумачитися абсолютно довільно.

Газети живуть завдяки сенсації. Їх задача – заманити читача. Тому такі подарунки від політиків, як висловлювання типу: "масмо, що масмо" (з цього "масмо" – мало що зрозуміле), про нескінченні "граблі для політиків" тощо, "приречені" на увагу ЗМІ, а не на користь вирішення справ. Їдкі коментарі, статті, карикатури, фотографії, що виставляють політика в непривабливому світлі, – всі ці прийоми негайно пускаються в хід.

Окремо про заголовки. Заголовок на першій смузі, надрукований великим шрифтом, привертає увагу. Оскільки газети купуються в поспіху, то покупець орієнтується перш за все на заголовки, не вчитуючись в зміст. Але коли починає вчитуватися, то знаходить, що помітний заголовок далеко не завжди відповідає змісту. Як правило, зміст набагато скромніше заявленої сенсації, а іноді й повністю суперечить заголовку.

Маніпуляції в ЗМІ за допомогою опитувань. Одним з прийомів маніпулювання, що використовується в ЗМІ, є публікація опитувань громадської думки. Напередодні вибо-

рів цей прийом стає особливо затребуваним. Технологія опитувань така, що припускає лише відповіді "так" чи "ні". Самі по собі запитання між опитуваним і інтерв'юером не обговорюються. Але ж весь фокус полягає в самій постановці питань "так" чи "ні".

У плані розвитку ЗМІ майбутнє за Інтернетом, який "обплутав" своєю мережею земну кулю. Коли у подальшому з'являться інші техніко-технологічні новації, маніпулятори, без сумніву, оволодіють ними, світ побачить нові маніпулятивні технології.

Питання для самоконтролю

1. Інформація та її вплив на суспільний розвиток.
2. Конституція України щодо упорядкування суспільних відносин в інформаційній сфері. Положення статей 3, 8, 22, 23, 31, 32, 34, 41, 54, 66, 68, 157 Конституції України.
3. Становлення прав людини і свобод у концепціях природного права.
4. Права людини у сучасних міжнародних документах.
5. Інформаційні права у класифікації прав людини.
6. Інформаційна політика розвинених країн та в Україні.
7. Маніпулювання свідомістю людини як фактор рефлексивного управління та формування суспільної думки.
8. Поняття, чинники, види маніпулювання свідомістю людини.

Розділ 2. ІНФОРМАЦІЙНЕ ПРАВО У СИСТЕМІ ПРАВА

2.1. Базові поняття

2.1.1. "Людина", "громадянин" і "особа" та "права" і "свободи"

Ще за глибокої давнини люди розуміли – все починається з розуміння сутності понять та їх термінологічного тлумачення, тобто – дефініцій. Дефініції віддзеркалюють істотні ознаки (зміст) предмета або явища за допомогою загальновживаних слів (імен). У трактаті "Категорії" великий філософ Аристотель звертав увагу на те, що імена і речі (предмети) перебувають в досить складних відносинах. Серед них є "омоніми" – слова-близнята, що позначають різні по суті речі, які, втім, пишуться однаково; "синоніми" - слова, схожі за значенням, але різні за написанням та звучанням; "пароніми" – слова одного кореня, але різного граматичного походження. Без розуміння змісту, який вкладається в те або інше слово, співвідношення між словами та комунікації людина сама по собі, просто як індивід, існувати не може. Комунікація – це спілкування, універсальна умова людського буття. Людське існування (екзистенція) створене словом. У 20-х рр. минулого сторіччя філолог, філософ, історик і математик О. Лосєв стверджував: "Слово виражає сутність речі. Назвати річ, дати їй ім'я, виділити її з потоку незрозумілих явищ, подолати хаотичну плинність життя - значить зробити світ розумнішим. Увесь світ, Всесвіт є не що інше, як імена і слова різних ступенів напруженості. Тому слово – є життя. Без слова та імені людина асоціальна, не здатна до спілкування, не соборна, не індивідуальна. Словом та ім'ям створений і тримається світ" [139, с. 3].

Зазначений аспект особливо важливий для людини, яка звикає до світу віртуальної діяльності. Нині він охоплює все те, що пов'язується з інформаційними відносинами в електронно-інформаційному середовищі та становленням інформаційного права у системі права. Знання змісту та співвідношення понять прямо пов'язано з вирішенням питань підстав та меж їх застосування в інформаційному законодавстві.

Український вчений О. Баранов у статті "Понятійний апарат інформаційного права" відзначає [141]: "Інформаційне право вимагає уважного ставлення до його термінологічної системи. Достатньо інтенсивний процес створення сучасного інформаційного законодавства зумовив появу термінів, які можуть неоднозначно трактуватись. Часто це відбувається тому, що впродовж короткого відрізку часу (10 – 15 років) відбулася істотна трансформація розуміння змісту багатьох понять, які застосовуються в інформаційному праві. Соціально-політичні реформи у 1990-х р. у нашій країні привели до зміни суспільної свідомості і, як наслідок, до зміни правосвідомості. У суспільстві новому стали сприймати такі поняття, як "свобода слова", "вільний доступ до інформації", "інформаційна безпека" тощо. З іншого боку, технічний прогрес сприяв появі багатьох термінів, які почали широко застосовуватися в законодавстві. Наприклад, буквально останніми роками стали широко вживатися такі поняття, як "електронний документ", "електронний підпис", "електронна торгівля", "веб-сайт", "веб-сторінка" тощо.

Гостроту ситуації додає факт того, що в інших галузях законодавства також з'являються норми, які регулюють інформаційні відносини. При цьому часто використовуються терміни, зміст яких явно дисонує з термінами, які використовуються в "класичному" інформаційному законодавстві.

Наявність сталої термінологічної системи інформаційного законодавства необхідна для того, щоб забезпечити вимоги законотворчої техніки і підвищення ефективності правозастосовної діяльності. Багато авторів звертає увагу на необхідність проведення досліджень з термінологічних проблем інформаційного права. Тому завдання формування чіткої, вивіреної, обґрунтованої термінології інформаційного законодавства, нормативного закріплення понять, особливо на сучасному етапі його формування, є досить актуальним".

Розглянемо важливі поняття, які мають особливе, пріоритетне значення у нормотворчій та правозастосовній діяльності.

У законодавстві України щодо суб'єктів інформаційних відносин застосовуються такі різні за змістом поняття, як "людина", "громадянин" або "особа".

В Конституції України [1] суб'єктами інформаційних відносин визнаються "людина" (ст. ст. 3, 21, 28, 32, 34), "громадянин" (ст. ст. 32, 41, 54) або "особа" (ст. 32). Конституція України застосовує також такі категорії, як "права і свободи людини" (ст. 3) та "права і свободи людини і громадянина" (ст. 55).

Згідно із Законом України "Про інформацію" [4] до суб'єктів та учасників інформаційних відносин віднесено поняття "громадяни" (ст. ст. 7, 42), хоча у тексті Закону застосовуються поняття "особа" (ст. ст. 2, 23, 38) та "фізична особа" (ст. 30).

Людина – узагальнююча назва для всіх представників людства, яка поєднує в собі відображення всіх спільних якостей людей (як біологічного, так і соціального змісту) [148, с. 110]. Кожна людина:

а) народжується індивідом – одиночний представник людського роду, окремо взята людина поза її соціальними якостями. Поняття відображає передусім природно задані властивості людини: стать, вік, фізіологічні особливості та природжені якості її психіки, які відображаються в темпераменті;

б) формується в процесі суспільного життя як особистість – конкретне виявлення соціальної сутності людства на рівні окремих його представників; сукупність інтелектуальних, соціально-культурних і емоційно-вольових якостей конкретної людини;

в) кристалізується в індивідуальність через реалізацію своїх природних, психічних, духовних та соціальних особливостей у соціально значущі якості протягом всього свого життя. Тобто індивідуальність – індивідуальна форма суспільного життя людини, сукупність унікальних та універсальних її якостей – спільних, типових (загальнолюдські природні та соціальні ознаки), особливих (конкретно-історичних) та одиничних (неповторних фізичних і психологічно-моральних особливостей).

Згідно із словником С.І. Ожегова, "человек – живое существо, обладающее даром мышления и речи, способностью создавать орудия и пользоваться ими в процессе общественного труда" [140, с. 875].

В розумінні юридичної науки людина є особою з природними, набутими від народження (невід'ємними) правами і свободами. Тлумачний словник української мови слово "людина" пояснює так [148, с. 503]:

1) будь-яка особа; кожний; людська постать;

2) особа як втілення високих моральних та інтелектуальних якостей.

У підручнику з теорії держави і права [142, с. 326] зазначається, що термін "людина" вказує на біосоціальну істоту, одну з форм земного життя, яка має здатність мислити, створювати й застосовувати для задоволення своїх потреб знаряддя праці, володіє мовою й розвивається за умови широкого та тісного спілкування із собі подібними.

Отже, категорія "людина" застосовується, коли необхідно наголосити, підкреслити природне походження прав і свобод, пріоритетність (верховенство) його потреб та інтересів у взаємостосунках з органами держави. Це обумовлено побудовою сучасної системи права України на засадах концепції природного права, про що йдеться у ст. 3 Конституції України.

Поняття "громадянин" у словнику С.І. Ожегова визначається як "лицо, принадлежащее к постоянному населению данного государства, пользующееся его защитой и наделенное совокупностью прав и обязанностей" [140, с. 146].

В Українській юридичній енциклопедії [143, с. 640] поняття "громадянин" визначено як фізична особа, статус якої обумовлений належністю до громадянства певної країни. Громадяни є найчисленнішою категорією населення, володіють повнішим обсягом прав і свобод, ніж інші – іноземці та особи без громадянства.

Громадянин є завжди людиною. Але з юридичної точки зору не кожна людина може бути громадянином. Звідси випливають певні відмінності у правовому статусі "людини" і "громадянина". Перебування людини у громадянстві країни обумовлює поширення на неї всього обсягу законодавчо гарантованих на території відповідної держави прав і свобод, зокрема пов'язаних з її участю в політичному житті, управлінні державними справами, що невластиве негромадянам, забезпеченням інформаційної безпеки тощо.

Відповідно до ст. 3 Закону України "Про громадянство України" [32] громадянами України є: 1) всі громадяни колишнього СРСР, які на момент проголошення незалежності України 24 серпня 1991 р. постійно проживали на території України; 2) особи, незалежно від раси, кольору шкіри, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, мовних ознак, які на момент набрання чинності Законом України "Про громадянство України" від 13 листопада 1991 р. проживали в Україні і не були громадянами інших держав; 3) особи, які прибули в Україну на постійне проживання після 13 листопада 1991 р. і яким у паспорті громадянина колишнього СРСР зразка 1974 р. органами внутрішніх справ України внесено напис "громадянин України", та діти таких осіб, які прибули разом із батьками в Україну і на момент прибуття в Україну не досягли повноліття, якщо зазначені особи подали заяви про оформлення належності до громадянства України; 4) особи, які набули громадянство України відповідно до законів України та міжнародних договорів України (ст. 3 Закону України "Про громадянство України"). Отже, поняття "громадянин" вказує на людину, котра має стійкі зв'язки з державою.

Етимологія поняття "особа" вказує на: 1) окрему людину; людину-учасника правових відносин; 2) людську індивідуальність, особистість [148, с. 601].

Українська юридична енциклопедія [145, с. 351] містить визначення поняття "особи" як людини, яка знаходиться в системі суспільних зв'язків та відносин. "Особа" володіє рисами та якостями, які визначають людину в суспільному значенні та містять її соціальну оцінку.

Ю.М. Тодика під категорією "особа" в законодавстві має на увазі "мешканця країни" [147, с. 49], тобто будь-кого, хто проживає або перебуває на території держави на законних підставах.

За О.В. Аніпілоговим [69, с. 17], зміст поняття "особа" є значно ширший, ніж термін "громадянин", що означає лише осіб, які володіють громадянством України. З іншого боку, поняття "особа" в юридичному (позитивному) значенні вважається більш загальним, ніж "людина". Воно передбачає такого носія прав і свобод, який володіє не тільки отриманими від народження правами і основоположними свободами, що властиво для статусу людини, а й набутим у процесі життя відповідним соціальним статусом, що визначає людину. Тобто поняття "особа" у зв'язку з державними інтересами може об'єднувати в собі поняття "людина" і "громадянин" та визначатися у правових нормах, що встановлені державою і забезпечуються її примусовою силою.

В нормах законодавства України не співпадає зміст не лише понять "особа", "людина" і "громадянин", а й зміст таких понять, як "права" і "свободи".

"Права" і "свободи" становлять окремі об'єкти правового регулювання. Так, Ю.М. Тодика відзначає, що "між термінами "права особи" і "свободи особи" є як загальне, так і відмінне, хоча інколи вони застосовуються як синоніми. Наявність в особи "права" свідчить про можливість отримання певних соціальних благ, тобто є "правом на" отримання чогось (на працю, освіту, достойний рівень життя і т. д.). Свобода – це можливість людини уникнути впливу з боку держави, державної влади тих чи інших обмежень. Свобода визначає незалежність особи від держави. Наприклад, "свобода" від будь-чого (від цензури тощо)" [147, с. 51].

О.Ф. Черданцев деталізує зміст зазначених понять наступним чином: "По-перше, носій права має можливість вибору одного з двох варіантів поведінки. При цьому він може реалізувати або не реалізувати своє право. За наявності юридично визнаної свободи кількість варіантів поведінки збільшується. Наприклад, свобода думки і слова може здійснюватися у найрізноманітніших діях – громадянин може висловити свої думки як письмово, так і усно в будь-яких формах та видах. По-друге, право громадянина є правом, оскільки закріплюється в позитивному праві (законах) держави. Свобода ж може існувати й без права та держави. Вона не випливає із закону, потребує права як способу й обмеження. По-третє, основному праву, закріпленому в конституції, відповідає позитивний, активний обов'язок держави, направлений на створення умов для реалізації права. Якщо ж відносини особи і держави урегульовані за допомогою категорії "свобода", то держава бере на себе обов'язки пасивні (негативні) не втручатися у сферу свободи, дозволеної законом. Активні дії при цьому вчиняє сам носій свободи. По-четверте, у випадку спорів з державними органами носій права повинен довести правомірність своїх дій, а у разі спорів, пов'язаних із реалізацією свободи, навпаки – державний орган обґрунтовує обмеження свободи рамками закону" [149, с. 111].

Отже, в юридичному (позитивному) значенні поняття "права" означає надані законом особі такі можливості, реалізація яких потребує сприяння з боку органів державної влади або органів місцевого самоврядування (він, як правило, вказує на визначені національним законодавством соціально-економічні та культурні права (права другого покоління), а термін "свобода" – можливості людини і громадянина, що можуть бути практично здійснені за відсутності втручання посіїв владних повноважень у відповідну сферу індивідуальної поведінки (цією категорією позначаються права першого покоління – громадянські свободи).

Проте, як зазначає О.В. Аніпілогов у [69, с. 20], не можна виключати подання позову до суду для захисту й окремих гарантованих законом свобод, які за текстом законодавства іменуються правами, наприклад, ст. 34 Конституції України визначає право кожного на свободу думки і слова, вільне вираження своїх поглядів; ст. 35 – право на свободу світогляду і віросповідання; ст. 36 – право громадян України на свободу об'єднання в політичні партії та громадські організації тощо. Ототожнення в низці положень Конституції України 1996 р. термінів "права" і "свободи" можна вважати проявом традиції щодо створення конституційних документів, в яких немає чіткого розмежування цих понять.

Одночасно, будь-яка "людина", той же "громадянин" чи "особа", яка має унікальні особисті персональні дані, інформацію, що ототожнює та надає можливість ідентифікувати біологічний стан, соціальний статус тощо конкретного індивіда. Застосовувати ці дані треба виходячи, насамперед, з того, що індивід від природи отримав життя та можливість на самовизначення впродовж нього. З цього випливає висновок про те, що з ме-

тою підсилення захисту прав і свобод та зменшення факторів маніпулювання відомостями людина має отримати пріоритет у праві володіння, користування та розпорядження (тирада повноважень права власності) своїми персональним даними за умов забезпечення балансу прав та обов'язків між людиною, суспільством та державою, що має бути визначено в інформаційному законодавстві.

2.1.2. "Інформація" та "дані"

Термін "інформація" походить від латинського "informatio", що передбачає семантично близькі визначення: "пояснення", "виклад", "тлумачення". Українська юридична енциклопедія перекладає слово "informatio" як "роз'яснення, уявлення" [144, с. 717] щодо "документованих або публічно оголошених відомостей про події та явища, що відбуваються у суспільстві й державі та навколишньому природному середовищі", яке відповідає визначенню, наданому у Законі України "Про інформацію" від 02.10.1992 р.

Відомий російський словник С.І. Ожегова надає таке визначення інформації: "сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством" [140, с. 253]. Там же надано дефініцію терміну "відомості" (рос. – "сведения"): "познания в какой-либо области, известия, сообщения, знания, представление о чем-либо" [140, с. 698] та терміну "познание – приобретение знаний, постижение закономерностей объективного мира" [140, с. 546].

За доктором юридичних наук, професором О.О. Гавриловим, "информацией являются используемые данные, представленные в форме, пригодной для передачи и обработки" [150, с. 2]. При цьому російський учений зазначає, що до 1970-х років термін "інформація" ані в загальній теорії права, ані в юридичних науках, ані в законодавстві не застосовувався; вживали таки еквіваленти, як "дані", "матеріали", "відомості" та ін. [150, с. 13].

Доктор юридичних наук, професор В.О. Конилов у монографії "Інформаційне право" посилається на визначення "інформації", яке відповідає визначенню, наданому у Федеральному Законі Російської Федерації "Об информации, информатизации и защите информации" від 20.02.95 р. [60] та ДСТ 51141-98. "Деловодство и архивное дело. Термины и обозначения": "Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления". Але зауважує: "Учитывая социальный аспект рассматриваемого предмета, добавим: в виде, понятном для восприятия человеком. Определение дает возможность "вывести" из понятия "информация" программы для электронных вычислительных машин (ЭВМ), отнесенные названным законом к средствам обеспечения ЭВМ " [92, с. 41].

А. Моль у роботі [163] зазначає, що є "інформація" – як відомі відомості та "нова інформація", яка надає нові знання. Це слід враховувати при нормативно-правовому регулюванні.

Щодо поняття "дані", то словник С.І. Ожегова надає таке визначення: "сведения, необходимые для какого-нибудь вывода, решения" [96, с. 155]; тобто поняття "інформація" та "дані" ототожнюються.

В українських стандартах, які пристосовані до міжнародних стандартів (ISO), термін "дані" визначений як "інформація, подана у формалізованому вигляді, придатному для передачі, інтерпретування чи оброблення за участю людини або автоматичними засобами" [151 – 153]. У "Правилах надання та отримання телекомунікаційних послуг", що затверджені постановою Кабінету Міністрів України від 09.08.2005 р. № 720, – "дані – інформація у формі, придатній для автоматизованої обробки засобами обчислювальної техніки".

Поняття "інформація" властиве мислячому суб'єктові, тим самим під інформацією мається на увазі не тільки зміст відомостей, але й їх інтерпретація, що у подальшому забезпечує, за необхідності, комунікаційну взаємодію. Проте постає питання – комп'ютер ("специальное устройство" – за С.І. Ожеговим) має можливість осягти або осягнути (рос. – постичь, постигнуть) відомості, тобто зрозуміти їх, чи це можливо лише для високоорганізованої матерії, що має складну динамічну систему управління, якою є мозок людини? Чому у вітчизняній, зокрема юридичній, практиці ототожнюються такі поняття, як "інформація" та "дані", а практика європейських стандартів та національних нормативно-правових актів використовує поняття "дані", "обробка даних", "захист даних" тощо (див. [56 – 58; 154])?

З огляду на загальносистемне уявлення поняття "інформація" має два аспекти:

- семантичний аспект: інформація розглядається як відомості, як якісне значення змісту повідомлення (семантичний, якісний аспект інформації). Звідси можна говорити про те, що інформація – це відомості про дійсність на основі мислення і висновків людей або вирішення задач засобами, що наділені "інтелектуальними" можливостями. Безпосередньо цим питанням у 1960-х р. займалися співробітники Всесоюзного інституту наукової та технічної інформації, які вперше в країні видали монографію під назвою "Основы научной информации", у якій підсумовується світовий та особистий досвід того часу [155];
- онтологічний аспект: інформація розглядається як кількісне значення міри пропускної здатності каналу комунікації (визначеності й упорядкованості (інтенсивності) потоку повідомлення в мережах передачі даних, що зветься "трафік") і упорядкування повідомлень (організація процесу кодування/декодування і передачі/приймання даних). Інформація в даному аспекті розглядається як упорядкована субстанція, яку можна описати математично. При цьому під системою упорядкування розуміється система з об'єктивно заданим алгоритмом, що може бути розпізнаний. Мова тут йде не про змістовний аспект інформації, а про можливості її неспотвореного перетворення-кодування для обробки даних в автоматизованих системах і переміщення їх по мережах комунікацій. Цим питанням, що отримало назву "математична теорія інформації", з 1948 р. займалися К. Шеннон, академік А.М. Колмогоров та ін. [155, с. 67].

Існує багато визначень "інформації", котрі умовно можна розділити на чотири групи: життєве розуміння інформації; поняття, що використовує формалізовані моделі реальних об'єктів і процесів; підхід з позицій теорії відображення і пізнання; урахування зв'язку інформації з властивостями матерії. Як ілюстрацію того, наскільки різноманітні підходи до розуміння "інформації" залежно від тих або інших цілей, наведемо деякі з них. Отже, "інформацією" називають:

- будь-які відомості про раніше невідомі події;
- відображення реальності у свідомості людини, представленої на її мові;
- основний зміст відображення;
- семантику або прагматику синтаксису мови представлення даних;
- змістовний опис об'єкта або явища;
- результат вибору;
- зміст сигналу, повідомлення;
- відбиту розмаїтість або її міру;
- зменшувану невизначеність;
- міру складності структур або організації;

- продукт наукового пізнання, засіб вивчення реальної дійсності;
- обов'язкову субстанцію живої матерії, психіки, свідомості;
- нескінченний процес триєдності енергії, руху і маси з різною густиною кодових структур безмежного Всесвіту;
- вічну категорію, що утримується в усіх без винятку елементах і системах матеріального світу, що проникає в усі сфери життя людей і суспільства;
- властивості матерії, її атрибут, якусь реалію, що існує поряд з матеріальними речами або в самих речах тощо.

Множинність підходів до визначень інформації надає, зокрема, на своїх сторінках журнал "Міжнародний форум з інформації і документації": "інформація – негативна ентропія", "те, що змінює наші знання", "відбита розмаїтість", "метаенергія".

Для Н. Вінера інформація – це форма організації живої істоти, що не залежить від матерії й енергії [157].

Академік В.М. Глушков зазначав: "Інформація в найзагальнішому її розумінні є міра неоднорідності розподілу матерії і енергії в просторі і часі, міра змін, які супроводжують всі процеси, що відбуваються в світі... Інформацію несуть у собі не тільки наповнені буквами сторінки книг чи людська мова, але й сонячне світло, складки хребта гір, шум водоспаду, шелест листя і т. д." [159]. При цьому виділяються два різновиди неоднорідності – статистична (характеризує поточний стан певної матеріальної чи енергетичної системи) та динамічна (її змінність у часі). Визначення поняття динамічної інформації виявилося винятково плідним при вивченні інформаційних властивостей фізичних систем. Це дало можливість виділяти та використовувати корисну інформацію з випадкових стаціонарних і нестаціонарних систем, зображень, просторових полів тощо, значно зменшивши її надлишковість. На базі цього досліджуються методи обробки сигналів, синтез алгоритмів і структур спецобчислювачів, покладених в основу створення елементної бази підвищеної "інтелектуальності" [249, с. 64-65].

І. Кочових, заступник Голови Ради Міністрів УРСР із науково-технічного прогресу в 1977 р., писав, що "фіксована інформація є пам'ять про минуле для використання в майбутньому, і нею володіють усі системи світобудови. ...Інформація є така ж субстанція, як Матерія й Енергія. Вони триєдині і складають разом усю світобудову. ...Інформація є відношення Матерії до Енергії. ...тобто Інформація є Час (але не календарний), а Час є Інформація. ...Усі системи, живі і неживі, утворюють навколо себе енергетичні й інформаційні полюси, причому інформаційні полюси є засобом зв'язку всіх систем у єдиному інформаційному полі Всесвіту. Ці полюси, що зараз називають аурою і ноосферою, насправді є інформаційним полем" [158].

При цьому, якщо з енергією, що, як відомо, не може бути знищена і нікуди не зникає, тільки переходить чи трансформується то в матерію (речовину), то в інші види енергії, начебто усе ясно, з інформацією відбуваються дивні речі. Незрозумілою, наприклад, є властивість інформації не зменшуватися від її споживання, а навпаки – збільшуватися, "розмножуватися".

Слово "інформація" відоме ще за часів Аристотеля. "Інформація як наукова категорія введена як первинне поняття, що поряд з поняттями матерії (речовини) і енергії не підлягає визначенню", – заявив на 6-му Міжнародному форумі інформатизації російський академік С.В. Свреїнов. Доктор технічних наук, професор Г.Н. Дульнєв у статті "Інформація – фундаментальна сутність природи" наводить розширене визначення інформації, запропоноване англійським ученим Ешбі: "Інформація є мірою зміни в часі і просторі структурної різноманітності систем...".

Доктор філософських наук з інституту філософії АН Білорусії А.К. Манєєв в глибокому дослідженні інформаційної сутності ноосфери пише [160]: "Любые процессы индуцирования, переработки и преобразования продуктов отображения являются информационными, а информация оказывается упорядоченной структурой".

У наш час доктор технічних наук, професор, президент Міжнародної академії інформатизації І. Юзвішин визначає: "Інформація – це фундаментальний генералізаційно єдиний безпочатково-безкінцевий законопроцес резонансно-стільникового, частотно-квантового і хвильового відношення, взаємодії, взаємопроникнення і взаємозбереження (у просторі і часі) енергії, руху, маси і антимаси на основі матеріалізації і дематеріалізації в мікро- і макроструктурах Всесвіту. ...У третьому тисячолітті інформація як абсолютна істина пізнання явищ і процесів Природи стане глобальним ресурсом науково-технічного прогресу, володіючи яким можна обійтися без тонн вугілля, цистерн нафти, вагонів залізної руди, інших матеріальних, трудових і фінансових ресурсів. Розшифрувавши інформаційно-кодові структури інформації, люди навчаться управляти процесами термоядерного синтезу, гравітації, електромагнітних явищ, самоосвіти і саморозпаду в глибинних надрах Землі..." [161].

Урешті-решт, як випливає із наведеного, універсального визначення поняття "інформації" не існує. Кожне з визначень вірно для певної галузі застосування, і кожне стає неконструктивним, якщо воно застосовується не за призначенням або не сприймається людиною. Дефініції у законах та їх проектах використовують семантичний аспект інформації, тобто змістовний опис об'єкта, предмета та ін.

У чинній нормативно-правовій базі "інформація" інтерпретується як знання, відомості, змістовний опис об'єкта або явища і т.п. Подібне трактування орієнтоване на застосування документа в реальному (аналоговому) середовищі існування, що утворене мислячими суб'єктами-людьми. Лише людина може мати знання, і тільки для неї різноманітні сукупності графічних символів можуть бути "відомостями". Сьогодні тільки для людини певна сукупність символів, знаків, сигналів може інтерпретуватися як "відомості про будь-що", а сам суб'єкт обов'язково має володіти деякою вихідною системою знань, наприклад, вміти читати. Для технічного об'єкта "інформація" не "відомості" і, тим більше, не "знання". У неживій природі (зокрема, у комп'ютері, мережах та ін.) об'єкти (предмети) взаємодіють з інформаційним кодом чи інформаційно-кодовою структурою, але не зі "знаннями" і "відомостями".

Варто розрізняти знання і відомості. Знання – це відображення дійсності у свідомості людей, що є продуктом їх духовної, матеріальної і суспільної діяльності на основі ідей, досвіду і достовірних фактів. Образно кажучи, знання = ідеї + факти + закони логічного мислення. Люди мають різні знання, які накопичуються та можуть змінюватися в обсязі інформації залежно від природних якостей суб'єкта. Якщо знання не сприймаються, то це проблема конкретного суб'єкта, але не інформації. Текст іноземною мовою має сенс для тих, хто знає відповідну мову, але не має значення для інших.

Структура знань може бути описана як тезаурус (від грец. "thesaurus" – скарбниця, комора, склад) одержувача, фактично його запас ключових слів – дескрипторів, зумовлений попереднім досвідом накопичення, осмислення фактів та їх взаємовідносин. По суті, тезаурус – це словник ключових слів, у якому вказані зв'язки слів за їх змістом. Він усуває синонімію, багатозначність слів, вказує базисні відношення між дескрипторами, які існують між ними незалежно від контексту, визначає здатність "витягати" з відомостей нові знання. Його застосовують при автоматизованому перекладі, інформаційному пошуку та інших видах автоматизованої обробки даних.

Відомості відносно об'єктивні. Вони цінні для одержувача тоді, коли змінюють його попередні знання про об'єкти і їх співвідношення, зв'язки з іншими об'єктами. Це положення не залежить від того, у чому ці попередні знання закладені – в апріорних ймовірностях, у деяких фактах, у конкретній формі змістовного опису і т. п.

Цитовані вище юридичні визначення визначають інформацію з позицій сприйняття її людиною. Вони, певною мірою, умовні і суб'єктивні, а конструктивне використання в сфері електронної взаємодії досить проблематичне. Навіть є можливість отримати парадоксальний висновок. Наприклад, комп'ютер не може сприймати відомості, тим більше знання, отже – комп'ютер не може обробляти інформацію. Парадокс означає, що в такому вигляді визначення інформації відображають незначні її властивості з позицій електронної взаємодії. Тут треба виходити з інваріантних властивостей інформаційного сигналу, коду (інформаційної ознаки), але не з інваріантності семантичних ознак інформації.

Машина не вміє мислити ("усвідомлювати", "уявляти", "роз'ясновати") як людина. Вона вміє тільки перетворювати виділену тим або іншим засобом множину кодів (сигналів, структур) на основі однозначно заданої послідовності фіксованих операцій. Приміром, оцінимо два документи зі зміненою послідовністю слів: "двічі по два – чотири" і "чотири є двічі по два". Якщо це традиційні документи, то вони містять ті самі відомості. Але якщо це е-документи, то машина розцінить їх як різні. Для традиційного документа захист інформації є захистом відомостей, для е-документа захист інформації є захист даних, тобто кодів (сигналів, структур). Самі відомості не мають значення, нехай це навіть безглуздий з позицій людини їх набір. Для машини важливе чергування кодів, до яких "прикріплені" ("пристосовані") відомості, і захист даних є збереженням порядку їх черги. У неживій природі об'єкти взаємодіють завдяки кодам, сигналам, структурам (тобто – завдяки формам), але не завдяки комунікації "знань", "інформації" чи "відомостей", що складає змістовно-розумову частину взаємодії.

2.1.3. Гносеологія категорії "право"

Стратегія України щодо європейської інтеграції [81, с. 7] декларує рух до демократії, соціального господарства, функціонування органів держави згідно з чинним законодавством та спрямування до держави громадянського суспільства, яке базується на засадах забезпечення прав людини і основоположних свобод. У статті 8 Конституції України визначено: *"В Україні визнається і діє принцип верховенства права. Конституція України має найвищу юридичну силу. Закони та інші нормативно-правові акти приймаються на основі Конституції України і повинні відповідати їй. Норми Конституції України є нормами прямої дії..."* [1].

Стосовно зазначених формулювань продовжуються суперечки. Вони і досі залишаються належним чином не осмисленими як теорією, так і юридичною практикою. Це породжує різні суб'єктивні інтерпретації у тлумаченні, зокрема того, що стосується сутності категорії "право" та його "верховенства".

У навчальному посібнику "Правознавство" [162, с. 56] *"право"* визначається як *"система соціальних норм"*, що посідає провідне місце. Автори далі зазначають, що *"в юридичній літературі право розглядається як загальносоціальне явище і як волевиявлення держави (юридичне право)"*. Потім вони поділяють "юридичне (позитивне) право" на об'єктивне і суб'єктивне. Перше – це система усіх правових приписів, що встановлені, охороняються, захищаються державою. Друге – певні можливості, міра свободи, що належить суб'єктові, який сам вирішує, користуватися ними чи ні. Таким чином,

"право" складається з так званих "загальносоціального явища" (не дуже зрозуміло, що це таке) і "волевиявлення держави" (тобто – із бажання, згоди або незгоди державної влади, зокрема, законодавця, суду на будь-що). Іншими словами, можна зробити висновок: "право" – це воля чинних органів влади (раніше – це була воля класу), що тлумачать його на свій розсуд, за якими стоїть та яких захищає держава.

Згідно з українською юридичною енциклопедією *"Право – система соціальних загальнообов'язкових норм, дотримання і виконання яких забезпечується державою"* [145]. Тобто енциклопедія зазначає, що "право" – це "норми" поведінки. З наведеного можна робити висновок – у теорії та практиці юриспруденції категорія "право" за сутністю розглядається як "явище + соціальні норми" або звичайно як "норми".

У природній об'єктивності такого уявлення маємо великий сумнів. Цьому сприяють думки, які обережно торкаються сутності змісту категорії "право" в роботі [164], хоча й наводиться вислів судді Конституційного суду ФРН Е.-В. Бьокенфьорда: *"Неможливо гарантувати свободу шляхом формальних юридичних приписів; свобода може бути гарантована тільки в межах фундаментальної системи цінностей, що міститься в конституції"*.

Та все ж, виникає питання: що таке "право" – "явище" чи "норми", чи – це їх суміш та яке до них має відношення поняття "справедливість", якої усі прагнуть?

Почнемо із зауваження того, що поняття "справедливість" (від лат. – "justitia"; за С. Ожеговим – це "система судових установ, а також сфера їх діяльності" [96, с. 912]) походить від категорії "право" (від лат. – "jus"). Справедливим вважається те, що виражає право, відповідає праву, те, що є правильним, правомірним, істинним, підтримує гармонійність у житті.

За формальною логікою (за суттєвими ознаками та відмінностями) зміст категорії "Право" не збігається із змістом понять "правотворча" або "законотворча діяльність" та "законодавство", вони є тільки формою виявлення "Права". Тобто "законотворча діяльність" – це розробка норм упорядкування суспільних відносин, а "законодавство" – це сукупність законодавчих актів, зміст яких визначається відповідними нормами, що затверджені у встановленому порядку. Іншими словами, держава не може мати монополію на "Право". Ця категорія має природний зміст, є базисом створення норм та законодавства й не повинна залежати від суб'єктивно-політичних уявлень.

Науково-юридичний зміст категорії "Право" (не побутовий, коли зазвичай це слово використовується як кому та де заманеться) може бути зрозумілим лише за умов відокремлення його від таких понять, як "закон", "норми", "нормативно-правові акти", "загальнообов'язкові норми", "волевиявлення держави", "правотворча діяльність", "законотворча діяльність". І це повинно здійснюватися на основі історично вироблених гуманістичних уявлень щодо людських стосунків, прав людини та свобод, що висвітлені у Конвенції Ради Європи 1950 року та Протоколах до неї (див. [81, с. 34-59]). Інакше кажучи "Право" – це не "явище" (тобто не форма прояв будь-чого), не "норми" (тобто, не правила поведінки), не "закони" (тобто не сукупність відповідних норм). "Право" – це природні загальнолюдські цінності щодо справедливості (тобто початкові світопереконання про справедливий устрій між людьми), що вироблені історією світової цивілізації та призначені для подолання такого соціального феномену, який Томас Гобс (1588 – 1679 р.) у книзі "Левіафан" (опублікована у період правління О. Кромвеля) визначив як "війна всіх проти усіх" [75, с. 234]. До речі, Лех Валенса (свого часу лідер "Солідарності", керівники якої після перемоги переконалися, що є звичайним для нових демократій) визначав дефініцію "демократія" як "війна всіх проти всіх під контролем права".

За Т. Гобсом, усі люди рівні від природи. Але оскільки вони егоїсти і прагнуть не тільки зберегти власну свободу, а й підпорядкувати один одного, то виникає ситуація

боротьби кожного з усіма. Це робить життя "безпросвітним, звіриним, коротким". У подібному суспільстві "людина людині – вовк". Щоб вижити в цій війні, люди об'єднуються та передають повноваження центральній владі. Таким чином, держава предстає як результат дії суспільного договору. Договір між людьми завершується вибором правителя або верховного органу (від цього залежить форма правління), який допомагає покласти край війні. Оскільки держава відображає бажання більшості об'єднатися, то проти цього не в силах боротися окремі люди. "Наступает мир", – вважав Т. Гобс. Без влади держави всі заклики до моралі перетворюються на пустий звук. Тільки держава вносить порядок у безладний потік людських пристрастей та інстинктів, за допомогою закону приборкує їх, щоб люди не могли шкодити один одному.

Важливо підкреслити: Т. Гобс був прихильником необмеженої влади держави, що поширюється як на поведінку людини, так і на її переконання. У ті часи таких понять, як "права людини", "громадянське суспільство", "свобода слова" тощо не існувало. Незважаючи на те, що філософ не ставив під сумнів "кастовість" і привілейованість заможної частини суспільства, головною умовою справедливості він вважав *"наличие внутреннего света, указывающего путь к истине"* і стверджував (у розвиток думки Френсіса Бекона – *"Истина дочь Времен, а не Авторитета"* [75, с. 219]): *"Философия есть дочь твоего мышления"*. Тобто він закликав людей не чекати негативних подій, а думати та шукати мудрість у стосунках.

"Право" не може бути регулятором суспільних відносин. Воно декларується у доктринах, концепціях, світових стандартах. Його реалізація потребує визначення у конституціях, нормативних актах та механізмах впровадження у життя. "Право" – це вищий базис відстоювання інтересів особи від посягань державних осіб. Гітлер і Сталін розглядали "Право" як відстоювання інтересів держави, навіть на шкоду особі; тобто народ, держава – все, людина із законом – потім. Ф. Бекон казав: *"Существуют три источника несправедливости: насилие, злонамеренное коварство, прикрывающееся правом и именем закона, и жестокость самого закона"*.

Академік АПрН України В.Г. Гончаренко зауважує: *"...ніщо не є законним, якщо воно суперечить розуму. В цьому давньоримському афоризмі міститься мудра настанова в сенсі справедливого регулювання відносин у суспільстві, адже право – це система наявних у даному суспільстві правових доктрин і цінностей та сформована на цій основі система загальнообов'язкових правил поведінки. Саме тому проголошений Конституцією принцип верховенства права є великим соціальним досягненням"* [168].

"Право" – це система цінностей, накопичених історією (правда, справедливість, мораль, свобода тощо), а не воля органів держави та законодавця. Ці цінності існують не для того, щоб панувати в реальному житті для окремих груп та осіб; як казав Ш. Лемель: *"Для других создают правила, для себя – исключения"*. Вони існують для врівноваження цінностей реальних, якою-сь мірою оріентувати їх у бік ідеалу, зменшити несправедливість, надати більшої правди у житті, позбавити нас від "макіавеллістів", маніпуляторів-політиканів, демагогів, заангажованих ЗМІ тощо. Тому "Право" має панувати над державою, адже воно є первинним, а держава та закони – вторинні. Держава не створює і не змінює "Право", вона лише здатна надавати йому формально юридичну визначеність та зобов'язана його захищати. Але політики й особи, обтяжені "народною довірою", та належні їм ЗМІ постійно намагаються нам навіяти, що не нашого розуму справа шукати правду і справедливість, втручатися у всякі там державні справи і таємниці, тим більше звертатися до Євросуду з прав людини. Дізнаються, наприклад, правду про таємницю знищення журналіста, підслуховування, отруєння Президента тощо – і вийде одна шкода. Деяким особам байдуже те, що прагнення до знання правди – це

найважливіший інстинкт розумної істоти, необхідний початковий етап у порядному та справедливому житті в цьому світі, що і є суттю та виправданням існування людини на глиняному клаптику під назвою Земля, що мчить у нескінченності.

Будь-яке обмеження знання нестерпне людині як форма обмеження його свободи – обмеження особи в задоволенні бажання і дії. Знати і жити – це одне і те ж. Проте існуюча в незалежній Україні реальність свідчить, що влада робила та робить кожного з нас не "людиною-особистістю", а "людиною державною", для якої "верховенство права" – на папері. Й це нерідко здійснюється за допомогою маніпулювання свідомістю людини, демагогії, брехні тощо, до чого ми звикли, бо усі роки "незалежності" нас привчають до старої "залежності", але вже в ринкових умовах.

У виступі на конференції "Україна-2007" у Європейському парламенті Олександр Северин на усю Європу та увесь світ зазначив наступне: *"...коли йдеться про права людини в Україні, слід розуміти дві речі.*

Перше. В Україні існує доволі непогана в частині, що стосується прав та свобод, Конституція України, стаття 3 якої декларує: "Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави".

Друге. Все це "верхівку" цікавить лише настільки, наскільки застосування відповідної риторики є корисним задля отримання, збереження влади... . Система жодним чином не зацікавлена в реалізації людських та громадянських прав і свобод. Радше – зацікавлена рівно настільки, наскільки це потрібно для окозамилення Європи" [169].

Для того щоб запустити механізми забезпечення принципу "Верховенства Права", слід відійти від застарілого правового мислення та сформувати мислення, що базується на природному тлі праворозуміння, яке не обмежується трактуванням "Права" як системи норм, встановлених або санкціонованих державою, а розглядає його як загально гуманістичну цінність, інститут, що стоїть на сторожі особистості, її прав і свобод, силу, здатну "приборкати" саму владу, захистити громадянина від її свавілля. Лише за цієї умови принцип "Верховенства Права" стане реальністю.

Враховуючи природне існування та призначення того, що вкладається у категорію "Право", можна логічно вивести його складові, які по суті є самостійними принципами, що лише за умов їх реалізації складають, визначають та забезпечують нормативний аспект його реалізації. До нього належать такі складові:

- пріоритетність прав людини і основоположних свобод;
- обмеження державної влади правами людини та свободами. Заборона їх патерналістського тлумачення, що відповідає природному праворозумінню;
- створення максимальних умов самостійності "Права" від політики; абсолютно відокремити ці речі неможливо, тому відносна, максимальна самостійність. "Право" визначає "поле"* діяльності для політиків та урядовців, яке має здійснюватися на принципах, що закладені у ньому. Політика та урядова діяльність усіх рівнів має базуватися на наступному:

1. *Народ є* не джерелом влади (стаття 5 Конституції), а *є одним її носієм.*

2. *Конституція має бути перероблена фахівцями-юристами* (бажаючими створити демократичну, соціальну, правову державу, а не країну, яка належить 200-300

---

* У юридичній літературі часто використовують термін "правове поле". Виник з англійського "legal environment", що при перекладі українською мовою дослівно означає "законне середовище" або "середовище закону".

сім'ям) у єдиний нормативно-правовий акт прямої дії, і *зробити це легітимним має народ*, а не окремі, навіть дуже авторитетні партії чи особи.

3. *Не повинно бути поділу влади на три складові*, тобто не мають існувати три окремі гілки влади (стаття 6 Конституції). Необхідно ділити не владу, а функції її здійснення. Необхідно обов'язково додати державі інформаційну функцію у зв'язку із розвитком інформаційного права та перспективами розвитку е-середовища.

4. *Створити незалежність судової влади від держави* та ввести жорстку громадянську контрольну функцію над її діяльністю. Заборонити судам у відмові в правосудді. Заборонити відомствам, що координують діяльність зв'язку (зокрема, Мінтрансзв'язку), у відмові подання та пересилання скарг громадян до Європейського суду.

5. *Заборонити зворотну дію закону.*

Цей перелік можна продовжити, і вважаємо, він буде продовжений. Головне у тому, що джерелом норм Конституції та інформаційного законодавства повинно бути "Право", що базується на природі самої людини, на розумі індивіда, на історичних цінностях, які визначені у світових стандартах. Людина є істотою, яка має свідомість, почуття і свободу волі, здатна (що дуже важливо) у справедливих соціальних умовах володіти собою, опановувати себе. Саме наявність громадянського суспільства та застосування принципу верховенства розуму у пошуках вирішення соціальних проблем (а не думки різнокольорового натовпу на майданах, або лобіювання кулуарних рішень у меркантильних інтересах суб'єктів у владі) в поєднанні з такою абстрактною, але важливою категорією, як справедливість, і є ідеальною ознакою дії у державі принципу "Верховенства Права".

2.2. Система права

Система права – це об'єктивно існуюча, єдина, цілісна, узгоджена і внутрішньо несуперечлива організація принципів суспільних відносин та їх віддзеркалення в нормах законодавства, об'єднаних у відносно самостійних структурних елементах, які визначають галузь права.

Основу системи права складають особливим чином структуровані і взаємозв'язані норми, що регулюють суспільні відносини. Норми об'єднуються в загальніші нормативно-юридичні утворення: інститути, підгалузі та галузі. Галузь права групується за ознакою єдності предмету і методу регулювання відносин, а законодавство окремої галузі визначається комплексом законів і підзаконних нормативні актів, що містять норми однієї або декількох галузей права.

Наука переслідує мету пізнання закономірностей виникнення та розвитку предмету дослідження, що здійснюється завдяки застосуванню відповідних методів. Не виключенням з цього є й система права, яка має свою методологію, тобто принципи та способи організації теоретичної та практичної діяльності [140, с. 352] у дослідженні теорії права та пошуку знання.

Ідея ясності і достовірності думки як критерію достовірності знання належить Р. Декарту (1596-1650 рр.). У "Правилах для руководства ума" він по-суті сформулював загальнометодологічні установки, що зберегли своє значення й у наш час [146, с. 272]:

"Необходимо считать истинным только то, что представляется уму столь ясным и отчетливым, что не дает повода подвергать это сомнению;

встречающиеся затруднения делить на столько частей, сколько возможно и нужно для лучшего их преодоления;

начинать с наиболее простых предметов и постепенно восходить к познанию сложного, предполагая порядок даже там, где объекты мышления не имеют естественной связи;

составлять возможно полные перечни и обзоры исследуемых предметов, чтобы была уверенность в отсутствии упущений".

2.2.1. Методологія теорії права

Методологія теорії права є системою особливих принципів, способів та прийомів вивчення загальних закономірностей виникнення, становлення і розвитку правових явищ. Для права властива наявність не одного окремо взятого принципу, способу або прийому в дослідженні предмету, а їх сукупність в застосуванні.

Основними у методології дослідженні теорії права є такі принципи [123]:

• історизм. Він означає розгляд існуючих соціальних та правових явищ не тільки під кутом зору справжнього їх стану, але і з позицій минулого та передбачуваного майбутнього. Вельми важливими при цьому є відповіді на питання, що стосуються причин і умов виникнення права, основних чинників його становлення та розвитку в теперішньому часі і минулому, основних перспектив та тенденцій їх еволюції в майбутньому;

• всесторонність. Основне значення його полягає в тому, щоб досліджувати правові явища не самі по собі, а в їх взаємозв'язку та взаємодії з іншими явищами, що співвідносяться з ними. Повнота і всесторонність дослідження припускають також розгляд права не в одному окремо взятому, а у всіх аспектах, що формують загальне бачення досліджуваних явищ;

• комплексність. Зміст цього принципу полягає в тому, щоб досліджувати його не тільки з юридичної точки зору, але і з позицій інших суспільних наук – філософії, соціології, політекономії, політології, враховуючі новітні досягнення зокрема щодо інформатизації.

Важливо розглядати всі складові сторони і елементи права не тільки в статиці, але і в динаміці – з погляду того, як вони виникли, розвивалися і якими вони стали тепер.

Разом з принципами пізнання велике методологічне значення для дослідження права мають конкретні методи. У науковій і учбовій літературі їх прийнято ділити на наступні групи:

• загальні методи. Вони застосовуються не тільки в теорії держави і права, але і в інших науках. Серед них – методи порівняння, аналізу і синтезу, абстрагування, системного і структурного підходів, методи підведення менш загального поняття під загальніше, перехід від абстрактного до конкретного та інші. Не всі ці методи мають однакове по частоті та ефективності застосування. Наприклад, методи аналізу і синтезу застосовуються в повсякденній науковій роботі набагато частіше, ніж, скажімо, системний метод. Проте всі вони мають важливе значення для отримання об'єктивних знань про право, для глибокого і усестороннього його дослідження.

• спеціальні методи. Вони розробляються в рамках окремих спеціальних наук і широко застосовуються для вивчення держави і права. До спеціальних методів звичайно відносять статистичні, соціологічні, психологічні, кібернетичні, математичні та багато інших методів. Практична значущість цих методів полягає у тому, що вони разом з іншими методами дозволяють поглянути на державу і право з позицій недержавно-правових дисциплін, допомагають створити повніше уявлення про право.

• приватні методи. Головна особливість їх полягає у тому, що вони виробляються самою теорією права та іншими юридичними науками і застосовуються тільки в межах

цих наук. До даної групи методів слід віднести порівняно-правовий метод, методи вироблення правових рішень, методи тлумачення юридичних норм та інші.

2.2.2. Динамізм у системі права

Сьогодні дослідження проблеми наявності або відсутності динамізму в розвитку права виходить з питання стосовно підходів до упорядкування відносин у сферах соціальної-економічної та політичної дійсності, які обумовлені появою нових інформаційно-технологічних відносин щодо формування електронно-інформаційного середовища. Необхідність глибокого і всебічного вивчення проблем системи права визначається не тільки їх теоретичною значущістю, а й тим, що такі дослідження служать передумовою вирішення завдань створення законодавства на науковій основі.

Доктор юридичних наук С.В. Поленіна у [190] справедливо визначає, що визнання динамізму системи права, що виявляється у формуванні нових галузей і інститутів у міру соціально-економічного розвитку, належить до безперечних досягнень юридичної думки. Проте в питанні про шляхи, способи і швидкість звершення змін у системі права ще багато невирішеного. В першу чергу це відноситься до дискусійної проблеми становлення нових галузей права.

Звертаючись до суті проблеми, вона відзначає [190, с.71], що фактично всі можливі випадки виникнення нових галузей права можуть бути зведені до двох основних: 1) поширення правової регламентації на ту частину соціальної дійсності, яка раніше не була об'єктом правового регулювання; 2) відбрунькування від однієї або декількох галузей права взаємозв'язаної сукупності норм (правових інститутів), що набули якісно нових властивостей. Самі по собі такі думки навряд чи можуть бути предметом суперечки. У тій або іншій формі з ними погоджуються багато дослідників. Проте при цьому більшість авторів обходить мовчанням найважливіше питання – як же виникає і протікає процес становлення нових галузей права або, точніше, коли і чому можна вважати, що утворювана одним з двох названих вище шляхів нова галузь права дійсно виникла?

Для відповіді на це питання необхідно перш за все з'ясувати, чи є які-небудь проміжні (перехідні) форми, наявність яких могла б свідчити про можливість виникнення нової галузі права. У першому випадку такою проміжною формою слід вважати появу правового інституту (іноді він "примикає" до однієї з галузей права), в якому новизна, специфіка предмета регулювання зумовили зародження паростків нових властивостей в частині методу, принципів і механізму правового регулювання. Якщо ж нова галузь утворюється шляхом відбрунькування від однієї або декількох галузей права певної сукупності норм, що набули якісно нових властивостей, такою проміжною (перехідної) формою у вигляді загального правила слід вважати появу комплексного міжгалузевого "прикордонного" правового інституту.

С.В. Поленіна зазначає, що суперечка про існування в системі права комплексних утворень, зокрема комплексних правових інститутів, має давню історію. Вперше ідею про наявність основних і комплексних галузей права, розташованих в системі права в різних класифікаційних площинах, висунув В.К. Райхер [191]. Його позиція у принципі була підтримана Ю.К. Товстим, хоча він виступив з твердженням, що комплексні галузі права на відміну від основних ніякого місця в системі права не займають, а їм відводиться лише умовне місце залежно від цілей систематизації при систематиці норм [192].

Ідея існування комплексних галузей права спочатку була підтримана також О.С. Іоффе і М.Д. Шаргородським, які вважали її плідною з погляду практичного застосування для систематики (структуризації) чинного законодавства. Разом з тим, вони заперечували проти твердження В.К. Райхера, що комплексні галузі можуть входити в систему права, вважаючи це неможливим [193].

Проти існування комплексних галузей права свого часу виступав С.С. Алексєєв, на погляд якого найслабіший пункт теорії В.К. Райхера у фактичному запереченні об'єктивної обумовленості системи права базисом даного суспільства, що виражається в ідеї про наявність множинності класифікаційних критеріїв розподілу права на галузі. Заперечуючи також Ю.К. Товстому, О.С. Іоффе і М.Д. Шаргородському, С.С. Алексєєв писав: "Якщо залишатися в межах фактів реальної дійсності, якщо, отже, не займатися довільним конструюванням комплексних галузей, то не можна не визнати, що всі ті сукупності норм, які в літературі зараховувалися до комплексних галузей (транспортне право, морське право, страхове право, банківське право та ін.), насправді не є підрозділами об'єктивно існуючої системи права. Всі вони вносяться або до галузей законодавства, або до галузей правової науки" [194]. Відкидаючи існування комплексних галузей права, С.С. Алексєєв, разом з тим, детально обґрунтував вельми плідну для пізнання шляхів розвитку системи права тезу про наявність в системі права комплексних (змішаних) правових інститутів [194, с. 82-93].

Супротивником розподілу галузей права на "основні" і "комплексні" виступив О.А. Красенів, який обґрунтовано показав, що такий розподіл заснований на змішуванні системи права із системою законодавства в цілому або з системою окремих законодавчих актів. Система права не складається, не утворюється із системи законодавчих актів. Система права – соціальна реальність, в якій юридично відображається структура регульованих відносин. Що ж до комплексних галузей, то вони суть не галузі права, а довільні (виходячи з тих або інших наукових, педагогічних або практичних міркувань), суб'єктивно сформовані групи норм права, що належать до окремих галузей системи права в цілому або до окремих правових інститутів системи конкретної галузі права зокрема [196].

С.В. Поленіна, відзначаючи дискусійність в системі права комплексних утворень, вважає реальним фактом існування "комплексних правових інститутів" [190, с. 74].

У роботі [195] наголошується, що комплексні правові інститути найчастіше визначаються як інститути окремої галуві, які включають ряд елементів іншого методу правового регулювання. Проте таке визначення застосовне не до всіх комплексних правових інститутів, а лише до певного підвиду комплекених міжгалузевих "прикордонних" інститутів.

Міжгалузеві інститути – найпоширеніший різновид комплексних правових інститутів. Вони виникають на стику суміжних галузей права, тобто галузей, що володіють відомою спільністю кола регульованих ними відносин. Так, стосовно цивільного права суміжними в найзагальнішому вигляді будуть всі галузі, що регламентують відносини, які мають майновий зміст (адміністративне, фінансове, трудове право і т. д.). Як вважає С.В. Поленіна, міжгалузеві комплексні правові інститути можуть бути поділені на міжгалузеві функціональні і міжгалузеві "прикордонні" [190, с. 75].

Міжгалузеві функціональні комплексні інститути виникають на стику неоднорідних галузей права, наприклад, цивільного і адміністративного. Неоднорідність названих галузей права зумовила наявність між нормами цивільного і адміністративного права, що стикуються при регламентації тих або інших відносин, наприклад, поставки або перевезення, лише функціонального зв'язку.

Інакше відбувається справа з комплексними міжгалузевими "прикордонними" інститутами, що утворюються на стику суміжних однорідних галузей права, напри-

клад, цивільного і сімейного. "Прикордонні" міжгалузеві інститути визначаються наявністю між нормами суміжних однорідних галузей права, що створюють даний інститут, рухомого предметно-регулятивного зв'язку. Найчастіше цей зв'язок виявляється у тому, що на предмет однієї галузі права накладаються деякі елементи методу правового регулювання іншої галузі. Прикладом такого підвиду міжгалузевих "прикордонних" інститутів може служити інститут відшкодування шкоди, заподіяної життю або здоров'ю людини у зв'язку з виконанням нею трудових обов'язків.

Виникнувши, "прикордонний" правовий інститут може розвиватися в декількох напрямах. Можливий зворотний розвиток "прикордонного" інституту, тобто такий варіант, коли він розвиватиметься переважно як інститут "материнської" галузі права. В цьому випадку привнесені риси іншої суміжної однорідної галузі права займатимуть все менше питомої ваги в регламентації даних відносин, і таким чином, інститут поступово втратить свій комплексний зміст. Можливим є і прямо протилежний варіант, коли у міру подальшого розвитку "прикордонного" відношення число запозичених рис неухильно збільшуватиметься, а сам інститут почне "спеціалізуватися" як інститут суміжної галузі. Врешті решт, такий процес також приведе до того, що даний правовий інститут втратить свій комплексний зміст і перейде із системи "материнської" галузі права в систему суміжної однорідної галузі.

В процесі спеціалізації "прикордонних" інститутів настає момент, коли число запозичених рис нібито врівноважується, стає майже рівновеликим. Тут віднесення "прикордонного" інституту до тієї або іншої галузі права по суті є умовне. Якщо стан подібної рівноваги триває достатньо довго, можлива своєрідна мутація взаємодіючих у рамках даного комплексного інституту рис суміжних однорідних галузей права. Спочатку вона може виявитися у вигляді лише незначних модифікацій предмета, методу, а також механізму правового регулювання, не властивих раніше даним галузям права. Проте, зберігаючись тривалий час, така "мутація" може набути стійкості, поступово заглиблюючись і розширюючись, додаючи "прикордонному" інституту нові якості і властивості. Цей третій можливий варіант розвитку "прикордонних" правових інститутів і приводить часто до появи надалі нової галузі права.

Але і тут для перетворення "прикордонного" інституту в нову галузь права, крім всього іншого, необхідно, щоб "прикордонний" інститут настільки розріс в ширину і у глибину, утворивши по суті якийсь комплекс взаємопов'язаних "прикордонних" інститутів, що володіють однорідними властивостями. Іншими словами, перетворення "прикордонного" правового інституту, а точніше, групи взаємопов'язаних "прикордонних" інститутів в нову галузь права можливо лише тоді, коли цей інститут набуває якоїсь певної критичної маси, лише після досягнення якої у нього з'явиться необхідна сума нових властивостей, що стосуються предмета, методу, принципів і механізму правового регулювання. Наявність їх, згідно з панівною в науці думкою, і дозволяє констатувати, що перед нами нова галузь права.

Важливішим показником перетворення групи взаємозв'язаних "прикордонних" інститутів на нову галузь права може служити поява нових, властивих тільки даній групі інститутів, понять і конструкцій, а також формування загальної частини, що містить принципи і засади, що поширюються однаково на всі відносини, що регламентуються цією галуззю.

Накопичення групою взаємопов'язаних "прикордонних" правових інститутів критичної маси – не просте розростання нормативного матеріалу до певної межі, досягнення якої автоматично означало б визнання факту існування нової галузі права. Досягнувши критичної маси, кількість переходить в якість, відбувається стрибок, у результаті якого з'являються нові властивості, що стосуються предмета, методу, принципів і механізму правового регулювання певної області суспільних відносин. Саме тому визнання комплексних інститутів не спричиняє обов'язкового визнання наявності комплексних галузей права, під якими розуміють сукупність комплексних інститутів. Більш того, сукупність "прикордонних" міжгалузевих комплексних інститутів тільки тоді й може кваліфікуватися як нова галузь права, коли вона набуває якісно нових властивостей і, отже, втрачає ознаки комплексності. Тобто природа галузі права як категорії соціальної дійсності виключає можливість існування комплексних галузей права.

Швидкість процесу досягнення "прикордонним" інститутом критичної маси, а отже, становлення нової галузі права залежать від швидкості дозрівання соціально-економічних умов, що породили нові явища в суспільному житті. Якщо ж зміна соціально-економічних умов відбувається еволюційним шляхом, швидкість формування нової галузі права переважно буває також відносно невелика, а сам процес становлення може тривати не одне десятиліття.

Таким чином, правова регламентація нових сфер соціальної дійсності, зокрема завдяки появі й активному розповсюдженню електронно-комп'ютерних технологій і мереж, прискорення темпів розвитку суспільних відносин, активізація законотворчої діяльності не залишають у наш час сумнівів у динамічності розвитку системи права.

2.2.3. Класифікаційні ознаки галузі права

Галузь права – це основний елемент (підрозділ) системи права, що є розподіленою по правових інститутах сукупністю юридичних норм, які регулюють однорідну область суспільних відносин.

Юридична наука щодо поділу системи права на галузі виходить з двох ознак:

- матеріальної, що відображає особливості регульованих суспільних відносин або предмет правового регулювання;
- методологічної, що є сукупністю юридичних прийомів і засобів впливу на суспільні відносини. Звичайно виділяють два методи: імперативний і диспозитивний.

Виходячи з означеного кожна галузь права має свій власний *предмет правового регулювання*, тобто вид суспільних відносин, що врегульовуються саме цією галуззю. Предмет правового регулювання галузі, як правило, не збігається з предметами інших галузей, а тому саме предмет правового регулювання є основним критерієм поділу правових норм на галузі.

Допоміжними критеріями цього поділу є *методи правового регулювання*, які визначаються формами та правовими засобами, за допомогою яких здійснюється вплив на відповідне коло суспільних відносин і їх учасників, та функції конкретної галузі – ті специфічні завдання, які виконує кожна галузь права. Тобто галузь права – це система конкретного виду суспільних відносин, яка властивими їй методами упорядковує їх у певній сфері суспільного життя. Таким чином, *головною класифікаційною ознакою у визначені нової галузі права є наявність у неї свого предмета та методів правового регулювання відповідних відносин.*

Але й в кожній із сфер суспільного життя відносини також неоднорідні, тому їх також можна поділити на більш вузькі, відносно відособлені групи відносин, які мають свої особливості, а отже, і певну функціональну самостійність. А це, в свою чергу, зумовлює необхідність і в рамках кожної галузі права виділяти відокремлені групи правових норм, що регулюють ці відокремлені групи суспільних відносин. Такі групи норм у межах конкретної галузі права, що регулюють якісно однорідні групи суспіль-

них відносин певного виду, становлять правовий інститут. *Правовий інститут – це група правових норм конкретної галузі права, що врегульовує певну групу функціонально однорідних відносин у межах певного їх виду.*

За своїм змістом інститути права бувають прості і складні. Простий інститут включає юридичні норми однієї галузі права. Складний, або комплексний, інститут права є сукупністю норм, що входять до складу різних галузей права, але регулюють взаємозв'язані споріднені відносини. Типовим прикладом є інститут власності, який є предметом регулювання конституційного, цивільного, сімейного, адміністративного і деяких інших галузей права. В рамках складного інституту виділяють субінститути.

Якщо окремі юридичні норми є первинною клітинкою права, а правові інститути їх блоки, то галузі права утворюють цілісні, відносно замкнуті підсистеми правового регулювання. Такими є конституційне, цивільне, трудове і всі інші галузі права.

Кожна галузь права має свою специфічну структуру. Звичайно виділяють загальну та особливу частини. У загальну частину входять інститути, які містять в собі положення, що "обслуговують" всі або майже всі інститути особливої частини, оскільки дія норм загальної частини розповсюджується на всі регульовані даною галуззю відносини. Інститути загальної частини конкретизуються в інститутах її особливої частини. Така побудова системи права дозволяє виключити дублювання, усунути громіздкість юридичних конструкцій і полегшити сприйняття і вивчення галузей права.

Отже, системність права полягає в тому, що кожна правова норма належить до певного правового інституту, конкретні правові інститути утворюють конкретну галузь права (кожна галузь права, як правило, складається із цілого ряду правових інститутів), а всі разом галузі права, що діють у конкретній державі, утворюють систему права цієї держави. Таким чином, під *системою права держави* розуміють внутрішньо організацію врегульованих у законодавстві держави взаємовідносин, яка передбачає наявність та певне взаєморозташування їх до складових частин, тобто поділ врегульованих на базі права відносин на галузі та інститути, які визначають юридичні норми, зокрема щодо сфери інформаційного законодавства.

Слід мати на увазі, що система права кожної держави, яка відображає зміст і особливості суспільних відносин у цій державі, як і самі суспільні відносини, є динамічною і постійно змінюється, розвивається. Оскільки окремі суспільні відносини можуть припинятися, то це зумовлює відпадання потреби в окремих правових інститутах або галузях права. Наприклад, із зникненням колгоспів відпадає потреба в колгоспному праві. Історії права відомі такі правові інститути, як рабовласницьке, кріпосне право тощо.

Якщо виникають нові суспільні відносини, які мають свій предмет та методи правового врегулювання, то це зумовлює виникнення нових правових норм, правових інститутів і навіть галузей права. Наприклад, не так давно виникло екологічне, атомне, космічне право. Прикладом становлення нової галузі права є запровадження в Україні інформаційного права – рішенням Президії ВАК України від 21.05.2003 р. № 26-11/5 затверджений паспорт нової спеціальності 12.00.07 – інформаційне право та правова інформатика [39].

Треба підкреслити умовність поділу юридичних норм на галузі, оскільки кожна галузь права, що має відносно самостійну систему норм, взаємодіє з іншими галузями права, що й приводить до появи таких понять, як "комплексний інститут права" або "міжгалузевий правовий інститут". Саме тому всі галузі права конкретної держави і утворюють її правову систему.

Єдність галузей права обумовлюється соціально-економічними та правовими передумовами. Соціально-економічними передумовами є, насамперед, однорідність соціально-економічної системи, що обумовлює зміст системи права. Правовими передумовами є єдність правових принципів, на яких базується система права, що закріплені в міжнародно-правових документах, в конституції держави і висловлюють її суть, єдність критеріїв, покладених в основу розмежування галузей права, та єдність функцій, які виконує кожна з галузей права.

2.3. Ознаки інформаційного права

2.3.1. Предмет, методи і принципи інформаційного права

У юридичних науках основними класифікаційними ознаками частини права, що претендує на самостійність як галузь права, обов'язково є свій предмет правового регулювання та методи правового регулювання, які базуються на відповідних принципах.

Предметом інформаційного права можна вважати упорядкування та правове регулювання суспільних інформаційних відносин, які відображають специфічні умови і правила поведінки різних суб'єктів права і управління в інформаційній сфері.

Звісно, що інформація завжди була та є об'єктом інформаційних відносин. Проте поява комп'ютерної техніки, інформаційно-комп'ютерних технологій та мереж сприяла підвищенню її ролі у життєдіяльності людини, суспільства та держави, привела не тільки до зміни суті, змісту і спрямованості багатьох суспільних відносин, а й до появи нового виду правових відносин – інформаційних відносин щодо електронно-інформаційного середовища. На жаль, серед учених і фахівців нема системної єдності в роботі та єдиного підходу, зокрема, до поглядів на інформаційне право та, навіть, до визначення його предмета.

Як зазначає російський вчений М.М. Рассолов у [94, с. 11], одні автори розглядають інформаційне право як нову комплексну галузь публічного права, що вивчає інформаційні відносини, які є предметом правового регулювання, а також суб'єкти інформаційних відносин і правовий режим інформаційних процесів у сучасному суспільстві [182]. Інші визначають інформаційне право як систему норм права, що регулюють суспільні відносини в інформаційній сфері суспільства і його частинах [183]. Треті стверджують, що інформаційне право – це правовий фундамент інформаційного суспільства, що формується у всіх країнах за допомогою глобальних інформаційних мереж та інших нових інформаційних технологій [91]. Четверті вважають, що інформаційне право діє лише в рамках організаційно-правових форм регламентації суспільних відносин, що виникають в процесі акумуляції, аналітичної обробки і розповсюдження інформації за допомогою електронних засобів [184]. Український вчений О.А. Баранов вважає, що інформаційне право має базуватися на таких видах відносин [185]:

- інформаційні відносини – це суспільні відносини, що мають місце в процесі створення, поширення, використання, збереження і знищення (утилізації) інформації;
- інформаційно-інфраструктурні відносини – це суспільні відносини, що мають місце в процесі забезпечення реалізації інформаційних відносин, тобто пов'язані з функціонуванням суб'єктів інформаційної інфраструктури, які надають інформаційні послуги і виконують роботи в інформаційній сфері, використовують інформаційні технології і ресурси, підтримують інформаційну безпеку тощо.

Не зважаючи на деяку різницю відносно розуміння суті інформаційного права, в наведених вище підходах є багато загального.

По-перше, визнається необхідність формування галузі права, яка в рамках інформаційного суспільства успадковує механізм інформаційно-правового регулювання відносин.

По-друге, в інформаційній сфері виділяються специфічні відносини як початкові поняття нової галузі правових знань. Вони безпосередньо пов'язані зі створенням, обробкою, використанням і розповсюдженням інформації.

І по-третє, всі вищезгадані автори виходять з актуальності соціального і юридичного аналізу суб'єктів інформаційних відносин, інформаційного обміну як такого, інформаційних мереж і нових інформаційних технологій в суспільстві.

Проте все ж таки залишається питання, що слід вкладати в зміст предмета інформаційного права.

Відштовхуючись від наведеного, можна виходити з того, що інформаційне право – це галузева юридична наука, що вивчає інформаційні відносини і інформаційну діяльність в суспільстві. При цьому правове впорядкування цих відносин і діяльності встановлює в цілому правове положення державних органів, суспільних організацій, засобів масової інформації, підприємницьких структур та інших суб'єктів, що регулюють публічні інформаційні відносини в певних сферах, а також приватноправові відносини різних суб'єктів інформаційної діяльності з громадянами.

Сьогодні ця сукупність правових норм має досить об'ємний за змістом, але слабко систематизований та узгоджений порядок щодо законів, розпоряджень, положень тощо в області права, інформатики та інформатизації. Норми інформаційних відносин охоплюють своєю регулюючою дією різноманітні "зрізи" суспільних відносин, відповідно до яких і може будуватися вся система інформаційного права і ті галузі права та розділи законодавства з якими вона пов'язана. Вони не завжди виступають в чистому вигляді. Деякі з них містять в собі положення, пов'язані з іншими галузями права: конституційним, цивільним, фінансовим, трудовим, кримінальним і т.д. Цей зв'язок необхідний, міцний і виконує істотну роль в правовому регулюванні інформаційних відносин.

Водночас, як вірно зазначив російський вчений В.А. Копилов в [92, с. 26-29], норми інформаційного права в тому або іншому вигляді активно впливають на всю соціальну сферу суспільства, пов'язану зі створенням, розповсюдженням, обробкою і споживанням інформації, а також на всю інформаційну сферу суспільства. Як сфера правового регулювання вона є сукупністю суб'єктів права, що здійснюють на основі інформаційного та іншого законодавства таку діяльність, яка дозволяє вирішувати конкретні інформаційні задачі в суспільстві, включаючи і сам механізм правового регулювання цієї сфери. Сама інформаційна сфера як об'єкт правового регулювання поділяється на п'ять таких основних наочних областей:

- створення і розповсюдження нової і похідної інформації;
- формування інформаційних ресурсів, інформаційних продуктів і надання інформаційних послуг;
- реалізація права на пошук, отримання, обробку, поширення і використання інформації;
- створення і застосування інформаційних систем, інформаційних технологій і засобів їх забезпечення;
- створення і застосування засобів і механізмів інформаційної безпеки.

З вказаного можна зробити висновок про те, що зміст інформаційного права визначає також і специфічна інформаційно-правова діяльність. З правової точки зору ця діяльність є певною сукупністю інформаційно-правових дій, що здійснюються конкретними суб'єктами і відповідно до вимог інформаційного законодавства. У цих діях є юридична мета, без констатації якої вони втрачають свій зміст. На практиці інформаційно-правова діяльність направлена на збір, обробку і поширення інформації, її оцінку, створення програмних продуктів і т. д. В процесі цієї діяльності розв'язуються цілі і

задачі правового регулювання, і в разі порушення інформаційного законодавства вживаються певні заходи.

Крім того, інформаційно-правова діяльність спрямована на забезпечення реальних умов для розвитку і захисту всіх форм власності на інформаційні ресурси, створення і вдосконалення інформаційних систем і мереж, забезпечення їх сумісності і взаємодії в єдиному інформаційному просторі України, створення умов для ефективного інформаційного забезпечення громадян та інших суб'єктів на основі державних інформаційних ресурсів, забезпечення національної безпеки та ін.

Сказане визначає наступні особливості предмету інформаційного права, покликаного здійснювати упорядкування і регулювання інформаційних відносин, а саме:

- вказаний вид відносин заснований на абсолютно нових для теорії права і держави поняттях – "дані", "комп'ютер", " інформаційно-комп'ютерні технології", "інформаційна структура", "інформаційні ресурси", "бази даних" та ін., – без яких у сучасних умовах все складніше ефективно здійснювати функціональну діяльність;
- оскільки інформація володіє унікальними якостями і властивостями, а також для кожної фізичної або юридичної особи складає основу життя і повсякденної діяльності, то кожна людина, підприємство, організація, фірма і т.д. може бути власником інформації;
- користування і розпорядження інформацією, базами даних та ін. у суспільстві реалізується через відповідних фізичних і юридичних осіб. Це потребує спеціальних норм щодо присікання порушення інформаційного, цивільного, кримінального та інших видів законодавства.

Проте особливості предмету інформаційного права зазначеним не вичерпуються. Тенденція на оновлення умов суспільного життя, ринкові відносини, що складаються в економіці, потребують створення гнучкіших систем збору, обробки, використання і поширення інформації, упровадження різноманітних інформаційно-комунікаційних систем і засобів для підвищення ефективності роботи органів державної влади, управління, правоохоронних структур, підприємств, банків тощо.

Зазначене також зумовлює необхідність подальшого дослідження предмета, методів і системи інформаційного права як юридичної науки, що формується, і як навчальної дисципліни. На наш погляд, інформаційне право повинне посісти певне місце як серед юридичних наук, так і серед навчальних дисциплін, які тією чи іншою мірою вивчають проблеми взаємодії права, інформатики й інформатизації.

При визначенні основ упорядкування і регулювання інформаційних відносин та становлення інформаційного права можна виділити чотири групи загальних юридичних наук.

Загальнотеоретичні науки – це теорія права і держави, конституційне право та ін. Наприклад, теорія права і держави на базі новітніх досягнень суспільствознавства вивчає теоретичні проблеми права і держави, необхідні для всіх юридичних наук. При цьому в рамках цієї фундаментальної галузі правознавства ставляться і висвітлюються деякі теоретичні аспекти інформації, державно-правового регулювання і права.

Галузеві юридичні науки – це цивільне, адміністративне, земельне, кримінальне право тощо. Всі ці галузеві юридичні науки в тому або іншому ступені займаються конкретними змістовними питаннями правового регулювання суспільних відносин, використовуючи при цьому свої специфічні засоби і методи дослідження. Кожна з галузевих юридичних наук є певною змістовною системою знань про сукупність тих або інших норм права, про регулювання за допомогою цих норм права конкретних суспільних відносин. Іншими словами, кожна галузева юридична наука вивчає тільки свою, відведену їй систему правових норм і регульованих цими нормами відносин: цивільне

право – систему цивільно-правових норм, що регулюють майнові й немайнові відносини в суспільстві (включаються так звані "особисті немайнові інформаційні відносини", які за кордоном розглядаються як відносини щодо "персональних даних"); адміністративне право – адміністративно-правові норми і відносини в різних областях державного управління (включаючи і деякі норми інформаційного права з адміністративним змістом); кримінальне право – систему кримінально-правових норм і їх реалізацію в боротьбі із злочинністю (включаючи норми про злочини у сфері комп'ютерних даних, які застосовуються і в рамках інформаційного права); власне інформаційне право – всю сукупність інформаційних відносин у суспільстві (включаючи і норми інформаційного змісту з інших галузей права) та ін.

Комплексні юридичні науки – це науки, які досліджують як правові, так і інші методи і засоби дослідження юридичних явищ і процесів. До таких комплексних юридичних наук можна віднести криміналістику, кримінологію, соціологію права та ін.

Прикладні юридичні науки – це науки, що обслуговують різні сфери юридичної діяльності в певних аспектах. До таких прикладних наук можна віднести судову статистику, судову медицину, судову психіатрію.

Інформаційне право, незважаючи на те, що деякі його норми застосовуються в інших галузевих юридичних науках, широко використовує ці норми в ході правової дії на інформаційні відносини і одночасно є самостійною галузевою правовою наукою та наукою про інформаційну діяльність. Щодо застосування інформаційного підходу до норм права, російський вчений Кудрявцев Ю.В. зазначає, що це "дозволяє як би з'єднати в рамках загальної моделі різноманітні явища – право, регулювання, правосвідомість, правозастосування і підвести їх під своєрідний спільний знаменник – інформацію. Це дозволяє в теорії створити достатньо стрункі модель системи, побачити раніше невідомі зв'язки і закономірності, а на практиці (враховуючи можливість кількісного виразу, інформаційних ознак) – розраховувати в майбутньому оптимальний режим функціонування права" [186].

Отже, інформаційне право як самостійна галузь знання (незалежно від того, що деякі його норми застосовуються в інших галузях права, як, скажімо, норми земельного права використовують в рамках цивільного права) розглядає і вивчає лише свою сукупність юридичних норм, актів, законів, що регулюють інформаційні відносини в суспільстві. І при цьому ця галузь права не претендує на "чужі" норми і не збирається їх "поглинати" з інших галузевих юридичних наук, кодексів і актів. Інформаційне право існує і розвивається в тісному зв'язку з останніми і сприяє вдосконаленню галузевих механізмів правової дії на суспільні відносини.

Інформаційне право, маючи свої початкові засади в теорії держави і права та будучи тісно пов'язаним з галузевими юридичними науками, підходить до предмета і об'єкта свого дослідження з самостійних позицій, відмінних від підходу до своїх об'єктів з боку інших юридичних наук. Воно включає всю сукупність норм права, що регулюють інформаційні відносини в суспільстві, і практику їх застосування, включаючи і сучасні науково-технічні, технологічні засоби і методи. При цьому предметом інформаційного права можна вважати інформаційно-правові відносини, що мають свій соціально-правовий зміст, а специфіка даних відносин обумовлена об'єктивними особливостями розвитку сучасного інформаційного середовища.

Методи інформаційного права – це засоби, прийоми і способи вивчення інформаційної діяльності, інформаційних процесів та інформаційних відносин. При цьому, посилаючись на [187], М.М. Рассолов відзначає, що "ідея адекватності предмета і методу

правового регулювання консервативна і суперечить сучасним тенденціям комплексного розвитку теорії права і законодавства" [94, с. 18].

О.А. Барапов у [188] зазначає, що "системи методів окремої галузі права – це певний набір методів, що є переважними та/або специфічними при визначенні того, яким чином або способом регулюються відносини у певній сфері суспільного життя. З цього визначення випливає те, що методи можна поділити на: *загальні*, котрі застосовуються в переважній більшості галузей права; *часткові*, що застосовуються в частині галузей права; та *індивідуальні (специфічні)*, що застосовуються тільки в конкретній галузі права. Під методом інформаційного права розуміється певний набір методів, що є переважними при визначенні того, яким чином або способом регулюються суспільні відносини в інформаційній сфері".

М.М. Рассолов у [94, с. 19-24] до методів інформаційного права відносить історичний метод і системний підхід. Історичний метод визначається конкретно-історичними, історико-емпіричними формами викладу предмета і способів правового регулювання, видів інформаційних ресурсів і користування ними, конкретних актів в області інформатики, відповідальності за порушення інформаційного законодавства. Тут важливе значення має з'ясування питання: як виникло те або інше явище щодо правового регулювання, які основні стани в своєму розвитку воно пройшло і які його історичні перспективи.

Системний підхід є сукупністю теоретичних принципів і положень, що дозволяють розглядати всі норми як систему, як єдине ціле в тісному зв'язку і взаємодії з іншими правовими нормами та інститутами, простежувати їх зміни в часі і робити обґрунтовані висновки щодо закономірностей розвитку всього механізму правового регулювання інформаційних відносин у суспільстві. Стосовно регулювання інформаційно діяльності системний підхід передбачає:

- визначення цілей даного виду правової дії з позиції правової системи в цілому;
- структурний аналіз процесу правового регулювання інформаційно-правової діяльності (суб'єктів і об'єктів, норм, зв'язків, дій та ін.);
- визначення ознак і міри впливу на цей процес зовнішнього середовища;
- дослідження процесів ухвалення і реалізації рішень в ході правового регулювання поведінки учасників інформаційних відносин;
- вживання встановлених в інформаційному законодавстві заходів до порушників норм.

До числа часткових методів інформаційного права М.М. Рассолов відносить дозвільний і обмежувально-заборонний методи, кожний з яких має свої риси і особливості застосування.

Дозвільний метод правового регулювання інформаційних відносин припускає такий зміст інформаційної діяльності даних учасників правовідносин, за якого їм надається свобода (власний розсуд) в реалізації своїх прав, цілей і задач. При цьому в ході реалізації вказаного дозвільного методу можуть застосовуватися й інші методи дії на поведінку учасників інформаційних правовідносин – делегуючий, рекомендаційний і санкціонуючий, а саме:

- делегуючий метод правового регулювання – це такий спосіб, за якого законодавець, відповідний державний орган або особа надає конкретні права і свободи учасникам інформаційних правовідносин у рамках конкретного розділу інформаційного законодавства;
- рекомендаційний метод правового регулювання інформаційних відносин виражається у тому, що законодавець надає учасникам правовідносин самим вибирати ті

або інші варіанти поведінки і згідно з цим діяти;

• санкціонуючий метод правового регулювання – це спосіб, за якого законодавець надає тому або іншому учаснику інформаційних відносин можливість самому ухвалювати рішення по проблемах, що цікавлять його, але ці рішення водночас мають бути санкціоновані у встановленому законом порядку.

Обмежувально-заборонний метод правового регулювання інформаційних відносин полягає в регламентації і встановленні суб'єктів даних правовідносин і певних заборонних заходів, які підлягають виконанню на практиці.

О.А. Баранов [188, с. 10] та В.А. Копилов [92, с. 101] виходять з того, що до загальних методів інформаційного права як комплексної галузі права варто віднести методи, що широко застосовуються і в інших галузях права, – це диспозитивний та імперативний методи. Перший з них є притаманним для приватного права (найбільш показовий приклад – цивільне право). Другий –для публічного (найбільш показовий приклад – адміністративне право).

На основі аналізу наукової літератури, інформаційного законодавства України до методів інформаційного права О.А. Баранов відносить [188, с. 11]:

- загальні: диспозитивний і імперативний; автономії і рівності сторін; індивідуальний метод регулювання;
- часткові: наказу, заборони, дозволу; узгодження, рекомендацій, координації, заохочення.

Принципи інформаційного права – це зафіксовані в правових формулах світових стандартів ідеї і положення, які визначають суть інформаційних відносин та надають системний зміст правовим нормам і інститутам в інформаційні сфері.

Згідно з М.М. Расоловим "одним из важных принципов информационного права является, на наш взгляд, *принцип приоритетности интересов государства* в определении всей государственной политики в сфере формирования информационных ресурсов и информатизации страны". Він обгрунтовує це тим, що "в соответствии со ст. 3 ФЗ Росии "Об информации, информатизации и защите информации" именно на государство возложены обязанности в области формирования информационных ресурсов и информатизации России" [94, с. 24].

До інших принципів інформаційного права вчений відносить принципи:

- "строгого соблюдения законности в информационных отношениях;
- соблюдения прав и личных интересов человека в информационном обмене;
- равенства граждан перед законом в случае совершения любых противоправных действий в сфере информации и информатизации;
- підтримка информационной безопасности;
- необходимости программно-целевого подхода к проблеме информатизации".

Згідно з В.А. Копиловим "принципы информационного права базируются на положениях основных конституционных норм (*звернемо увагу – не на законі, як у М.М. Расолова, а на Конституції прим. авт.*)..., а также на особенностях и юридических свойствах информации как объекта правоотношений" [92, с.103]. Далі вчений визначає перелік принципів, тобто:

- "приоритетность прав личности;
- свобода производства и распространения любой информации;
- запрещение производства и распространения информации, вредной для личности, общества и государства;
- свободный доступ к информации;
- полнота обработки и оперативности предоставления информации;

- законность, непротиворечивость законодательству РФ;
- ответственность за нарушение норм;
- отчуждение прав на использование согласно закону или договора;
- возможность включения в общественный оборот;
- двуединства информации и ее носителя (право собственности на информацию);
- распространения информации;
- организационная форма информации (юридического подтверждения формы представления информации);
- экземплярность информации".

О.А. Баранов у [189. с. 3-13] падає своє бачення правових принципів, що властиві інформаційному праву. Вчений пропонує "в якості базового принципу інформаційного права ...застосовувати принцип забезпечення інформаційної безпеки з урахуванням того, що забезпечення інформаційної безпеки є однією з основних атрибутивних властивостей систем, у тому числі соціальних. Цей принцип знайшов відображення в ст. 17 Конституції України: "Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу".

Похідними від цього базового принципу пропонуються наступні принципи:

- "свободи одержання і поширення інформації;
- об'єктивності, вірогідності, повноти і точності інформації;
- гармонізації інтересів особи, суспільства і держави в інформаційній діяльності;
- мінімізації негативного інформаційного впливу;
- мінімізації негативних наслідків функціонування інформаційних технологій;
- недопущення несанкціонованих поширення, використання і знищення інформації;
- невідторгаємість інформації;
- єдність і відмінність інформації і носія інформації;
- об'єктність надання інформації;
- первинність створення інформації;
- обмеження доступу до інформації;
- обов'язковість опублікування;
- гармонізація інформаційного права, всієї системи українського законодавства з міжнародним законодавством і законодавством інших країн".

Автор зауважує, що "...сформована система принципів інформаційного права не є остаточною, тому що в діалектичному процесі створення правових норм інформаційного законодавства і розвитку загальної системи права держави, правосвідомості в Україні принципи можуть піддаватися відповідним змінам як по кількості, так і по змісту".

Погоджуючись з переліком принципів інформаційного права, наданим О.А. Барановим, але враховуючи звичайне нігілістичне ставлення окремих владних осіб до права як головної категорії юриспруденції та бажаючи злагоди та порозуміння в суспільстві, вважаємо за необхідне звернути увагу не те, що будь-яка ієрархія (зокрема, переліку норм (статей) у законі) створюється для того, щоб її дотримувались. І це не дань формалізму. Це потреба в логічній систематизації, спрямованій на створення умов щодо підвищення порядності відносин у суспільстві, що сприяє можливості створення правової держави, де "право" та "проста людина" – насамперед. Зазначимо, що за ієрархією (тобто пріоритетність в застосуванні) у Конституції України має місце стаття 3 (а не стаття 17), яка визначає, що: "Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. ...Утвердження і забезпечення прав і свобод людини є головним обов'язком держави" [1]. Виходячи з цього, вважаємо, що першим принци-

ном інформаційного права повинен бути принцип пріоритетності прав людини за умов додержання балансу прав людини, суспільства і держави.

Резюмуючи зазначене вище, надамо визначення поняття "інформаційне право" – це система суспільних уявлень про духовні цінності та справедливий життєвий устрій, історично сформованих світовою цивілізацією, та сформульовані на їх основі соціальні принципи взаємостосунків у вигляді правових формул (норм права) щодо відносин суб'єктів в інформаційній сфері, які виникають у процесі створення, збирання, зберігання, користування, використання і поширення інформації, даних та інформаційних ресурсів (продуктів), що охороняються та захищаються державою у нормах інформаційного законодавства.

2.3.2. Інформаційно-правові відносини

Регулювання інформаційних відносин здійснюється за допомогою встановлення певних інформаційно-правових норм, тобто шляхом встановлення правил поведінки суб'єктів інформаційних відносин на базі положень інформаційного права. Інформаційно-правові норми регулюють взаємостосунки громадян, засобів масової інформації, організацій, фірм тощо між собою, їх взаємні права та обов'язки і в результаті цього надають цим відносинам особливий зміст, зміст інформаційно-правових відносин або інформаційних відносин. Суб'єкти таких відносин виступають як носії специфічних, інформаційних прав і обов'язків.

Отже, будь-яке положення інформаційного права реалізується за допомогою інформаційно-правових норм, зобов'язуючи учасників (суб'єктів) цих відносин до здійснення конкретних дій і надаючи конкретним особам право вимагати, керувати даними діями. Таким чином, до інформаційних відносин відносяться ті суспільні відносини, які відображають положення інформаційного права.

Інформаційні відносини поділяються на активні інформаційні дії, пасивні інформаційні дії, посередницьку інформаційно-правову роботу, допоміжні інформаційні дії, а також на організаційні майнові і немайнові відносини. У цьому аспекті підставами виникнення інформаційних відносин можуть виступати положення конституційних актів, законів, договорів або угод, заподіяння шкоди або збитку [190]. В цілому суть інформаційно-правових відносин у суспільстві можна визначити таким чином [94, с. 42]:

по-перше, інформаційні відносини визначаються об'єктивними політико-економічними відносинами, заснованими на різноманітності форм власності (зокрема і на інформацію і інформаційні технології), і є суспільними відносинами громадян, засобів масової інформації, підприємств, фірм, інших суб'єктів права;

по-друге, інформаційні відносини – це відносини між громадянами, ЗМІ, державними органами тощо, врегульовані нормами інформаційного законодавства, які відображають положення інформаційного права;

по-третє, інформаційні відносини є засобом вирішення задач в області формування єдиного інформаційно-правового простору країни, захисту прав і основоположних свобод, інформаційного обміну, підтримки інформаційної безпеки та ін.

Інформаційні відносини мають соціально-правову структуру і складаються з наступних основних компонентів: суб'єктів та об'єктів інформаційного права.

Виходячи із загальної теорії права *суб'єктами інформаційного права* є фізичні, юридичні особи і держава (ст. 7 Закону України "Про інформацію").

Фізична особа – суб'єкт інформаційного права – це конкретна людина (наприклад, автор програми, головний редактор газети, телеведучий, підприємець, просто читач, глядач та ін.), яка бажає і може брати участь в інформаційних відносинах. Залежно від складності і змісту відносин число суб'єктів може бути різним, але не меншим двох, оскільки будь-які відносини – це відносини між конкретними особами, що працюють з інформацією, або даними і, отже, тут, як мінімум, має бути дві сторони, які здійснюють свої права і обов'язки в інформаційній сфері. Причому правове положення вказаних суб'єктів тут може бути далеко не ідентичним: одні можуть виступати в ролі керівників ЗМІ, інші в ролі авторів, які мають бажання передати свої твори останнім, одні можуть здійснювати права рекламодавця, інші – вимагати розмістити їх рекламу, треті робити і те і інше. Тому громадяни, які в цьому випадку користуються встановленими в інформаційному законодавстві правами і мають відповідні обов'язки, є суб'єктами інформаційного права.

У системі інформаційно-правових відносин обов'язки і права тісно пов'язані один з одним: праву відповідають обов'язки, а обов'язку відповідає право, хто користується правами – несе і певну відповідальність, на кого покладаються обов'язки – одержує і певні права. При цьому особа може стати суб'єктом інформаційних відносин тільки тоді, коли вона володіє інформаційною правоздатністю й інформаційною дієздатністю.

Інформаційна правоздатність – це здатність суб'єкта інформаційного права (журналіста, автора програми ЕОМ тощо) мати інформаційні права і обов'язки.

Деякі інформаційні права належать громадянам через Конституцію України і для їх набуття не потрібно здійснювати дії. Такі права на свободу слова, думки і на отримання інформації. В інших випадках, для того щоб одержати певні інформаційні права, громадянину слід змінити свій статус, або стосовно нього повинні бути зроблені певні юридичні дії. Так, особа не має права заснувати ЗМІ у зв'язку з тим, що відбуває покарання в місцях позбавлення волі за вироком суду; для того, щоб одержати назване право, їй треба вийти на свободу і приступити до нормального життя.

Інформаційна дієздатність – це здатність суб'єкта інформаційного права впроваджувати своїми діями в життя інформаційні права та зобов'язання.

На відміну від правоздатності, дієздатність в інформаційній сфері виникає не у кожної людини. Дієздатність виникає у тих осіб, які через свою підготовку, здібності, посади, здоров'я та ін. за інформаційним законодавством одержують можливість особисто застосовувати свої права і брати на себе зобов'язання. Проте, наприклад, права психічнохворих можуть здійснювати за них родичі, близькі, органи, під опікою яких вони знаходяться. У всіх інших випадках, коли дієздатність громадянина не обмежена за інформаційним законодавством, дієздатність співпадає з правоздатністю і правоспроможна особа є одночасно по-своєму і дієздатною.

Юридична особа – суб'єкт інформаційного права – це організація, створена і зареєстрована у встановленому порядку (ст. 80 Цивільного кодексу України), здатна набувати інформаційних прав і зобов'язань в інформаційній сфері. Суб'єктами інформаційного права можуть бути підприємства, установи, організації, банки тощо. Вони є суб'єктами права у всіх тих інформаційних відносинах, в яких вони здійснюють свої інформаційні права й інтереси.

Юридичні особи в інформаційній сфері також наділяються правоздатністю і дієздатністю. Межа і зміст правоздатності визначаються інформаційним законодавством. Проте дієздатність юридичної особи має свою специфіку і виражається у тому, що в інформаційній сфері ці суб'єкти часто діють через своїх керівників або як колективні органи управління. Наприклад, акціонерне товариство – газета реалізує багато своїх інформаційних прав через директора, головного редактора або правління газети.

Важливим суб'єктом інформаційного права є *держава,* що має певні органи державної влади і управління, засоби масової інформації (газети, журнали, видавництва, телебачення, агентства, їх об'єднання тощо), архіви, культурні фонди, бібліотеки, банки даних та ін. Держава, виступаючи як власник основних інформаційних ресурсів і технологій, формує інформаційну політику країни, забезпечує її єдиний інформаційний простір, вирішує багато проблем у міжнародному інформаційному обміні.

Основними категоріями суб'єктів відносин в інформаційній сфері є:

- виробники інформації, інформаційних ресурсів, інформаційних продуктів, інформаційних послуг, а також інформаційних систем, технологій і засобів їх забезпечення;
- власники інформації, інформаційних ресурсів, інформаційних продуктів, інформаційних послуг, а також інформаційних систем, технологій і засобів їх забезпечення;
- споживачі інформації, інформаційних ресурсів, інформаційних продуктів, інформаційних послуг.

Об'єкти інформаційного права – це все ті матеріальні, духовні й інші соціальні блага, явища та процеси, з приводу яких суб'єкти інформаційного права вступають в інформаційно-правові відносини, що є предметом їх інтересів, прав і обов'язків.

В інформаційних відносинах об'єктами права, насамперед, є інформація, дані, бази даних, різноманітні інформаційні ресурси, програми, друковані твори, тиражі газет, книг, журналів, аудіо- і аудіовізуальні матеріали, рекламні продукти, самі комп'ютери, інформаційні системи, засоби інформатизації і зв'язку та ін. Саме ці об'єкти права часто потрапляють у поле зору інформаційних договорів, угод, спорів тощо.

Також в інформаційних відносинах об'єктом права є певні дії, вчинки і поведінка суб'єктів права. Дії, поведінка можуть бути об'єктом інформаційного права в дуже широкому спектрі різноманітних відносин. Так, органи державної влади і управління, органи місцевого самоврядування не повинні втручатися в творчу діяльність громадян і їх об'єднань, недержавних організацій культури за винятком, коли така діяльність веде до пропаганди війни, насильства, жорстокості, расової, національної, релігійної, класової нетерпимості, порнографії.

Деякі цінності можуть бути об'єктами права не у всіх інформаційно-правових відносинах, і на них накладаються певні обмеження. Так, забороняється рекламувати, передавати інформацію про продукцію, яка підлягає обов'язковій сертифікації, але що не має сертифікату відповідності; тільки за певних умов включаються у відкриті інформаційно-правові відносини відомості, що становлять державну таємницю та ін.

Право в інформаційній сфері як основа інформаційних відносин, тобто правомочність суб'єкта інформаційного права діяти за своєю програмою і вимагати діяти згідно із законом від інших, прийнято називати суб'єктивним правом. У сучасних умовах суб'єктивні інформаційні права громадян і інших учасників відносин є виразом ринкових відносин – це ті права громадян, підприємств, редакцій газет, видавництв, бібліотек та ін., що охороняються інформаційним законодавством на користь особи, держави і суспільства.

Суб'єктивне право в інформаційній сфері тісно пов'язане з положеннями інформаційного права. Якщо ті або інші дії чи факти не регламентовані відповідним положенням права, то вони не вважатимуться інформаційно-правовими відносинами і їх учасники не отримають результатів своїх поставлених цілей і задач. Суб'єктивні інформаційні права, якими користуються різні суб'єкти в ході суспільних відносин – це об'єктивні правові категорії; вони визначають об'єктивні інформаційно-правові процеси в суспільстві, виражають в інформаційних відносинах демократичні принципи і їх виконання гарантується законом.

Обов'язок суб'єкта права як компонент інформаційних відносин виражається у тому, що він покликаний діяти певним чином за принципами інформаційного права, тобто не скоювати певних дій або утримуватися від їх здійснення. Інформаційний обов'язок суб'єкта як елемент відносин – це не тільки юридичний, але й соціальний обов'язок. Він відрізняється від інших видів обов'язків (моральних, релігійних та ін.) тим, що лежить у сфері інформаційних відносин, і якщо обов'язок проігнорований, то зацікавлена особа може задіяти певні заходи державного примусу. Тобто обов'язок одного суб'єкта взаємовідносин відповідає праву іншого об'єкта взаємовідносин. Так, обов'язок виробника щодо обов'язкового вироблення та надання екземпляра документа, відповідає праву одержувача вимагати доставки вказаного документа; праву вимагати від осіб не практикувати розкриття відомостей з інформаційних систем відповідає обов'язок вчиняти подібні дій тільки згідно з законодавством.

2.3.3. Інформаційне право як наука та як навчальна дисципліна

Накопичення людством знань, що викликане взаємодією і взаємопроникненням наук, породжує нові види наукової діяльності, які прагнуть до становлення спеціалізації в обсязі нової науки і нової навчальної дисципліни. Можливість розвитку будь-якої науки передбачає наявність її автономності, самостійності функціонування. Претензії на самостійність повинні відповідати цілком певним вимогам, найважливіші з яких – реальність предмета науки і вчення, їх практична потреба, проникнення до сутності явищ предмета, що вивчається, вияв властивих закономірностей тощо. Проте будь-яка теорія спочатку є чисто описова: вона навчає тому, що є. Після цього стає порівняльною: вона порівнює вчорашні події з теперішніми. Зрештою, вона стає пояснювальною теорією. В цьому полягає еволюція будь-якої науки [199]. Не винятком з цього і юридичні науки та юридичні дисципліни.

Інформаційне право як наука. Сучасна наука щодо сфери інформаційного права та інформаційного законодавства формується на базі терміна "інформатика", який поряд с терміном "кібернетика" вживається у дослідженнях загальних закономірностей керування. Академік НАН України І.В. Сергієнко зазначає: "...інформатика розглядається передусім як наука про побудову комп'ютерних технологій. У процесі цієї побудови використовуються і методи кібернетики, і комп'ютери (чи їх комплекси), і різноманітні системи зв'язку та телекомунікаційні мережі, методи прикладної математики та математичного моделювання, системний аналіз, методи оптимізації та широкий арсенал інструментарію для розробки програмного забезпечення" [250, с. 6].

Наука щодо сфери інформаційного права досліджує принципи інформаційних відносин, систему інформаційного законодавства та норми, ефективність їх дії при застосуванні, об'єднує норми в правові інститути, прагне до кодифікування інформаційного законодавства, тобто – до оптимізації системи інформаційного законодавства.

Як зазначалось у п. 2.3.1, предметом інформаційного права є інформаційно-правові відносини, що мають свій соціально-правовий зміст. Предметом науки про інформаційне право є сама система інформаційного права та інформаційне законодавство. Інформаційне право як наука вивчає наукові проблеми формування і розвитку цієї нової системи права. Її основні напрями визначені у [92, с. 111] та передбачають:

- визначення понятійного апарату інформаційного права, основних термінів і їх дефініцій, що застосовують в системі інформаційного права;
- дослідження особливостей інформаційного права як нової галузі права;

• дослідження структури і складу інформаційного права як галузі права, вивчення взаємозв'язків цієї галузі права з іншими галузями права в загальній системі права;

• дослідження інформаційно-правових норм, їх побудови та їх оцінка;

• вивчення інформаційних відносин як відносин особливого роду, дослідження особливостей поведінки суб'єктів інформаційних правовідносин, прав, обов'язків і відповідальності осіб – учасників інформаційних відносин;

• вивчення особливостей і юридичних властивостей інформаційних об'єктів, з приводу яких виникають інформаційні відносини;

• дослідження і розробка принципів інформаційного права, особливостей застосування методів правового регулювання інформаційних відносин;

• вивчення джерел інформаційного права – інформаційного законодавства, судових рішень, інших актів правозастосування;

• систематизація і кодифікування інформаційно-правових норм, об'єднання їх в інститути і підгалузі інформаційного права;

• розробка теоретичних основ і способів формування збірника законів як основного акта кодифікації інформаційного законодавства;

• дослідження застосування і методів підвищення ефективності правових норм.

При дослідженнях інформаційного права та інформаційного законодавства застосовують методи, які є методологічною основою юридичних наук, зокрема такі, як:

• формально-догматичний метод досліджує "догму" (ідею) інформаційного права. Звичайно, при будь-яких наукових дослідженнях першим застосовується саме цей метод, який передбачає аналіз історії формування і розвитку того чи іншого аспекту предмета дослідження, його понятійного апарату, тлумачення термінів, виявлення окремих частин і окремих інститутів. Метод передбачає класифікацію і систематизацію явищ, понять, інститутів. В результаті цього дослідник надається можливість їх зіставлення, а отже, повнішого уявлення про них. За допомогою класифікації і систематизації розрізнені знання і уявлення про досліджуваний предмет упорядковуються. В результаті застосування формально-догматичного методу знання про інформаційне право приводяться в систему, одержують визначену, чітку форму їх уявлення, зручну для їх занам'ятовування і подальшого вивчення;

• порівняльно-правовий метод дослідження заснований на зіставленні двох або більше однотипних елементів інформаційного права (інститутів, понять, норм і т. п.) з елементами інших національних правових систем (американської, європейської і т. п.) з метою виявлення загальних і відмінних ознак таких елементів. Порівняння як логічний прийом припускає, що в досліджуваних елементах обов'язково є подібні складові. Таке порівняльне вивчення дозволяє одержати важливий матеріал для занозичення, класифікації і, зрештою, вдосконалення системи інформаційного права. Метод є ефективним засобом пізнання, розкриття суті інформаційно-правових явищ і положень інших національних інформаційних правових систем, виявлення їх переваг і перенесення цих переваг у національну інформаційно-правову систему;

• метод звернення до наук, що вивчають інші, суміжні галузі права, дозволяє ефективно застосовувати положення і висновки, що розробляються цими науками в системі права. Так, з метою підвищення ефективності можуть застосовуватися методи загальної теорії права, конституційного, адміністративного, цивільного, фінансового, кримінального і інших галузей права. Для дослідження інформаційного права необхідно вивчати та застосовувати методи інформатики і правової інформатики, кібернетики, семіотики і семантики;

• метод статистичної обробки зібраного матеріалу, застосування якого дозволяє виявляти особливості і повторюваність явищ, подій, фактів у системі інформаційного права;

• методи алгоритмізації і моделювання активно застосовуються для дослідження, опису структур і елементів системи інформаційного права, для опису поведінки суб'єктів інформаційних правовідносин. Застосування методів дозволяє уявляти структури і елементи інформаційного права, інформаційні процеси в зручнішому для вивчення вигляді;

• метод системного підходу може застосовуватися на всіх етапах вивчення інформаційного права, його елементів і частин як універсальний метод, заснований на докладному дослідженні всіх можливих шляхів, способів і варіантів вирішення задачі, а також наслідків від застосування методів і способів вирішення задачі дослідження.

Інформаційне право як навчальна дисципліна має на меті навчання студентів, аспірантів стосовно інформаційного права та інформаційного законодавства. Основними напрямами цього є впровадження у навчальний процес: планів та методики навчання; лекційних матеріалів і матеріалів проведення семінарів та практичних занять; підручників і методичних посібників; методології оцінки знань щодо інформаційного права та інформаційного законодавства.

Потребує відповідної уваги й питання вдосконалення процесів підготовки фахівців вищої кваліфікації – кандидатів та докторів наук з інформаційного права, зокрема, затвердження нового, окремого паспорта спеціальності, зміст та напрями дослідження якої повинні стосуватися лише проблем нової галузі права – інформаційного права (сьогодні це визначено як спеціальність 12.00.07 – адміністративне право; фінансове право; інформаційне право, за якою проводиться захист дисертацій та присудження наукових ступенів і присвоєння учених звань).

Невід'ємною складовою викладання інформаційного права є застосування інформаційно-комп'ютерних технологій в традиційному навчальному процесі і, що більш актуальне, – активізація дистанційного інтерактивного навчання.

Питання для самоконтролю

1. Стан сучасного інформаційного законодавства України та його недоліки.
2. Поняття "людина", "громадянин" і "особа", "права" і "свободи".
3. Поняття "інформація" і "дані" та відповідні до них інформаційні відносини.
4. Гносеологія категорії "право" та її визначення.
5. Поняття та динамічність у розвитку "системи права".
6. Класифікаційні ознаки галузі права.
7. Предмет, методи і принципи інформаційного права.
8. Джерела інформаційного права.
9. Інформаційно-правові відносини.
10. Суб'єкти та об'єкти інформаційного права.
11. Інформаційне право як наука та як навчальна дисципліна.

Розділ 3. ІНСТИТУТИ ІНФОРМАЦІЙНОГО ПРАВА

Як зазначалося у підрозділі 2.2.3, класифікаційною ознакою при визначенні нової галузі права є наявність у неї свого предмета та методів правового регулювання відповідних відносин. У кожній із сфер суспільного життя відносини неоднорідні, тому їх також можна поділити на більш вузькі, відокремлені групи відносин, які мають свої ознаки, а отже, і певну функціональну самостійність. Такі групи норм у межах конкретної галузі права, що регулюють однорідні групи суспільних відносин у рамках певного їх виду та функціональної спрямованості, складають правовий інститут. Таким чином, правовий інститут – це група правових норм конкретної галузі права, що врегульовує певний масив функціонально однорідних відносин у межах певного їх виду.

Питання інститутів інформаційного права в цьому дослідженні розглядається з точки зору принципів у підходах до удосконалення правового регулювання інформаційних відносин, а також щодо деяких, на наш погляд, принципових правових конструкцій, що можуть бути застосовані при систематизації та упорядкуванні усього інформаційного законодавства.

Наприкінці 1990-х – початку 2000-х рр., в Україні у аспекті спроб узгодження усіх чинних в інформаційній сфері норм та створення єдиного базового акта щодо інформаційного законодавства, було досить багато пропозицій від міністерств, комітетів та організацій стосовно необхідності створення узагальнюючого документа, що визначає основні засади державної інформаційної політики України, систему ідей, стратегію та принципи розвитку інформаційної сфери. Також у 2001 р. під керівництвом Державного комітету інформаційної політики, телебачення та радіомовлення України був розроблений проект Інформаційного кодексу України, про що йтиметься у Розділі 5 нашого дослідження.

Враховуючи погляди фахівців різних галузей господарства та громадськості, результати аналізу чинного законодавства України у сфері інформації, інформатики і інформатизації та розроблену нами схему щодо загальної структури інформаційного права (Додаток 1), яка надає можливість визначитися із основними інститутами та окреслити області функціонально-правового призначення інших інститутів, наведемо деякі узагальнення, що можуть бути корисними для удосконалення інформаційного законодавства та наступної його кодифікації.

3.1. Основні інститути

3.1.1. Засоби масової інформації

До основних законів України щодо сфери засобів масової інформації (далі – ЗМІ) відносяться:

Конституція України (ст. ст. 3, 15, 31, 34, 54);

Закон України "Про мови в Українській РСР" від 1989 р.;

Закон України "Про інформацію" від 1992 р.;

Закон України "Про друковані засоби масової інформації (пресу) в Україні" від 1992 р.;

Закон України "Про телебачення і радіомовлення" від 1993 р.;

Закон України "Про національний архівний фонд і архівні установи" від 1993 р.;

Закон України "Про інформаційні агентства" від 1995 р.;

Закон України "Про бібліотеки і бібліотечну справу" від 1995 р.;

Закон України "Про рекламу" від 1996 р.;

Закон України "Про видавничу справу" від 1997 р.;

Закон України "Про кінематографію" від 1998 р.;

Закон України "Про захист суспільної моралі" від 2004 р.;

Закон України "Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації" від 1997 р.;

Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 2007 р. та інші акти, що зазначені у [95].

Згідно з українською юридичною енциклопедією [144, с. 526] під засобами масової інформації розуміються "матеріальні та ін. носії інформації, органи та організації (юридичні особи), зареєстровані у встановленому законом порядку, які забезпечують публічне поширення друкованої та аудіовізуальної інформації". Під поняттям "масова інформація" розуміється інформація, призначена для широких мас (див. словник С.І. Ожегова [140, с. 343]). Тому, всі види діяльності, спрямовані на виробництво і публічне поширення масової інформації, та організації, що це здійснюють, підпадають під поняття як друкованих, так і електронних "засобі масової інформації".

У загальному плані функціонування і розвиток ЗМІ полягає у:

- забезпеченні конституційних гарантій свободи слова та реалізації права людини на інформацію;
- сприянні гармонізації відносин між особою і державою та громадськими структурами;
- розвитку ринку інформаційних ресурсів у поєднанні з державним регулюванням інформаційної діяльності, створенні умов для комерційної діяльності в інформаційній сфері;
- захисті авторських прав на інтелектуальну власність;
- демонополізації інформаційних служб і структур;
- удосконаленні засобів поширення інформації на базі новітніх технологій, зокрема впровадження оптико-волоконних та супутникових каналів зв'язку; створенні мультимедійних систем і мереж, розширенні можливостей медіа-індустрії;
- інтеграції України в міжнародний інформаційний простір, сприянні конвергенції ЗМІ з метою створення конкурентоспроможної інформаційної продукції на внутрішньому та зовнішньому ринках.

Розвиток у ЗМІ передбачає:

- у правовій сфері:

– удосконалення правового регулювання всієї системи друкованого та електронного інформування щодо функціонування ЗМІ як інституту інформаційного права держави;

– запобігання зловживанням правом на свободу інформації, поширенню неправдивої, неперевіреної та маніпулятивної інформації, посилення юридичної і етичної відповідальності за правопорушення в інформаційній сфері;

– підтримку розвитку ЗМІ мовами національних меншин, насамперед у місцях їх компактного проживання;

– захист журналістів і персоналу засобів масової інформації від дій, які перешкоджають виконанню ними професійних обов'язків, а також громадян, установ, підприємств і організацій від зловживань працівників ЗМІ;

- в економічній сфері:

– сприяння розвитку ринку інформаційних продуктів і послуг та електронної комерційної діяльності;

– недопущення реклами, спроможної завдавати шкоди інтересам споживачів;

– розширення доступу всіх верств населення до електронних ЗМІ, стимулювання попиту на них у суспільстві;

– утвердження принципу пріоритетності вітчизняного виробника інформпродукту в цілому; проведення виваженої цінової політики щодо ЗМІ, впровадження стратегії диференційованих цін, яка забезпечує їх доступність для соціально малозахищених верств населення, людей з обмеженими фізичними можливостями, жителів віддалених та важкодоступних районів.

• в організаційній сфері:

– створення аналітичних служб для моніторингу процесів і тенденцій у розвитку вітчизняних і зарубіжних ЗМІ та підготовки пропозицій для прийняття управлінських рішень;

– розширення застосування потенціалу ЗМІ, зокрема мультимедійних, в удосконаленні освітнього процесу; створення спеціалізованого освітнього телеканалу та культурологічних програм на телебаченні;

– підвищення ролі суспільного радіомовлення і телебачення;

– створення і розвиток електронних аналогів друкованих ЗМІ.

Правове упорядкування та регулювання інформаційних відносин у ЗМІ повинно носити комплексний системний зміст, виходячи із забезпечення прав людини і свобод за умов дотримання балансу інтересів людини, суспільства і держави, а також сприяти протидії будь-яким засобам маніпулювання свідомістю.

Основними принципами у розвитку ЗМІ мають бути:

• недопущення підпорядкування ЗМІ кон'юнктурним інтересам влади і бізнесу та посилення можливостей їх впливу на ЗМІ (тиск, постачання ЗМІ неповною, невизначеною, спотвореною або помилковою інформацією, відвертою дезінформацією, умисні недомовки, зрощення структур влади, бізнесу, преси тощо);

• регулювання рівня концентрації і монополізації ЗМІ (перешкода зменшенню незалежних джерел інформації, зосередженню ЗМІ в руках представників економічної еліти, безправ'ю журналістів і т. п.);

• коректування існуючого інформаційного законодавства щодо ЗМІ і їх відношення з державою і суспільством, зокрема у частині підвищення гарантій свободи слова, вільного поширення масової інформації, забезпечення плюралізму ЗМІ, доступу до офіційної інформації.

Повинні бути створені такі правові, організаційні, економічні і технологічні умови, за яких ЗМІ ефективно виконуватимуть функцію об'єктивного, правдивого інформування населення, соціальних інститутів і держави. Під цією точкою зору слід розглядати все існуюче і перспективне законодавство, підзаконні акти і окремі правові норми, що стосуються ЗМІ. Особлива увага має приділятися правовим положенням, що встановлюють відповідальність за правопорушення в інформаційній сфері.

Видавнича справа як комплекс взаємопов'язаних заходів (соціальних, економічних, правових, наукових, матеріально-технічних тощо) з регулювання й управління у сферах видавничій, поліграфічній та розповсюдження інформаційно-видавничої продукції спрямована, зокрема на:

• у видавництві:

– формування та оновлення національного видавничого асортименту для забезпечення потреб усіх соціальних груп українського суспільства виданнями з різних галузей знань державною мовою та мовами національних меншин;

– забезпечення високого рівня інформаційно-видавничої продукції завдяки підвищенню мовної культури і покращенню редакційної підготовки текстів;

– наповнення національного інформаційного простору суспільно важливою видавничою продукцією, переважно виданнями підручників, словників, енциклопедій, дитячою, художньою, науково-технічною, технологічною і методичною літературою;

– розвиток електронних видань, зокрема поширення інформації на компакт-дисках та інших цифрових носіях; виготовлення електронних книжок, засобів для отримання, обміну та розповсюдження інформації через Інтернет;

– розвиток всеукраїнської мережі книгорозповсюдження та державне регулювання економічними методами книжкового ринку;

• у поліграфії:

– розробку та впровадження цифрових технологій в додрукарські, друкарські і після друкарські процеси;

– збільшення обсягів виготовлення багатоколірної продукції на аркушевих і рулонних друкарських машинах;

– широке застосування офсетного плоского, флексографічного і цифрового друку;

– розробку та впровадження заходів з автоматизації формних, друкарських і брошурувально-палітурних процесів;

– створення вітчизняних екологічно чистих поліграфічних матеріалів: офсетного, книжково-журнального і газетного довговічного паперу та картону переважно з використанням вторинної сировини за технологіями обробки без хлоромістких компонентів; електронного паперу; чорних, кольорових і тріадних фарб для різних способів друку, лаків, змивних та очищувальних засобів, світлочутливих і термочутливих формних матеріалів на алюмінієвій основі, фотополімеризаційно здатних пластин, палітурних матеріалів.

Телерадіомовлення та кінематографія спрямовані, зокрема, на:

• у телерадіомовленні:

– створення служб цифрового аудіовізуального зв'язку і мовлення із запровадженням передачі й комутації цифрових сигналів у пакетному режимі;

– побудову системи інтерактивного телебачення з застосуванням прямого інтерактивного каналу сторінок телетекста, а для зворотного інтерактивного каналу телефонної мережі з орієнтацією на застосування для реалізації інтерактивних служб інших засобів, зокрема, мереж стільникового телефонного зв'язку;

– впровадження сучасних цифрових студій із застосуванням нових комп'ютерних технологій виробництва програм і сучасних методів опрацювання та накопичення інформації у форматі стиснутого цифрового телевізійного і радіомовного сигналу для передачі по розподільних електронних мережах;

– створення первинної супутникової мережі розподілу програм безпосереднього багатопрограмного цифрового телевізійного і звукового мовлення;

– використання побутового відеозапису в цифрових форматах і поширення цифрових записів програм на оптичному та магнітному носіях;

– впровадження цифрового телебачення підвищеної чіткості;

– розширення номенклатури послуг аудіовізуальних систем і служб, включаючи інтерактивні послуги, пов'язані з телезанятами, телеголосуванням, телекупівлею, іграми, банківськими операціями тощо;

• у кінематографії:

– реформування існуючої матеріально-технічної бази кінематографії, оснащення закладів кінематографії новітніми електронними цифровими технологіями виробництва і показу фільмів, переведення кінопродукції на електронні носії інформації;

– розвиток інфраструктури кінематографії в умовах ринкової економіки.

Бібліотечна, архівна та музейна справи спрямовані, зокрема на:

• у бібліотечній справі:

– переведення бібліотечних фондів на паперових носіях у електронну форму;

– створення електронних підручників, енциклопедій, словників і довідників;

– доповнення існуючої системи депозитарного зберігання друкованих видань депозитаріями комп'ютерних версій творів друку, електронних публікацій і науково та соціально значимої інформації української зони Інтернету;

– створення інтегрованого електронного довідково-пошукового апарату, що розкриватиме фонди провідних книгозбірень країни;

– організація системи дистанційного бібліотечного обслуговування;

• в архівній справі:

реалізація цільової програми створення страхового фонду документів національного архівного фонду з огляду на їх унікальність, не тиражованість і не відтворюваність;

– сприяння створенню приватних архівів з метою збирання і зберігання архівних документів недержавного походження

системне впровадження в архівну справу інформаційно-комп'ютерних технологій, оцифровування документальної спадщини, запровадження міжнародних стандартів з електронного діловодства і електронного документообігу;

• у музейній справі:

– створення матеріально-технічної бази комп'ютеризації музейної справи;

– впровадження новітніх технологій та передового дизайну в експозиційно-виставкову роботу;

– створення національної автоматизованої інформаційної системи, організацію спеціальної підтримки її мережевих потреб, що включатиме Інтернет-портал, систему музейних веб-серверів;

– створення міжмузейної комп'ютерної мережі та налагодження взаємодії з різними інформаційними системами галузевого та державного рівня, а також з Інтернет;

– організація постійно діючих віртуальних музеїв, тимчасових експозицій та виставок з можливістю їх поширення на зовнішніх фізичних носіях та засобами Інтернет;

– створення системи дистанційного експонування музейних цінностей для осіб з обмеженими фізичними можливостями.

Проте, як вважаємо, правове упорядкування та регулювання інформаційних відносин у сфері ЗМІ повинно носити комплексний, системний зміст, виходячи із забезпечення прав людини і свобод за умов дотримання балансу інтересів людини, суспільства і держави, а також сприяти протидії будь-яким засобам маніпулювання свідомістю. Новими бути створені такі правові, організаційні, економічні і технологічні умови, за яких ЗМІ ефективно виконуватимуть функцію об'єктивного, правдивого інформування населення, соціальних інститутів і держави. З цієї точки зору слід розглядати існуюче і перспективне законодавство, підзаконні акти і окремі правові норми, що стосуються ЗМІ. Особлива увага має приділятися правовим положенням, що встановлюють відповідальність за правопорушення в інформаційній сфері.

Особливе питання – про державний нагляд за ЗМІ. Не зважаючи на те, що в Україні існує Комісія з питань захисту суспільної моралі, результати її діяльності носять лише рекомендаційний зміст, що за умов поширення вульгарності, культу насильства, дурощів, завдяки наданій свободі слова, маніпулюванню свідомістю людини та ін. не сприяє підняттю "планки" моральності у суспільстві. Тобто, сучасний стан нормативно-правового регулювання у сфері ЗМІ не повною мірою відповідає інтересам зміцнення громадської злагоди української нації і потребує вжиття наукових, організаційних та методологічних заходів, спрямованих на формування системи актів, об'єднаних цілями та завданнями щодо підвищенню рівня духовності та моралі у суспільстві, за допомогою заходів покарання для правопорушників.

3.1.2. Наука та освіта

До основних законів України щодо сфери науки та освіти належать:

Конституція України (ст. 53);

Закон України "Про наукову і науково-технічну діяльність" від 1991 р.;

Закон України "Про інформацію" від 1992 р.;

Закон України "Про науково-технічну інформацію" від 1993 р.;

Закон України "Про наукову і науково-технічну експертизу" від 1995 р.;

Закон УРСР "Про освіту" від 1991 р.;

Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 2007 р. та інші акти, зазначені в [95].

В області науки має бути:

• більш значна підтримка державою національних наукових шкіл, що мають фундаментальні наукові результати світового рівня в сфері інформатики й інформатизації;

• підтримка просування кінцевих програмно-технічних продуктів вітчизняних розробки і виробництва на світовий ринок;

• розробка і реалізація процедур проведення відкритих конкурсів на розробку інформаційних і телекомунікаційних систем для державних замовників;

• забезпечення прямого конкурсного відбору виконавців державних замовлень для створення інформаційно-телекомунікаційних систем з чітким пріоритетом вітчизняних;

• регулярне проведення оцінки стану підгалузей інформаційної сфери;

• сертифікація продукції вітчизняних розробників і виробників, особливо в області створення та адаптації технологій подвійного застосування;

• підтримка і розвиток державної системи підготовки наукових кадрів і кадрів розробників та виробників різних засобів інформатизації;

• формування технопарків для створення ліцензованого новітнього програмного забезпечення, просування вітчизняних програмних продуктів на світовий ринок;

• створення електронно-обчислювальних систем нетрадиційної архітектури і систем штучного інтелекту, що акумулюють досягнення вітчизняної та світової науки і відкривають якісно нові можливості доступу до інформації та знань.

До числа першочергових заходів може бути віднесена розробка:

• критеріїв відбору перспективних тем науково-дослідних робіт;

• правових положень, спрямованих на вдосконалення порядку сертифікації продукції розробників і виробників вітчизняних програмних та технічних засобів;

• положень про пільги розробникам і виробникам вітчизняної наукоємної програмно-технічної продукції.

Розвиток новітніх систем і технологій має забезпечуватися впровадженням:

• систем цифрового аудіовізуального зв'язку і мовлення з застосуванням передачі та комутації цифрових сигналів у пакетному режимі;

• систем інтерактивного телебачення із застосуванням прямого інтерактивного каналу телетексту, зворотного інтерактивного каналу телефонної мережі, інших засобів, зокрема мереж стільникового телефонного зв'язку;

• систем цифрових студій із застосуванням комп'ютерних технологій виробництва програм і сучасних методів опрацювання та накопичення інформації у форматі ефективно стисненого цифрового телевізійного і радіомовного сигналу для передачі розподільними мережами;

• первинних супутникових мереж розподілу програм безпосереднього багато програмного цифрового телевізійного та радіомовлення;

• побутового відеозапису у цифрових форматах і поширення цифрових записів програм на оптичних і магнітних носіях;

• мультимедійних технологій та інтерактивних систем зв'язку з цифровим розподілом аудіовізуальної інформації.

В області освіти. Для забезпечення навчання повинні бути вирішені наступні завдання:

• вибір та впровадження адекватних освітнім технологіям і навчальним процесам сучасних інформаційно-комп'ютерних технологій (комп'ютерні навчальні програми, супутникове і кабельне телебачення, засоби мультимедіа тощо);

• створення загальнодоступних інформаційних ресурсів (бази і банки даних, електронні бібліотеки і т.д.), орієнтованих на вирішення освітніх задач, зокрема неприбуткових;

• створення мережі спеціалізованих освітніх центрів регіонального і міського підпорядкування, а також центрів підготовки та перепідготовки викладачів і вчителів, оснащених сучасними засобами інформатизації.

В області забезпечення сфери інформаційних послуг культурного змісту, що відповідає українським культурно-історичним традиціям, повинні розв'язуватися наступні завдання:

• розробка дешевих засобів комп'ютеризації масових бібліотек, музеїв, архівів і інших установ культури, розробка і широке впровадження засобів електронної поліграфії в практику книговидання і масового друку;

• створення загальнодоступних баз даних для гуманітарних і соціальних наук;

• створення широкої мережі культурно-інформаційних і інформаційно-розважальних центрів у регіонах, великих і малих містах, у тому числі й у країнах ближнього зарубіжжя.

• збільшення обсягів виробництва обладнання для зберігання, консервації та реставрації бібліотечних, архівних і музейних фондів, апаратури для захисту цих фондів від несанкціонованого доступу.

Розпорядженням Кабінету Міністрів України від 5.11.2008 р. № 1421-р схвалена Концепція Державної цільової науково-технічної програми впровадження і застосування грід-технологій на 2009-2013 роки. Грід-технології дають змогу виконувати велику за обсягом обробку даних у галузі науки, промисловості, соціальної сфери та створювати систему за назвою, так би мовити, обчислювальний Інтернет. До основних завдань програми віднесено, зокрема, створення національної град-інфраструктури з впровадженням комплексної системи захисту даних.

Резюмуючи викладене щодо перспектив у області освіти, зазначимо, що її інформатизація означає не просто застосування програмно-технічних засобів. Вона веде до радикальної зміни суті й організації процесів навчання і розвитку людини. Формується система безперервної, дистанційної і відкритої освіти, що базується на поєднанні мережних комп'ютерних і комунікаційних технологій, які дозволяють наблизити процес навчання до наукового пошуку і досягти головної мети сучасної освіти – сформувати професіонально компетентну, творчу особистість.

Основою нормативно-правової бази у інформаційної сфері, зокрема щодо науки та освіти, є Закон України "Про інформацію" від 1992 р. Цей закон визначає нормативні основи діяльності в усій інформаційної сфери і у свій час був дуже прогресивним. Сьогодні він потребує значного удосконалення. Головний недолік у тому, що він вже не в змозі консолідувати інформаційні відносини, які існують в галузях господарства, та врахувати зміни, що виникли у зв'язку з розвитком інформаційно-комп'ютерних технологій та мереж. Він також має значні прогалини щодо питань пов'язаних з забезпеченням прав людини і свобод стосовно маніпулювання свідомістю людини. Останнє дуже важливо з погляду того, що однією з головних цілей та завдань інформаційного законодавства є створення правових умов протидії маніпулювання свідомістю людини. Враховуючи те, що чинне інформаційне законодавство має дуже значну кількість різних за рівнем ієрархії та призначенням нормативно-правових актів, а також те, що сучасні реалії потребують створення єдиного інформаційного поля щодо традиційних відносин та відносин у зв'язку з розвитком інформаційно-комп'ютерних технологій та мереж, пропонується здійснити узагальнення, удосконалення та систематизацію інформаційних відносин у вищому за ієрархією нормативному акті – кодифікованому акті щодо інформаційної сфери.

3.1.3. Інформатизація та Національна програма інформатизації

До основних законів України щодо сфери інформатизації та Національної програми інформатизації відносяться:

Закон України "Про інформацію" від 1992 р.;

Закон України "Про Національну програму інформатизації" від 1998 р.;

Закон України "Про Концепцію Національної програми інформатизації" від 1998 р.;

Закон України "Про електронні документи та електронний документообіг" від 2003 р.;

Закон України "Про електронний цифровий підпис" від 2003 р.;

Закон України "Про телекомунікації" від 2003 р.;

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 2005 р.;

Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 2007 р. та інші акти, визначені у [95].

Згідно зі статтею 2 Закону України "Про Національну програму інформатизації" – Національна програма інформатизації визначає стратегію розв'язання проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення [30]. Національна програма інформатизації є передумовою розвитку інформаційного суспільства в Україні, що визначається Законом України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 2007 р. [37]. Цей Закон з'явився завдяки, зокрема зверненню до Президента України Громадської ради з питань інформаційно-комунікаційних технологій з пропозицією про невідкладні заходи щодо розвитку інформаційного суспільст-

ва в Україні [200]. Представники Громадської ради зазначали: "Правова неврегульованість значного кола суспільних відносин з питань інформаційного суспільства та інформаційно-комунікаційних технологій, невизначеність між українською нормативною базою та європейським законодавством створюють перешкоди на шляху розбудови інформаційного суспільства. Задля впровадження принципів правової держави в інформаційну сферу необхідне прийняття низки законопроектів, гармонізація ряду чинних законів з міжнародним законодавством, подекуди скасування чинних нормативно-правових актів, нарешті – кодифікація існуючого інформаційного законодавства".

Стратегічні завдання побудови інформаційного суспільства мають включати:

1. Реалізацію системи заходів щодо створення адекватного нормативно-правового, нормативно-технічного та інституційного забезпечення розвитку інформаційного суспільства із урахуванням світового досвіду.

2. Створення в індустрії ІКТ конкурентного середовища із прозорими правилами і гарантіями захисту прав інвесторів, що необхідно для залучення інвестицій (з боку як іноземних, так і українських інвесторів).

3. Прискорений розвиток інформаційно-комунікаційної інфраструктури країни шляхом створення належних умов для залучення значного обсягу інвестицій як з боку підприємств індустрії ІКТ, так і з боку споживачів продукції та послуг ІКТ – населення, підприємств, установ та організацій. Зниження собівартості телекомунікацій та доведення цін і тарифів на користування інформаційно-комунікаційною інфраструктурою до рівня європейських країн.

4. Поширення можливостей доступу громадян до інформаційних технологій, Інтернету та інформаційних ресурсів з метою освіти, навчання, спілкування із державними органами у рамках "електронного урядування", розвитку незалежних мас-медіа, реалізації засад громадянського суспільства. Забезпечення рівних можливостей доступу до інформації, подолання соціальних та регіональних форм інформаційної нерівності. Створення всеукраїнської мережі пунктів колективного доступу населення до ІКТ на основі співпраці між державою та підприємцями, у тому числі малим бізнесом.

5. Створення венчурної індустрії та технологічних кластерів економіки знань (експортно-орієнтована індустрія розробки програмного забезпечення) з метою реалізації інтелектуального та науково-технічного потенціалу України та зайняття нею гідного місця у міжнародному розподілі праці, розвитку освіти, запобігання відтоку висококваліфікованих спеціалістів ("відтоку мозків"), збільшення валютних надходжень.

6. Вдосконалення захисту інтелектуальної власності на програмне забезпечення та бази даних задля підвищення інвестиційної привабливості індустрії ІКТ.

7. Впровадження концепції "електронного урядування" (надання урядових послуг з застосуванням ІКТ) з метою підвищення ефективності обслуговування органами державної влади та місцевого самоврядування населення та бізнесу, зменшення корупційного фактору, посилення зв'язку між державою і громадянами, покращання іміджу державних органів серед громадян, створення засад громадянського суспільства.

8. Впровадження інформаційно-аналітичних систем та електронного документообігу в сфері державного управління задля підвищення ефективності управління і створення бази для проведення адміністративної реформи; впровадження систем управління підприємством та електронного документообігу на підприємствах – задля підвищення ефективності управління та продуктивності праці, зменшення собівартості продукції, підвищення конкурентоспроможності, збільшення надходжень до бюджету, створення нових робочих місць.

9. Впровадження систем електронного бізнесу (електронної торгівлі) задля ефективного задоволення потреб споживачів, зменшення витрат на торговельні операції та, як результат, збільшення прибутковості підприємництва, прискорення обігу грошей у банківській сфері, ефективної боротьби із зростанням цін, підвищення рівня прозорості економіки.

10. Впровадження технологій "дистанційного навчання", "телемедицини", "віддаленої роботи" задля підвищення якості освіти та охорони здоров'я, створення нових робочих місць та боротьби з бідністю, запобігання "відтоку мозків", проведення ефективної регіональної політики та вирівнювання рівнів соціально-економічного розвитку регіонів.

11. Створення масової системи освіти громадян із застосування ІКТ та пропаганди науково-технічних знань у цій сфері. Розвиток "електронної довіри" населення до можливостей ІКТ та створення належних умов безпечного користування інформаційними мережами.

12. Реалізація системи заходів, спрямованих на формування іміджу України як країни високих технологій, у якій гармонійно поєднуються духовні, інтелектуальні та науково-технічні надбання із демократичними здобутками (як для залучення іноземних інвесторів, так і для виведення на новий рівень експортно орієнтованої індустрії ІКТ, а також для збільшення довіри до українських фінансових інструментів на міжнародних фінансових ринках, протидії негативному інформаційному впливу інших країн, у перспективі – зміни ролі України у міжнародному співтоваристві).

На базі зазначених вище пропозицій Законом України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 2007 р. було визначено, що національна політика розвитку інформаційного суспільства в Україні ґрунтується на засадах: пріоритетності науково-технічного та інноваційного розвитку держави; формування необхідних для цього законодавчих і сприятливих економічних умов; всебічного розвитку загальнодоступної інформаційної інфраструктури, інформаційних ресурсів та забезпечення повсюдного доступу до телекомунікаційних послуг та ІКТ; сприяння збільшенню різноманітності та кількості електронних послуг, забезпеченню створення загальнодоступних електронних інформаційних ресурсів; поліпшення кадрового потенціалу; посилення мотивації щодо застосування ІКТ; широкого впровадження ІКТ в науку, освіту, культуру, охорону здоров'я, охорону навколишнього середовища; підтримка інформаційної безпеки. Така політика передбачає, зокрема:

1. *Перехід до пріоритетного наукового та інноваційного розвитку*, що потребує :

- впровадження ІКТ в усі сфери життєдіяльності суспільства та держави;
- координації та консолідації зусиль держави, бізнесу і громадськості щодо реалізації Основних засад та завдань з розвитку інформаційного суспільства в Україні;
- узгодженості загальнодержавних, галузевих, регіональних програм та бізнес-проектів у сфері розвитку і застосування ІКТ;
- удосконалення координації діяльності органів державної влади та органів місцевого самоврядування щодо створення елементів інформаційної інфраструктури, зокрема при побудові корпоративних інформаційно-аналітичних систем;
- створення електронних інформаційних ресурсів, які повинні застосовуватися в інформаційному обміні;
- впровадження механізмів надання органами державної влади та органами місцевого самоврядування, юридичним та фізичним особам інформаційних послуг із застосуванням Інтернет;

• усвідомлення змісту політики розвитку та становлення інформаційного суспільства в Україні керівниками громадських організацій, підприємств, установ і організацій усіх форм власності та різного підпорядкування, органів державної влади, органів місцевого самоврядування всіх рівнів;

• підвищення ролі генерального державного замовника Національної програми інформатизації; вдосконалення механізму формування і виконання цієї програми, збільшення її фінансування з включенням до складу зазначеної програми всіх проектів інформатизації, які фінансуються за рахунок коштів Державного бюджету України;

• надання державної підтримки та стимулювання впровадження ІКТ в освіту, науку, бізнес, виробництво, ринок цінних паперів, біржі (товарні, сільськогосподарські та інші) тощо;

• залучення до формування національної політики та розв'язання проблем розвитку інформаційного суспільства широкого кола фахівців із відповідних сфер (науковців, керівників, виробників, економістів, маркетологів, соціологів, викладачів тощо) і громадськості;

• спрямування зусиль органів державної влади на формування сприятливих умов для впровадження та застосування ІКТ, визначення їх у програмах розвитку України;

• пропагування переваг побудови інформаційного суспільства – від застосування можливостей ІКТ вразливими верствами населення, зокрема малозабезпеченими, людьми, що потребують соціальної допомоги та реабілітації, до створення новітніх знань та конкурентоспроможних технологій;

• включення найважливіших питань з розвитку інформаційного суспільства в Україні до програм діяльності Кабінету Міністрів України, державних програм економічного і соціального розвитку України.

2. *Законодавче забезпечення розвитку інформаційного суспільства.* З метою підвищення ефективності розвитку інформаційного суспільства необхідно створити цілісну систему законодавства, гармонізовану з нормами міжнародного права з питань розвитку інформаційного суспільства, зокрема здійснити кодифікацію інформаційного законодавства. Підготовка законопроектів повинна відбуватися з проведенням їх громадських обговорень.

При створенні інформаційного законодавства слід керуватися загальними принципами Конституції України, а також базуватися на принципах свободи створення, отримання, використання та розповсюдження інформації; об'єктивності, достовірності, повноти і точності інформації; гармонізації інтересів людини, суспільства та держави в інформаційній діяльності; обов'язковості публікації інформації, яка має важливе суспільне значення; обмеження доступу до інформації виключно на підставі закону; мінімізації негативного інформаційного впливу та негативних наслідків функціонування ІКТ; недопущення незаконного розповсюдження, використання і порушення цілісності інформації; гармонізації інформаційного законодавства та всієї системи вітчизняного законодавства.

З метою реалізації зазначених принципів необхідно підготувати та прийняти Інформаційний кодекс України, включивши до нього розділи, зокрема про засади електронної торгівлі, правову охорону прав на зміст комп'ютерних програм, удосконалення захисту прав інтелектуальної власності, в тому числі авторського права при розміщенні та використанні творів у Інтернет, про охорону баз даних, дистанційне навчання, телемедицину, надання органами державної влади та органами місцевого самоврядування юридичним та фізичним особам інформаційних послуг із застосуванням Інтернет, комерційну таємницю тощо.

Підготувати та внести зміни до законодавства з питань інформатизації, зокрема з урахуванням вимог щодо: надання органами державної влади та органами місцевого самоврядування юридичним та фізичним особам інформаційних послуг із застосуванням Інтернет; запровадження електронного документообігу та електронного цифрового підпису, дистанційного навчання, телемедицини, електронних платіжних систем, електронного бізнесу, електронних бірж, аукціонів і депозитаріїв.

3. *Формування сприятливих економічних умов розвитку інформаційного суспільства.* З урахуванням тенденцій розвитку світової економіки, які визначаються зростанням впливу ІКТ, поступовим переходом розвинутих країн від індустріальної економіки до економіки знань, основними макроекономічними завданнями у процесі розвитку інформаційного суспільства визначити:

• підвищення конкурентоспроможності національної економіки, забезпечення постійного економічного зростання держави та матеріального добробуту її громадян за рахунок впровадження ІКТ;

• забезпечення підвищення вкладу в економічне зростання держави підприємств, що провадять діяльність у сфері інформатизації, і галузей, які широко використовують ІКТ, шляхом формування збалансованої регуляторної, зокрема, податкової політики;

• сприяння підприємницькій діяльності у сфері ІКТ за рахунок формування системи адміністративних, правових і економічних механізмів, які стимулюватимуть попит на інформаційну продукцію, залучення інвестицій в ІКТ, розвитку конкуренції, просування вітчизняної продукції на міжнародний ринок.

Розглянути можливість:

• включення вартості засобів ІКТ, придбаних для особистого користування, до складу податкового кредиту при нарахуванні податку на доходи фізичних осіб;

• включення витрат, спрямованих підприємствами та організаціями на фінансування відповідних навчальних закладів та ІКТ-орієнтованих підрозділів з навчання та підвищення кваліфікації працівників сфери ІКТ, до складу валових витрат;

• розробки та впровадження стимулів для підприємств, що провадять діяльність у сфері інформатизації;

• створення бізнес-інкубаторів, технопарків, центрів високих інформаційних технологій та інших інноваційних структур та підтримки їх діяльності.

4. *Розвиток загальнодоступної інформаційної інфраструктури,* що формується шляхом:

• розвитку національної, галузевих і регіональних інформаційних систем, мереж та електронних ресурсів, інформаційно-аналітичних систем органів державної влади та органів місцевого самоврядування;

• створення вітчизняними виробниками на основі фундаментальних і прикладних досліджень новітніх конкурентоспроможних ІКТ, засобів інформатизації та комп'ютерних програм, зокрема з відкритими кодами;

• прискорення робіт, пов'язаних з розробкою, створенням та застосуванням суперкомп'ютерних систем, зокрема комп'ютерної інфраструктури на основі GRID та інших перспективних технологій;

• активізації впровадження систем електронних розрахунків за придбані товари, виконані роботи та надані послуги;

• створення в електронній формі архівних, бібліотечних, музейних фондів та інших фондів закладів культури, формування відповідних інформаційно-бібліотечних та

інформаційно-пошукових систем з історії, народної творчості, сучасного мистецтва України тощо;

• виконання зобов'язань щодо міжнародного співробітництва, спрямованого на розвиток інформаційної інфраструктури та забезпечення розширення участі України у відповідних міжнародних ініціативах.

5. *Забезпечення повсюдного доступу до телекомунікаційних послуг та інформаційних ресурсів,* що передбачає:

• створення в усіх населених пунктах України можливостей для доступу до мережі Інтернет, у тому числі шляхом розбудови мережі пунктів колективного доступу;

• прискорення проведення конверсії радіочастотного ресурсу на користь користувачів;

• визначення стратегії розвитку універсальних телекомунікаційних послуг, розгляду доцільності створення фонду універсальних послуг для забезпечення доступу малозабезпечених верств населення до цих послуг, розроблення юридичного та фінансово-економічного механізму функціонування зазначеного фонду;

• визначення найбільш сприятливих технічних, організаційних, економічних і комерційних умов взаємопідключення телекомунікаційних мереж різних операторів.

6. *Сприяння збільшенню різноманітності та кількості електронних послуг,* для чого необхідно:

• визначити статус і перелік обов'язкових електронних послуг, які повинні надаватися органами державної влади та органами місцевого самоврядування юридичним і фізичним особам, забезпечити реалізацію принципу "єдиного вікна";

• вжити додаткових заходів, спрямованих на створення сприятливих умов для надання послуг із застосуванням ІКТ, зокрема особам, які потребують соціальної допомоги та реабілітації;

• подолати відставання у впровадженні сучасних ІКТ суб'єктами господарювання, зокрема у виробництві, застосуванні технологій електронної комерції;

• сприяти діяльності існуючих та появі нових національних компаній інтеграторів, розробників програмно-апаратних комплексів у сфері електронної комерції, опрацьовувати економічні механізми стимулювання переходу до цих технологій суб'єктам середнього і малого підприємництва;

• прискорити впровадження ІКТ в аграрному секторі економіки України, передбачивши надання широкої номенклатури електронних послуг населенню сільської місцевості;

• стимулювати створення мережі навчальних центрів, курсів з вивчення особливостей електронної комерції, з перепідготовки керівників, фахівців різних сфер діяльності для роботи в нових умовах;

• підвищити ефективність та прозорість державних закупівель, передбачивши інтенсифікацію впровадження системи електронних закупівель, впровадити заходи щодо створення галузевих вертикальних Інтернет-порталів;

• забезпечити підготовку нормативно-правових актів щодо використання фізичними та юридичними особами платіжних карток з метою поширення безготівкових розрахунків в Україні та розвитку національної системи масових електронних платежів.

7. *Створення загальнодоступних електронних інформаційних ресурсів,* для цього забезпечити:

• зменшення нерівності в доступі до інформаційних ресурсів, насамперед осіб, які потребують соціальної допомоги та реабілітації, малозабезпечених верств населення, селян;

• гідну інформаційну ідентифікацію України у глобальному Інтернет-просторі;

• генерування національних інформаційних ресурсів в економічній, науково-технічній, соціальній, національно-культурній сферах, охороні довкілля тощо, звернувши особливу увагу на організацію української лінгвістичної системи та українського лінгвістичного порталу в Інтернет;

• відповідність електронних інформаційних ресурсів стандартам і технічним регламентам, загальнодержавним, галузевим та локальним класифікаторам і довідникам;

• створення системи центрів даних, що надають послуги з їх зберігання і захисту, створення віртуальних серверів, веб-хостингу тощо;

• сприяння демократичним перетворенням у суспільстві шляхом забезпечення доступу населення до інформаційних ресурсів і систем надання інформаційних послуг органами державної влади та органами місцевого самоврядування із застосуванням Інтернет, зокрема шляхом оприлюднення проектів відповідних нормативно-правових актів, впровадження нових форм взаємодії з громадськістю із застосуванням ІКТ (стосовно опитувань, консультацій, громадських експертиз тощо);

• створення необхідної технічної і технологічної інфраструктури, електронних інформаційних ресурсів в архівах, бібліотеках та музеях, науково-дослідних установах з визначенням вимоги щодо обов'язкового зберігання в єдиному електронному форматі результатів наукової діяльності та забезпечити вільний доступ до результатів наукових досліджень, створених за рахунок коштів Державного бюджету України;

• збереження в електронному вигляді рідкісних даних, що зберігаються на носіях, які можуть зіпсуватися чи зруйнуватися, із визначенням умов їх збереження;

• визначення юридичного статусу засобів масової інформації, що створюють виключно електронні інформаційні ресурси;

• формування сприятливих умов співпраці держави та приватного сектору економіки при створенні загальнодоступних електронних ресурсів.

8. *Підготовка людини для роботи в інформаційному суспільстві.* Однією з головних умов успішної реалізації Основних засад є забезпечення навчання, виховання, професійної підготовки людини для роботи в інформаційному суспільстві. Для цього необхідно:

• розвивати національний науково-освітній простір, який ґрунтуватиметься на об'єднанні різних національних багатоцільових інформаційно-комунікаційних систем;

• розробити методологічне забезпечення застосування комп'ютерних мультимедійних технологій при викладанні шкільних предметів та дисциплін, врахування в системах навчання студентів педагогічних вищих навчальних закладів і перепідготовки вчителів особливостей роботи з ІКТ;

• забезпечити пріоритетність підготовки фахівців з ІКТ;

• вдосконалити навчальні плани, відкрити нові спеціальності з новітніх ІКТ, втілити принцип "освіта протягом усього життя";

• створити системи дистанційного навчання та забезпечити на їх основі ефективне впровадження із застосуванням ІКТ на всіх освітніх рівнях усіх форм навчання;

• забезпечити на відповідному рівні навчальні заклади та наукові установи сучасними економічними та ефективними засобами ІКТ і необхідними інформаційними ресурсами;

• забезпечити вільний доступ до засобів ІКТ та інформаційних ресурсів, особливо у сільській місцевості та важкодоступних населених пунктах;

• підвищити на засадах співпраці приватного сектору економіки та органів місцевого самоврядування комп'ютерну грамотність населення, зокрема пенсіонерів, малозабезпечених, людей, що потребують соціальної допомоги та реабілітації, селян;

• забезпечити розвиток національної науково-освітньої інформаційної мережі та інформаційних ресурсів за головними галузями знань, її приєднання, зокрема, до європейських науковоосвітніх мереж.

9. *Створення системи мотивацій щодо впровадження і застосування ІКТ.* З цією метою необхідно:

• забезпечити комп'ютерну та інформаційну грамотність як основу розбудови інформаційного суспільства та сприяння розвитку людського потенціалу, звернувши особливу увагу на організацію допомоги пенсіонерам, малозабезпеченим, людям, що потребують соціальної допомоги та реабілітації, селянам;

• розробити систему адміністративних, правових та економічних заходів, які стимулюють попит на інформаційну продукцію;

• сприяти підвищенню рівня життя кожній людини за рахунок застосування ІКТ, зокрема суттєвого розширення номенклатури надання відповідних електронних послуг населенню; проводити дослідження щодо можливостей ІКТ для поліпшення якості життя людей;

• поліпшити рівень комп'ютерної та інформаційної грамотності державних службовців, проводити їх періодичну атестацію і заохочувати працівників, які активно застосовують ІКТ у професійній діяльності;

• постійно вивчати та оприлюднювати результати застосування ІКТ у повсякденному житті людини, що дасть змогу своєчасно приймати певні політичні рішення, вносити необхідні корективи до відповідних стратегій і програм розвитку, зокрема – Основних засад.

10. *Наука та культура в інформаційному суспільстві.* Особливу увагу в розбудові інформаційного суспільства необхідно приділити випереджальному розвитку фундаментальних і прикладних досліджень та наукомістких технологій, розвитку вітчизняної індустрії програмування, інфраструктури виробництва ІКТ.

З метою підвищення ефективності науки та культури в інформаційному суспільстві вважати пріоритетними:

• проведення фундаментальних та прикладних досліджень з питань розвитку інформаційного суспільства;

• збереження і розвиток культурної, мовної, конфесійної різноманітності та культурних надбань в межах інформаційного суспільства, що задекларовано у відповідних документах ООН, зокрема в Загальній декларації ЮНЕСКО про культурне різноманіття;

• запровадження ІКТ у бібліотеках, архівах, музеях та інших закладах культури, що сприятиме забезпеченню повного і постійного доступу населення до надбань культури, писемності, традицій та звичаїв усіх корінних народів і національних меншин України;

• переведення в електронну форму національних надбань у сфері культури та мистецтва;

• залучення можливостей вітчизняних програмістів для розроблення і поширення програмного забезпечення із застосуванням української мови, мов національних меншин України для більш повного залучення до застосування ІКТ різних верств населення, зокрема пенсіонерів, малозабезпечених, людей, що потребують соціальної допомоги та реабілітації, селян.

11. *Охорона здоров'я в інформаційному суспільстві.* Залучення ІКТ для поліпшення демографічної ситуації, збереження і зміцнення здоров'я населення, підвищення якості та ефективності медико-санітарної допомоги, забезпечення соціальної справедливості та прав громадян на охорону здоров'я є одним з пріоритетних завдань для України.

Впровадження ІКТ у сферу охорони здоров'я потребує:

• заохочення до спільних дій органів державної влади та органів місцевого самоврядування, фахівців галузі охорони здоров'я, представників приватного сектору економіки із залученням міжнародних організацій з метою створення надійних, високоякісних і доступних систем телемедицини, масових електронних медичних та оздоровчих засобів для домашнього користування;

• підвищення організаційного і технологічного рівня розвитку ІКТ в охороні здоров'я, забезпечення готовності медичних працівників для роботи з ними;

• розширення можливостей надання сучасних медичних послуг, яке має відбуватися за умов нормативно-правового та методологічного визначення послуг телемедицини;

• забезпечення доступу до світових медичних знань та актуальних на місцевому рівні інформаційних ресурсів з метою підвищення ефективного виконання державних дослідницьких і профілактичних програм з охорони здоров'я (чоловіків і жінок), зокрема щодо репродуктивного здоров'я, інфекційних захворювань (СНІД, туберкульоз тощо);

• розроблення стандартів обміну медичними даними за умови забезпечення недоторканності приватного життя.

12. *Охорона навколишнього природного середовища.* Сучасний розвиток суспільства, попри всі здобутки цивілізації, поставив світ, у тому числі й Україну, перед фактом критичного зменшення (вичерпання) природних ресурсів, а також забруднення навколишнього природного середовища. Тому питання охорони довкілля набувають для людства дедалі вагомішого і важливішого значення.

Виконання поставлених завдань може бути забезпечено шляхом:

• розвитку співпраці органів державної влади та органів місцевого самоврядування з представниками громадськості, приватного сектору економіки, міжнародних екологічних організацій, вдосконалення системи управління у сфері охорони навколишнього природного середовища та стабільного використання природних ресурсів за рахунок впровадження ІКТ;

• розширення доступу громадськості до екологічної інформації, своєчасного інформування про результати регіонального екологічного аудиту та екологічного моніторингу, прийняття рішень щодо екологічних проблем і врахування інтересів громадськості при їх вирішенні.

13. *Інформаційна безпека в інформаційному суспільстві.* Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання 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.

Вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

• 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 інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

• розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Резюмуючи викладене зазначимо, що інформація поза будь-яким матеріальним виразом недоступна для законодавчого регулювання відносин суб'єктів у зв'язку з її пошуком, створенням, обробкою, поширенням, використанням тощо. Встановлюючи норми, що стосуються інформації, законодавці завжди мають на увазі цілком певні форми її уявлення, зачіпаючи тим самим сферу інформатизації. Процеси інформатизації як процеси розвитку індустріально-інформаційного виробництва в суспільстві, неможливо регулювати без орієнтації на цільове призначення інформації, що є їх продуктом. Важливість проблеми розвитку інформаційного законодавства визначається також тією обставиною, що норми законів цієї сфери істотно впливають на законодавче регулювання відносин суб'єктів у всіх сферах, областях, зрізах та інших компонентах життя суспільства. Будь-який вид відносин суб'єктів супроводжується або закінчується інформаційними та інформаційно-телекомунікаційними відносинами.

3.2. Інші інститути

3.2.1. Інтелектуальна власність

До основних законів України щодо сфери інтелектуальної власності відносяться:
Конституція України (ст. ст. 41, 54);
Закон України "Про охорону прав на винаходи і корисні моделі" від 1993 р.;
Закон України "Про охорону прав на промислові зразки" від 1993 р.;
Закон України "Про охорону прав на знаки для товарів і послуг" від 1993 р.;
Закон України "Про авторське право і суміжні права" від 1993 р. та інші акти, зазначені у [95].

Дискусії щодо інтелектуальної власності (права на об'єкти промислової власності, а також об'єкти авторського та суміжних прав) почалися задовго до появи інформаційно-комп'ютерних технологій та мереж.

Термін "інтелектуальна власність", що прийшов на зміну терміна "духовна власність", був запроваджений для задоволення насамперед економічних потреб. Вживання цього поняття правомірно, якщо поставитися до нього як до умовної категорії ("юридичної фікції"), що має економічний сенс, предметом правового регулювання якої є дії щодо створення та використання нематеріальних об'єктів – нових знань, які одержують юридичну оболонку охороноздатності. Історично право на об'єкти промислової власності було оформлене законодавчо в Англії в 1623 р. (перший патентний закон – "Статут про монополії" розробив вчений, лорд-канцлер Френсіс Бекон разом з юристом

Едуардом Кохом), значно раніше, ніж було визначено законом авторське право (перший закон про авторські права – "Статут королеви Анни", 1709 р.) [84, с. 133-138].

Згідно зі статтею 2 (VIII) Конвенції, що заснувала ВОІВ – Всесвітню організацію інтелектуальної власності (Стокгольм, 1967 р., дипломатична конференція держав-членів Паризької (1893 р.) і Бернської (1896 р.) конвенцій), юридичне визначення зазначеного терміну наступне: "інтелектуальна власність – це права, що відносяться до літературних, художніх й наукових творів, виконавчої діяльності, звукозапису, радіо- й телевізійних передач, винаходів, наукових відкриттів, промислових зразків, товарних знаків, знаків обслуговування, фірмових найменувань й комерційних позначень, а також – до захисту від недобросовісної конкуренції" [201]. У найширшому розумінні інтелектуальна власність означає: "закріплені законом права, які є результатом інтелектуальної діяльності людини в промисловій, науковій, літературній і художній сферах" [202]. Обсяг зазначених прав (виключних або невиключних) визначає сферу і час використання об'єкта творчості, що отримав від держави охоронний документ (патент, свідоцтво). Для контролю господарського обігу результатів творчості застосовують територіальні юридичні норми, що закріплюються національним і міжнародним законодавством за видами правового упорядкування відносин.

Види упорядкування відносин. Варто зазначити, що єдиної міжнародної конвенції щодо охорони (що передбачає надання державою охоронного документа – патенту або свідоцтва) інтелектуальної власності не існує. З позаминулого століття інститути патентного та авторського права не піддаються уніфікації, і єдина конвенція навряд чи буде вироблена. Тому існують два види правового упорядкування відносин, пов'язаних з різними об'єктами творчості: авторське право і право промислової власності, або патентне право. Обидва зазначених види засновані на результатах розумової праці, однак регулюють різні правовідносини, коло об'єктів їх охорони близьке, але не ідентичне.

Охорона об'єкта авторського права поширюється тільки на певні види і форми представлення інформації. Це право регулює відносини, що виникають у зв'язку з використанням творів літератури, мистецтва і науки, зокрема, з комп'ютерними програмами і базами даних. Правове упорядкування відносин щодо авторських прав передбачає наявність механізму підтримки особистих немайнових прав автора (право на ім'я, на неперекручування тексту) і механізму підтримки його майнових прав (право на використання об'єкта інтелектуальної власності та розпорядження щодо використання), що дозволяє юридично вводити в господарський обіг результат творчості.

Охорона об'єкта промислової власності поширюється на зміст інформації, обсяг якої визначається патентною формулою – коротким словесним описом, що обумовлює сутність новації, її рівень відмінності від вже відомого, і передбачає упорядкування відносин, пов'язаних з винаходами, корисними моделями, промисловими зразками, селекційними досягненнями, що повинні відповідати встановленим критеріям новизни, наукового (винахідницького) рівня і промислового застосування [203; 204].

До об'єктів промислової власності належать також засоби індивідуалізації: товарні знаки і торгові марки, знаки фірмових найменувань і найменування місць походження товарів, що оцінюються значною сумою. Прикладом такого засобу індивідуалізації, як електронна адреса окремої особи є його мережний аналог – доменне ім'я.

Сьогодні наростаючі суперечності між системою індивідуалізації у формі товарного знаку, торгової марки, фірмового найменування і системою індивідуалізації у вигляді доменних імен не дають державних гарантій захисту від недобросовісної комерційної діяльності. Нові категорії правопорушників реєструють чужі товарні знаки як назву домена і відмовляються від прав на них тільки в обмін на певні виплати значних

коштів від вартості об'єкта охорони з боку законного власника товарного знака (наприклад, вартість знака фірми "Кока-кола" – 10 тис. дол., товарного знака "Джин" – 60 тис. дол.). Власник відомої корпорації Аді Даслер не раз звертався з позовом до електронних конкурентів, захищаючи свої права на товарний знак "Adidas" [83, с. 134]. Так, існує веб-сторінка www.adidas.spb.ru. Суфікс spb.ru – це стандартне позначення для Санкт-Петербурзького регіону. Товарний знак "Adidas" належним чином зареєстрований у Російській Федерації. Звичайний відвідувач мережі вважає: є марка "Adidas", я хочу подивитися і купити товар цієї фірми, у Санкт-Петербурзі дешевше обійдеться. Він набирає домен, однак насправді, навіть якщо товар і є, то ця сторінка не має нічого спільного зі славетною фірмою. Тим самим фірма "Adidas" має реального електронного конкурента-шахрая, який порушує законодавство Росії про товарні знаки і знаки обслуговування.

За кордоном зазначені дії правопорушника становлять делікт щодо законодавства про товарні знаки і знаки обслуговування, законодавства про припинення недобросовісної конкуренції та законодавства про захист персональних даних. У деяких країнах (наприклад, Великобританія, Канада, Німеччина, Італія) несанкціоноване використання імені, тобто персональних даних, є предметом розгляду в суді не тільки згідно із законодавством про захист персональних даних, але і з законодавством про припинення недобросовісної конкуренції [206].

Як визначається у [207], в Росії судова практика у справах, пов'язаних з порушенням авторських прав в Інтернеті, практично відсутня, кількість судових розглядів украй мала, рішення суперечливі та, на наш погляд, не досить логічні. Так, на підставі рішення арбітражного суду [208] – "основна мета найменування домену (адреси) у мережі Інтернет – відрізнити одну область інформаційного простору від іншої, що домен не є ні товаром, ні послугою" корпорації "Кодак" було відмовлено в позовній вимозі про заборону використання у назві веб-сторінки (домену) тотожній назві її товарного знака.

Сформована мережна практика полягає в тому, що одержати вже існуюче доменне ім'я можна в разі згоди зацікавлених сторін. Доменне ім'я хоча і "безтілесне", але містить елементи традиційних об'єктів інтелектуальної власності. Доменні імена більш схожі з грішми і цінними паперами, що оформлюються в електронному вигляді: контроль за їх використанням може забезпечити спеціальна електронна система. Використовувати чуже доменне ім'я, не вносячи змін до DNS (реєстру), неможливо, але DNS контролюють треті особи, яких проблеми інтелектуальної власності та захисту даних, можна сказати, мало цікавлять.

Компанії-провайдери, що реєструють назви, право на їх використання надають на певний відрізок часу, після закінчення якого треба оплатити продовження послуги. Якщо оплата не зроблена, то ця назва відразу надходить у відкритий продаж, і протягом декількох годин власником цієї назви стає вже інша особа.

За пропозицією уряду США з 1998 р. ВОІВ проводить консультації по згаданих проблемах. Ця інституція вважає за необхідне розробити рекомендації для організації, що несе відповідальність за надання доменних імен в усьому світі – ICANN ("Інтернет-корпорація із надання імен і номерів"). У 1999 р. було прийняте рішення про те, що ICANN повинна запровадити процедуру однакового вирішення спорів у зв'язку з використанням доменних імен у всіх доменів першого рівня [209]: будь-який заявник, який бажає зареєструвати доменне ім'я, повинен давати згоду на застосування до нього цієї процедури в разі, якщо в нього виникне спір з власником загальновідомого товарного знака. Крім цього, ВОІВ займається питаннями врегулювання спорів відносно доменних імен, що знаходяться в наступних доменах першого рівня: .com, .net, .org, .nu. Зазначені

процедури щодо врегулювання спорів стосовно імен в інших доменах (російських – .ru, українських – .ua) поки що не передбачені.

Інша проблема. Усі згодні, що інтерактивні мультимедійні CD-ROM із текстами, звуками, фотографіями, рухливими зображеннями є результатом праці, але що це – літературна робота, аудіовізуальна робота або щось інше?

Можна дотримуватися думки, що представлення інформації в е-середовищі є результатом інтелектуальної праці. Навіть та інформація, що не відповідає нормам охороноздатності, в мережах набуває ознак об'єктів інтелектуальної власності – у неї вкладена творча праця. Це веде до того, що подібна інформація повинна охоронятися згідно із законодавством про інтелектуальну власність. Але як підходити до правового регулювання прав на гіпертекстову сторінку, що використовує широке коло елементів: текст, малюнок, товарний знак, промисловий зразок, знак найменування, аудіо, дизайн, фото та ін. зображення? Як довести свій пріоритет? Результати інтелектуальної праці можуть бути легко об'єднані в єдиний продукт, як, наприклад, на CD-ROM. Це веде до розмивання меж між різними типами і рівнями інтелектуальності робіт, а значить – до розмивання меж між видами правової охорони. Іншими словами, все упирається в проблему забезпечення доказу протиправних дій в умовах нестабільності даних (інформації в електронному вигляді). В мережах вони не підлягають індивідуалізації, у кращому випадку, вимагають великих витрат і зусиль. Правових формул, що забезпечують регуляцію суспільних інформаційних відносин, пов'язаних із використанням у мережах об'єктів інтелектуальної власності, немає. Від відповідей на поставлені питання залежать можливості реального захисту авторських і патентних прав у міжнародному масштабі.

Головне полягає в тому, що з розвитком електронно-інформаційного середовища, дигіталізації інформації (перетворення в цифрову форму) і появою мереж, що не визнають національних кордонів, наочно демонструється криза (штучність) традиційних юридичних уявлень про регулювання прав на результати інтелектуальної діяльності людини. Схоже, що, як сьогодні так і у майбутньому реалізація права авторів щодо поширення інформаційних продуктів їх творчості в мережах буде існувати тільки в юридичних текстах, але не в реальному житті. Тим більше, законодавством будь-якої країни ніколи не передбачався та не передбачається державний моніторинг порушення прав у сфері інтелектуальної власності. Це проблема зацікавлених у пошуках делікту осіб.

Функціонування прав. Авторське право припускає захист майнових і немайнових прав. До немайнових прав віднесено право на авторство, на ім'я, на оприлюднення, на захист репутації автора. Відповідно до майнових прав автор має виключне право на використання об'єкта інтелектуальної власності, іншими словами, право на відтворення, поширення, публічне виконання, переклад, переробку і продаж (введення в господарський обіг). Звідси виникло узагальнююче поняття авторського права як права автора на тиражування, тобто право на "копірайт" (від англ. – copyright). Це існує тільки в тому випадку, коли робота зафіксована в письмовій або іншій об'єктивно вираженій формі, тобто робота розміщена на матеріальному носії. Автор може тиражувати об'єкт права сам або передавати свої права на тиражування іншим особам безкоштовно або за плату. Передача прав здійснюється на підставі ліцензійного договору, у якому узгоджується обсяг прав (увесь об'єкт інтелектуальної власності або його частини, час та територія використання тощо).

Більшість конфліктів щодо прав авторів стосуються винагороди, а також втраченої ними вигоди. Автори правомірно наполягають на необхідності вказувати їх ім'я і неприпустимість перекручування змісту твору. Рідше виникають питання і вимоги щодо дотримання прав авторів на публічне виконання творів. Це пов'язано з тим, що в

цьому разі значно складніше притягти порушника прав до відповідальності, складніше довести факт вини, її обсяг.

Традиційно об'єктами авторського права не є офіційні документи (зокрема, законодавство), державні символи і знаки, твори народної творчості, повідомлення про події і факти, що мають відомий зміст. У той же час безліч інформаційних повідомлень в цифровому вигляді, що зведені в якусь базу даних, становлять інтерес і можуть вимагати не тільки їх охорони, але й захисту. При сьогоднішньому рівні технічних можливостей сконіювати з мережі базу даних не завжди можливо, тому й особливих проблем із її захистом не виникає. Проблеми можуть виникнути із захистом від копіювання окремих творів, що знаходяться в базі даних.

Звичайно, сказане стосується законодавства, що написане, доопрацьовується і затверджується людьми, які розглядають інститут інтелектуальної власності з позицій паперового документообігу, реальності існування і можливості контролю використання матеріальних носіїв. Тільки є тут одне "але", а саме: увага не звертається на те, що в е-середовищі інформаційні відносини не дуже хочуть відповідати писаним на папері правилам. Усе упирається, як уже раніше зазначалося, у проблему забезпечення доказів протиправних дій в умовах нестабільності даних. У принципі, конкретні порушення існують і будуть існувати. Але в мережах їх складно ідентифікувати з відповідними особами. Дуже складно відстежити навіть цілком легальну роботу людини, яка не хоче зробити щось протиправне. Вона працює, але працює анонімно. Її електронні сліди мало про що говорять, хоча і можуть бути доказом протиправних дій. Виникає цікавий момент – порушень немає тому, що немає юридичних конструкцій, здатних регулювати суспільні відносини. Іншими словами, виник новий світ, відмінний від реального – світ електронно-інформаційного простору, який вимагає нетрадиційних рішень у правовому упорядкуванні та регулюванні інформаційної діяльності у житті людини, суспільства і держави. Є також думка, що для майнових прав автора об'єкта творчості нинішня епоха розвитку Інтернет несе загибель. Право авторів обмежувати рух інформації, що знаходиться на чужих носіях, у тих правових формулах, у яких воно зараз існує, поступово буде відходити в минуле.

Про стан захисту. При поліграфічному виготовленні твору об'єкт авторського права захищається завдяки матеріальному носію, копіювання якого є трудомісткою справою.

Сучасні інформаційні технології копіювання дозволяють це робити легко, швидко і дешево. Чим дешевше електронне копіювання та більше народу спілкується за допомогою мереж, тим складніше не тільки утримуватися, але й просто помічати використання інтелектуальної власності.

Веб-сайти сьогодні вже прирівняні до творів літератури, науки (у тому числі комп'ютерні програми) або мистецтва. Згідно з п. 3 ст. 9 Закону України "Про авторське право і суміжні права" перед публікацією веб-сайта варто одержати свідоцтво на володіння авторськими правами або хоча б подати заявку на реєстрацію. Реєстрація визнається судом як юридична презумпція авторства, тобто вважається дійсною, якщо в судовому порядку не буде доведене протилежне. Для захисту авторських прав на програму або веб-дизайн необхідно роздрукувати на папері букво-графічний код програми (файл, написаний мовою HTML) в обсязі, що надає можливість його ідентифікувати і відрізнити від інших інформаційних продуктів. При цьому необхідно надати на депонування магнітний носій, що містить інформаційний продукт. Проте, легкість отримання інформаційних текстів за допомогою сучасних комп'ютерних засобів, інформаційних технологій та мереж зводять нанівець усі зусилля утримати владу над немаterіальним. Можна зробити доступ до тексту платним. Але відразу в е-середовищі з'явиться те ж саме, але вже безкоштовне.

Очевидно, щось не так із законами. Потрібно щось змінювати – не можна ж усіх виробників компакт-дисків, виконавців фонограм тощо записувати в злочинці. Порядні люди не зажадають чужу річ, більшість не прагне заглядати в чуже приватне листування. За безкоштовну книгу теж ніхто не агітує. Але ці ж чесні люди у своїй більшості придбають неліцензійну касету з фільмом або відішлють другові файл із книгою. У принципі, навіть розповідь по телефону змісту фільму, що сподобався, або наспівування модної пісеньки вже є предметом порушення авторського права. З цього випливає важливий висновок – інформаційне законодавство відстає від технологій. Безкоштовна книга, швидше за все, книга, за яку заплатив хтось інший. Безкоштовний файл – піди знайди, хто його власник, і навіщо взагалі його шукати...

Теоретично отут нібито все зрозуміло – коли неможливо відстежувати кожний випадок порушення закону, то такий закон не повинен існувати. Якщо принцип "невідворотності покарання" не працює в абсолютній більшості випадків, то засоби реалізації законів просто не будуть працювати. Мати закони, за якими неможливе гарантоване правозастосування – нерозумно. Якщо порушниками закону дійсно є не всі, а тільки окремі, як висловлюється міліція – "фігуранти", то потрібно змінювати закон, а не намагатися змінювати непрацюючу систему правозастосування. Не допоможуть і "показові процеси", головне, в очах громадян вони несправедливі – караються не ті, які заслуговують покарання, а тільки ті, хто потрапив під руку сучасному, вкрай, звичайно, "справедливому" українському "правосуддю".

Сьогодні в Україні більшість не дуже вірить у захист авторських прав, а меншість – намагається зберегти і нав'язати традиційне розуміння авторського права цій більшості за допомогою силових структур і "асфальтових катків". Але невдоволення існуючим порядком речей зростає, і зростає усвідомлення причин цього невдоволення. Так може продовжуватися ще кілька років, поки інформаційні технології відносно дороги, а кількість людей, що активно перебувають в мережах, ще невелика. І це не тільки наша проблема.

У 1995 р. Європейський Союз розробив рекомендації ENFOPOL про законний моніторинг мереж, що є обов'язковим для країн-членів ЄС. Документ обумовлює необхідність розробки національної нормативно-правової бази, що відповідає його положенням, регламентує методи і способи моніторингу телекомунікацій. Проте, проблема "захисту даних" продовжує мати великі складності застосування національних законів при міжнародному інформаційному обміні, який потребує уніфікованої нормативно-правової бази.

Про "посткопірайт". Звичайно люди згодні дотримуватись деяких інтересів автора: не спотворювати твір, не забувати вказувати його ім'я. Але вони хотіли б вільно копіювати твори. Існуюча концепція, що визнає немайнові права автора, але ігнорує його майнові права дістала назву "копілефта" (від англ. copyleft). І в цьому є сенс.

Зі збільшенням числа відвідувачів мереж загальноприйнята в речовому світі "тверда", підтримувана законом і судом, концепція "копірайта" зміщується у бік не менш загальновживаного "копілефта". Як вбачається, "копілефт" буде існувати не в силу закону, а в результаті дотримання "правил гарного тону", "ділової етики", тобто шляхом "саморегуляції".

Панування "копілефта" ні в якому разі не можна вважати початком анархії у відносинах між творцями і споживачами їх продукції. "Правила гарного тону", хоча і не закріплені законом, передбачають їх неухильне виконання. Їх недотримання може призвести до неприємних наслідків, як мінімум до підриву репутації. Хоча для нашої мен-

тальності "тримати слово" продовжує бути дуже значною проблемою, вирішення якої потребує часу.

З іншого боку, засоби сучасної криптографії, зокрема електронного підпису, дозволяють технологічно захистити більшість з авторських прав. Звичайно, підписаний твір можна копіювати, але зміну, що не передбачена автором цього твору, можна знайти. Та й атрибутувати підписаний твір буде простіше. Можна також вважати, що поширення концепції "копілефта за замовчуванням", перехід процедур дотримання принципів "копірайта" в розряд "правил гарного тону" та відповідна технологічна підтримка з боку криптографії може посилити можливості захисту немайнових прав автора.

Про privacy. Існує й інша концепція, що обмежує рух даних, – privacy, тобто те, що стосується прав людини і основоположних свобод, зокрема її приватного життя.

У будь-якої новації, тобто нової інформації, є автор (власник, володілець, потім розпорядник, на базі виключної або не виключної ліцензії), що має персональні дані, які, у принципі, є його власністю. Використання відомостей про автора повинно здійснюватись тільки з його дозволу. Використовувати зміст приватного листа з пікантними деталями на підставі того, що ім'я автора і текст листа не перекручені, можна тільки з дозволу авторів. Використовувати відомості щодо винаходу можна тільки з дозволу автора (власника, володільця, розпорядника), який має відповідні персональні дані, захист яких передбачений міжнародним правом. Тобто бачимо тут два інститути права, що можуть функціонувати одночасно та разом – право інтелектуальної власності та право власності на персональні дані, які можуть підкріплювати та посилювати один одного. Виходячи з зазначеного можна пропонувати – здійснити удосконалення законодавства із захисту персональних даних у плані запровадження у національне законодавство право власності людини на свої персональні дані. Це потребує створення у державі відповідного механізму захисту згідно з положеннями європейських стандартів.

3.2.2. Захист персональних даних

На другий рік після "оксамитової революції" 1991 р. Угорщина одним з перших міжнародних актів підписала та ратифікувала Конвенцію Ради Європи № 108 від 28 січня 1981 р. "Про захист прав осіб у зв'язку з автоматизованою обробкою персональних даних" [56]. У 1992 р. парламент країни прийняв базовий закон та призначив комісара із захисту персональних даних. Конституційний Суд Угорщини почав розглядати питання, зокрема щодо особистого ідентифікаційного коду [80, с. 146-153; 210].

В Україні стан справ з розв'язанням питань із захисту персональних даних згідно з положеннями європейських стандартів значно скромніший. Ще у 1994 р. була підписана "Угода про партнерство та співробітництво, яка започатковує партнерство між Європейськими Співтовариствами та їх державами-членами, з одного боку, та Україною, з іншого боку", ратифікована Законом України від 10.11.1994 р. № 237/94-ВР. У 1998 р. затверджена Стратегія інтеграції України до Європейського Союзу (Указ Президента України від 11.06.1998 р. № 615/98), де у п. 4.4. визначались етапи інтеграції щодо захисту інформації про особу. Потім була низка численних указів Президента, постанов та розпоряджень КМ України щодо концепцій та програм інтеграції, рішень "круглих столів" та парламентських слухань, а також план Мін'юсту України під назвою "План заходів щодо виконання Плану дій Україна-ЄС на 2005 рік", що передбачало ратифікацію Конвенції Ради Європи № 108 і Додаткового протоколу до неї 2001 р. з одночасним прискоренням розгляду законів та внесенням змін у законодавство, зокрема щодо захисту персональних даних.

На превеликий жаль, за 18 років державотворення питання із запровадження в Україні міжнародних принципів із захисту персональних даних практично не вирішене, незважаючи на те, що це питання в Україні дуже детально досліджено та надані законодавчі пропозиції щодо нормативно-правового, організаційного та методологічного упорядкування інформаційних відносин у цій сфері, зокрема див. [68, 80, 175, 198].

Європейська концепція. Сьогодні захист персональних даних людини є фундаментальним правом, гарантованим *Європейською Конвенцією про захист прав людини і основоположних свобод* 1950 року, стаття 8 якої проголошує: "1. Кожна людина має право на повагу до її особистого і сімейного життя, житла і таємниці кореспонденції. 2. Держава не може втручатися у здійснення цього права інакше ніж згідно із законом та у випадках, необхідних у демократичному суспільстві в інтересах національної та громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням і злочинам, для захисту здоров'я або моралі чи з метою захисту прав і свобод інших людей" [55].

Наприкінці 1970-х р. суперечність між активним впровадженням засобів автоматизованої обробки даних та їх поширенням у телекомунікаційних мережах, зловживання при використанні персональних даних, потреба у впорядкуванні експортно-імпортних операцій привели до необхідності розробки міжнародно-правового акту, який мав забезпечити узгодженість законодавств європейських країн у сфері захисту персональних даних. Комітетом Ради Європи з питань захисту даних були сформульовані принципи захисту від неправомірного збирання, обробки, зберігання та поширення персональних даних. Ці принципи 28 січня 1981 р. отримали закріплення у першій і єдиній на сьогодні міжнародній угоді – *Конвенції Ради Європи "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних"* [56] (відома як Конвенція № 108 згідно з порядком у серії Європейських договорів; далі – Конвенція РЄ № 108). Повне й безпосереднє виконання її правових норм є обов'язковим для усіх держав-членів, що її ратифікували. Координування та нагляд за цією діяльністю покладено на Комісара РЄ із захисту даних, який підпорядкований Генеральному Секретарю Ради Європи. З того часу захист персональних даних виокремився у автономний вид діяльності.

Держави, які підписали цей документ, зобов'язуються керуватися її положеннями при розгляді питань, пов'язаних із захистом персональних даних, що підлягають чи не підлягають автоматизованій обробці, як у суспільному, так і приватному секторах. Вони визначають види персональних даних, які підлягають захисту (стаття 3 Конвенції РЄ № 108).

Кожна держава-член Конвенції РЄ № 108 зобов'язана здійснити корегування національного законодавства в частині втілення принципів та поставленої мети – забезпечення на території держави-члена поваги до прав та основних свобод кожної особи незалежно від її громадянства або місця проживання (стаття 4 Конвенції РЄ № 108).

Стаття 5 Конвенції РЄ № 108 визначає принципи "якості" з точки зору законності обробки персональних даних, тобто вони:

- отримуються та обробляються правомірно та законно;
- зберігаються для визначених і законних цілей та не застосовуються у спосіб, несумісний з цими цілями;
- мають бути адекватними, відповідними, не надмірними з точки зору цілей, заради яких вони зберігаються;
- мають бути точними та, в разі необхідності, мають поновлюватися;
- зберігаються у формі, що дозволяє ідентифікувати суб'єктів даних не довше, ніж це необхідно для цілі, заради якої такі дані зберігаються.

Стаття 6 Конвенції РС № 108 передбачає особливий режим певних категорій даних, зокрема, тих, що свідчать про расову приналежність, політичні погляди або релігійні чи інші переконання, а також персональних даних, що стосуються здоров'я або статевого життя, кримінальних вчинків, з огляду на загрозу їх використання для дискримінації індивідів за тією чи іншою ознакою.

Засоби та заходи, що застосовують до таких даних, повинні передбачати безпеку персональних даних від випадкового та несанкціонованого доступу, знищення, модифікації, блокування, розповсюдження та випадкової втрати (стаття 7).

Стаття 8 Конвенції РС № 108 передбачає додаткові гарантії для суб'єкта даних для ефективної реалізації права на приватність інформації персонального змісту, які включають такі правові можливості:

- бути ознайомленим про існування файлів персональних даних, умови їх обробки, у тому числі про особу, яка визначає цілі обробки і є відповідальною за додержання правил обробки, так званого "контролера файла";
- одержувати підтвердження обробки і ознайомлюватися з самою інформацією, що обробляється;
- вимагати виправлення або знищення персональних даних, які обробляються з порушенням вказаних принципів; і нарешті,
- звертатися за правовим захистом у разі порушення відповідних прав.

Виходячи з інтересів держави допускається обмеження у правах фізичних осіб, якщо це стосується державної чи суспільної безпеки, фінансової стабільності, боротьби зі злочинністю, захисту прав та свобод інших осіб (стаття 9).

Транскордонні потоки даних мають здійснюватися за умов захисту персональних даних. Допускається обмеження цієї вимоги в разі, коли національне законодавство передбачає особливий порядок упорядкування суспільних інформаційних відносин та визначення окремих видів персональних даних у зв'язку із специфічністю деяких відомостей, крім випадків, коли законодавство іншої держави-члена має аналогічний ступінь захисту (стаття 12).

Для захисту персональних даних кожна держава-член зобов'язана призначити один або більше Уповноважених органів нагляду та направити відповідне повідомлення Генеральному секретарю Ради Європи. Завдання інституту Уповноваженого передбачають створення належного організаційно-правового регулювання діяльності щодо захисту персональних даних у країні (стаття 13).

Держави-члени зобов'язані підтримувати своїх громадян, які проживають за кордоном, і надавати допомогу Уповноваженому органу своєї держави у питаннях захисту персональних даних (статті 14 – 17).

Для обговорення проблем, що пов'язані із узгодженням позицій різних країн, діє Міжнародна конференція країн із проблем захисту інформаційних прав громадян. При ній створено декілька робочих груп, у тому числі міжнародну робочу групу із захисту персональних даних у телекомунікаціях. Основне завдання робочої групи – розробка рекомендацій з питань національного та міждержавного упорядкування відносин, які виникають при обміні персональними даними. Одинадцять рекомендацій, прийняті Кабінетом Міністрів Ради Європи, охоплюють різні напрями захисту персональних даних, а саме: № R(81)1 – автоматизовані бази медичних даних; № R(83)10 – наукові дослідження та статистика; № R(85)20 – прямий маркетинг; № R(86)1 – соціальна безпека; № R (87)15 – поліція; № R(89)2 – працевлаштування; № R(91) – передача даних суспільними установами; № R(90)19 – фінансові платежі та пов'язані з ним операції; № R(95) – телезв'язок; № R(97) – генетичні дані; № R(99)5 – Інтернет.

Таким чином, в інтересах подальшої деталізації та уніфікації національних законодавств Консультативний комітет Ради Європи у питаннях захисту персональних даних заохочує секторний (галузевий) підхід, напологливо дотримується та намагається розвивати загальні правила щодо окремих аспектів їх обробки, продовжує удосконалювати положення Конвенції РС № 108 стосовно проблем європейської інтеграції. У цьому плані Кабінет Міністрів Ради Європи затвердив *Поправки до Конвенції РС № 108 щодо приєднання до неї Європейських Співтовариств від 15.06.1999 р.* [81, с. 91-92]. Вони передбачають застосування положень Конвенції № 108 РС до даних, які стосуються груп осіб, асоціацій, фундацій, компаній, корпорацій та будь-яких інших установ, що безпосередньо чи опосередковано формуються з окремих осіб, незалежно від того, мають такі установи правосуб'єктність чи ні.

Щоб процеси торгівлі не потерпали від європейських вимог щодо захисту даних, такі держави як Австралія, Китай, Нова Зеландія, окремі країни Південної Африки стали також приймати відповідні закони з питань захисту даних. Близько 40 країн світу мають закони з питань захисту персональних даних. Але інформаційне законодавство багатьох з них має суттєві недоліки. Навіть у найбільш демократичних країнах поширеним є несанкціоноване прослуховування та інші порушення законів, що визначають порядок доступу до даних, що поширюються за допомогою електронних каналів зв'язку [211].

Додатковий протокол до Конвенції № 108 від 08.11.2001 року [81, с. 81-82]. Він конкретизує вимоги Ради Європи до держав-членів Конвенції стосовно призначення національних органів нагляду і забезпечення транскордонних потоків даних. Протокол відзначає, що орган нагляду повинен мати, зокрема, повноваження щодо розслідування і втручання в необхідних випадках, а також мати право брати участь у судових засіданнях або оповіщати судові органи про порушення національного законодавства. Орган нагляду повинний виконувати свої функції в повній незалежності.

Директиви Європейського Парламенту і Ради 95/46 ЄС [57]. Дотримуючись визначених Конвенцією РС № 108 основоположних принципів захисту даних, Європейський парламент ухвалив Директиву 95/46/ЄС "Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних" (далі Директива 95/46/ЄС). На додаток до запроваджених Конвенцією РС № 108 принципів Директива 95/46 ЄС передбачає наступне.

Так, стаття 11 встановлює, що в разі отримання персональних даних не від самого суб'єкта даних, а з інших джерел суб'єкт даних має бути сповіщеним про цілі збору і обробки, її одержувачів, наявність права доступу та виправлення даних. Стаття 12 передбачає право суб'єкта даних вимагати сповіщення третім особам про зміну, знищення чи блокування інформації, що її було сповіщено раніше. Стаття 14 надає особі право заперечувати обробці персональних даних за певних обставин та заборонити використання даних у цілях рекламної діяльності чи прямого маркетингу.

Крім того, Директива 95/46/ЄС встановлює нові правила, які до цього не містилися у Конвенції Ради Європи 1981 р. Ідеться про рішення, що їх приймають автоматизовані системи під час оцінки якостей людини на основі аналізу інформації, що стосується цієї людини. Директива 95/46/ЄС надає особам право ознайомитися з логічною формулою, що застосовується у системі (стаття 12), і право оскаржити таке рішення (стаття 15). Ці положення були запозичені з законодавства про захист персональних даних Франції, яке відображає ідею захисту людини перед "бездушною" машиною.

Директива 95/46/ЄС запроваджується процедура попереднього сповіщення контролером (особою, яка визначає цілі обробки і є відповідальною за додержання правил

обробки) про заплановану обробку наглядовій інстанцій. Відповідні відомості вносяться до реєстру, який веде наглядовий орган. Така процедура має на меті забезпечити відкритість цілей обробок і основних умов її здійснення для перевірки їх відповідності положенням національного законодавства і запобігання можливим порушенням.

Визначена також процедура попереднього контролю, за якою держави мають встановлювати, обробка яких персональних даних може мати підвищений ризик для безпеки осіб, та проводити їх перевірки до початку обробки даних (стаття 20). До того ж, запроваджується механізм внутрішнього контролю за обробкою. З цією метою контролер (особа, яка визначає цілі обробки і є відповідальною за додержання правил обробки) зобов'язаний призначити службовця, який буде контролювати додержання правил обробки. Це нововведення прийшло до тексту Директиви 95/46/СС з відповідних положень законодавства Німеччини.

Окремі вимоги встановлені щодо "вразливих даних". Дані, які за своє природою несуть підвищений ризик їх використання не на користь людині, тобто здатні завдати шкоди її основним свободам і безпеці. За загальним правилом такі дані не повинні піддаватися обробці. Стаття 8 містить загальну заборону на обробку даних, що розкривають расове або етнічне походження, політичні погляди, релігійні або філософські переконання, членство у профспілках, а також даних стосовно стану здоров'я або статевого життя суб'єкта даних.

Не менш принциповим є положення Директиви 95/46/СС про заборону передачі даних до третіх країн, що не забезпечують адекватного рівня захисту. Цим, зокрема, встановлюється, що для транскордонних потоків даних з країн Європейського Союзу від одержувача даних у третій країні вимагається надання достатніх гарантій щодо дотримання ним відповідних умов.

Директива Європейського парламенту і Ради 97/66/СС [58]. Дотримуючись визначених Конвенцією РС № 108 та уточнених Директивою 95/46/СС принципів захисту даних, Європейський парламент ухвалив Директиву 97/66/СС "Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі" (далі Директива 97/66/СС).

Директива 97/66/СС зазначає, що у телекомунікаційному секторі Європейського Співтовариства запроваджуються нові передові цифрові технології та нові телекомунікаційні послуги, які зумовлюють певні вимоги до захисту персональних даних користувача. У випадку з телекомунікаційними мережами загального користування є необхідним розробити спеціальні правові, регулятивні та технічні положення з метою захисту персональних даних. Зазначені положення повинні бути гармонізовані, щоб уникнути перешкод на внутрішньому ринку телекомунікацій та не мати перешкод на шляху поширення і розвитку телекомунікаційних послуг і мереж між державами. Враховуючи, що користувачами телекомунікаційних послуг є фізичні і юридичні особи, Директива 97/66/СС передбачає захист персональних даних як фізичних осіб, так й захист законних інтересів юридичних осіб.

Директива 97/66/СС акцентує увагу на те, що дані, які стосуються абонентів і які обробляються для встановлення дзвінків, містять інформацію про особисте життя фізичних осіб і пов'язані з правом на збереження таємниці їх листування чи пов'язані із законними інтересами юридичних осіб. Такі дані можуть зберігатися тільки тоді, коли це необхідно при наданні послуги для цілей виставляння рахунків чи розрахунків за з'єднання, і тільки протягом обмеженого часу. Будь-яка обробка, яку може здійснити постачальник загальнодоступних телекомунікаційних послуг для цілей просування на

ринку власних телекомунікаційних послуг, може дозволятися лише в разі, коли абонент надає на це згоду.

У разі недотримання прав користувачів та абонентів національне законодавство має передбачити засіб судового захисту; враховуючи, що санкції повинні накладатися на будь-яку особу, яка не дотримується національних заходів, вжитих відповідно до Директиви 97/66/СС, незалежно від того, є така особа суб'єктом приватного чи публічного права.

Найбільш важливими положеннями Директиви 97/66/СС є такі:

- положення Директиви 97/66/СС уточнюють та доповнюють Директиву 95/46/СС щодо гарантій конфіденційності зв'язку, а також передбачають захист законних інтересів абонентів-юридичних осіб у телекомунікаційних мережах (стаття 1);
- Директива 97/66/СС застосовується до обробки персональних даних у зв'язку з наданням загальнодоступних послуг у телекомунікаційних мережах загального користування, зокрема, через цифрову мережу зв'язку з комплексними послугами та цифрові мобільні мережі загального користування (стаття 3);
- постачальник загальнодоступної телекомунікаційної послуги повинен вживати відповідні технічні та організаційні заходи для гарантування безпеки своїх послуг, якщо потрібно, спільно з оператором телекомунікаційної мережі загального користування у тому, що стосується безпеки мережі (стаття 4);
- держави-члени забезпечують у національних положеннях конфіденційність зв'язку за допомогою телекомунікаційної мережі загального користування та загальнодоступних телекомунікаційних послуг. Зокрема, вони забороняють прослуховування, перехоплення, зберігання та інші види перехоплювання і нагляду за зв'язком, за винятком випадків, коли на це існує законний дозвіл (стаття 5);
- держави-члени застосовують національні положення для узгодження прав абонентів, які з'єднуються та отримують деталізовані рахунки, з правом на невтручання в особисте життя абонентів, з якими з'єднуються (стаття 7);
- персональні дані, що містяться у друкованих чи електронних телефонних довідниках, які є загальнодоступними чи надаються через довідкову службу, повинні обмежуватися тим, що необхідно для визначення певного абонента, якщо тільки абонент не надав своєї неоднозначної згоди на публікацію додаткових персональних даних. Абонент має право на безкоштовне вилучення його даних із телефонного довідника на його прохання (стаття 11);
- застосування автоматичних систем виклику без людського втручання (пристрій автоматичного виклику) чи факсимільних пристроїв (факсу) для цілей прямого маркетингу може дозволятися тільки стосовно абонентів, які дали на це попередню згоду (стаття 12);
- держави-члени можуть приймати законодавчі положення для обмеження сфери дії обов'язків та прав, коли таке обмеження є необхідним заходом для гарантування національної безпеки, громадського порядку, сприяння розслідуванню, розкриттю і переслідуванню кримінальних злочинів чи запобігання несанкціонованого застосування телекомунікаційної системи, як про це йдеться у статті 13 (1) Директиви 95/46/СС (стаття 14).

Важливим для усіх європейських стандартів у сфері захисту персональних даних є те, що визначені у них принципи стосуються питань підтримання правопорядку та національної безпеки взагалі. Так принцип заборони передачі даних до третіх країн, що не забезпечують адекватного рівня захисту, застосовується до передачі персональних даних під час правоохоронної діяльності поліцейських установ європейських країн. Відповідні вимоги щодо надання адекватного рівня захисту прав суб'єктів даних, не

нижчого за рівень захисту, передбачений вказаними європейськими стандартами, містяться в таких спеціальних міжнародних актах, як Шенгенська Конвенція [81, с. 262-272], Конвенція про Європол [81, с. 206-247] тощо. Отже, співробітництво правоохоронних органів України з поліцейськими установами і органами юстиції країн Європейського Союзу, зокрема, взаємний інформаційний обмін, неможливе, доки законодавство України в цій частині не буде приведено у відповідність до вимог Конвенції РЄ № 108 і вказаних Директив Європейського Союзу.

Захист персональних даних в Україні.

До чинних законів України, які торкаються сфери захисту персональних даних (в аспекті поняття "інформація про особу", що не одне й теж), відносяться, зокрема:

- Конституція України, у статті 32 якої проголошується: "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. Кожний громадянин має право ознайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації" [1];
- Цивільний кодекс України від 2003 р.;
- Закон України "Про інформацію" від 1992 р.,
- Закон України "Про нотаріат" від 1993 р.,
- Закон України "Про адвокатуру" від 1992 р.,
- Закон України "Про організаційно-правові основи боротьби з організованою злочинністю" від 1993 р.,
- Закон України "Про міліцію" 1991 р.,
- Закон України "Про банки і банківську діяльність" від 1991 р. та інші нормативно-правові акти чинного законодавства України, так як немає такої сфери життєдіяльності людини, суспільства або держави, де персональні дані не застосовуються.

На перший погляд, стан нормативно-правового упорядкування відносин щодо персональних даних не викликає занепокоєння, сьогодні у законодавстві України є норми, які врегульовують відносини щодо "інформації про особу". Повсякденні реалії, що постійно потребують застосування такої інформації у будь-яких справах, не дуже викликають стурбованість у зв'язку з несанкціонованим її використанням та поширенням. Усі давно звикли до цього, бо є непохитна парадигма: держава – насамперед, потім усе інше, зокрема права і основоположні свободи людини. Хоча є думка, що слід менше ідеалізувати те, що вкладається у поняття "держава", за яким стоять лише конкретні особи. Держав як утворень, призначених для примушення, багато, а Україна – одна. Зауважимо, у цій частині дослідження ми не торкаємось такого антисоціального та антидержавного явища, як маніпулювання свідомістю людини, зокрема завдяки створенню у корисних цілях так званого "негативного портрета" особи шляхом компілювання різних за призначенням, але тенденційно підібраних персональних даних. Хоча на фоні бурхливих політичних та комерційних протистоянь активно розквітають несанкціоноване збирання та продаж різних за змістом та обсягом окремих відомостей та баз персональних даних. Ця не врегульована законом комерційна діяльність не дуже

привертає до себе уваги наділених владними повноваженнями осіб тієї держави, яку вони представляють та повинні захищати, зокрема з точки зору відповідного оподаткування та поповнення бюджету.

З 1992 р. законодавство України використовує поняття "інформація про особу", а не поняття "персональні дані", як це визначено у стандартах Ради Європи та Європейського Союзу, повне й безпосереднє врахування та виконання норм яких є обов'язковим для усіх держав-членів. У Європі персональні дані – це *будь-які відомості про особу, що ідентифікована або може бути ідентифікованою*, а в Україні – це тільки *відомості у паспорті* (частина перша статті 23 Закону України "Про інформацію" від 02.10.1992 р. у ред. від 23.06.2005 р.), яким хтось надав статус "основних", хоча деякі відомості для когось є основні, а для інших можуть бути й не основні, та навпаки. Причому, далі, у частині другої ст. 23 вищезазначеного Закону, по відношенню до одного й того ж предмету правового регулювання замість слова "відомості" з'являється слово "дані". У чому різниця між "відомостями" та "даними" – кожен, мабуть, вправі вирішувати сам. Тут теж мають місце перспективи виникнення конфліктів між різними суб'єктами даних – їх власниками, володільцями, розпорядниками та, зокрема, щодо "об'єктивності" розгляду відповідних справ у судах. Це, так би мовити, перший та один з багатьох юридичних аспектів не вирішення проблеми.

Звернемо увагу на комерційний бік "медалі", про що йдеться у статті "До питання е-торгівлі та захисту персональних даних" [176]. Природно, що там, де "пахне" грошима, відразу виникає й активно розвивається відповідна комерція та злочинність. Збір, збереження і продаж персональних даних – звичайно не виняток. Раніше персональні дані накопичувалися в картотеках і державних реєстрах. Тепер вони активно обробляються в комп'ютерах у приватних і комерційних інтересах. Роблячи покупки в електронних магазинах або отримуючи дисконтні картки, споживач змушений повідомляти свої персональні дані. Власники зазначених підприємств, з одного боку, зацікавлені у відомостях про стан попиту на ринку, який може бути оцінений завдяки відомостям про покупців та потенційних споживачів їх продукції, а з іншого – не завжди забезпечують захист персональних даних людини, навіть можуть збирати та пропонувати зазначені дані для продажу й отримання іншого виду прибутку, без диверсифікації щодо номенклатури продукції. Останнє в умовах ринку – значний важіль у конкурентній боротьбі, гарантія від розорення при змінах кон'юнктури.

Більш того, процес отримання персональних даних перетворюється на окремий бізнес, метою якого є тільки збір, обробка та поширення персональних даних на комерційних засадах. Відомості про людину, її матеріальний стан, особисте життя та багато ін. відбираються з різних баз даних або шляхом пропозицій подати свої дані (для отримання бонусів, призів тощо) та реалізуються на дисках або розміщуються в Інтернеті, що є предметом несанкціонованої законом та не бажаної для людини так званої комерції. Проте частиною п'ятою статті 31 Закону України "Про інформацію" встановлено: "Всі організації, які збирають інформацію про громадян, повинні до початку роботи з нею здійснити у встановленому Кабінетом Міністрів України порядку державну реєстрацію відповідних баз даних". Головне полягає у тому, що аналогічна норма є важливою складовою європейських стандартів та національних законодавств країн світу щодо захисту персональних даних. В Україні механізм реєстрації баз персональних даних понад 18 років не має запровадження, не говорячи вже про єдину та узгоджену систему захисту персональних даних у державі, яка відповідала б принципам європейських стандартів.

Як зазначено у статті 32 Конституції України, право особи на контроль за збиранням, використанням та поширенням його даних, як складової частини права на недото-

рканність приватного життя, може обмежуватися в інтересах національної безпеки, економічного добробуту та прав людини. Боротьба із злочинністю має на меті саме захист цих цінностей, а тому обмеження права на приватність під час правоохоронної діяльності є виправданим.

Однак, з іншого боку, будь-яке обмеження права може перетворитися на його порушення, якщо законодавством детально не регламентуються умови і порядок застосування таких обмежень, не передбачаються механізм контролю і гарантії відновлення обмежених прав. Саме такі недоліки властиві чинному законодавству України в галузі регулювання обробки персональних даних правоохоронними органами. Так, наприклад, частина третя статті 32 Конституції України надає громадянам право на доступ до відомостей, що стосуються їх особисто, які не є державною або іншою захищеною законом таємницею. Цим фактично визнається, що персональні дані можуть бути віднесені до державної або іншої захищеної законом таємниці, що позбавляє громадян права на доступ до неї.

Заплутаність в питанні визначення режиму щодо персональних даних за чинним законодавством України, віднесення їх чи до відкритої, чи до конфіденційної або таємної стала однією з причин розгляду Конституційним Судом України справи № 18/203-97 від 30.10.1997 р. щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К.Г. Устименка) [80, с. 121-125].

Такий стан справ, незважаючи на який можна продовжувати нескінченно, на превеликий жаль, існує з часів проголошення незалежності України.

Як ми вже неодноразово зазначали, зокрема у [68, 80, 83, 175, 198], спроби приведення положень законодавства України у сфері захисту персональних даних у відповідність з принципами європейських стандартів здійснюються понад дванадцять років – з 1997 року.

Спочатку було визначено етапи створення та вимоги до законопроекту за умов приведення законодавства України до законодавства європейських інституцій, а саме:

- по-перше, закон про захист персональних даних повинен бути рамковим, тобто – визначати межі правового регулювання, та – базовим для корегування законодавства за галузями народного господарства;
- по-друге, так як закон покликаний вирішувати насамперед питання, які безпосередньо стосуються гуманітарних проблем захисту окремої фізичної особи, його основою повинні бути принципи, визначені у відповідному міжнародно-правовому акті щодо гуманітарних питань. У світі таким єдиним правовим актом визнана Конвенція РЄ № 108 та Додатковий протокол до неї від 08.11.2001 р.;
- по-третє, у повсякденному житті фізична особа виступає у двох іпостасях: як "людина" та як "громадянин". У принципі, для створення умов дійового захисту персональних даних у законодавстві це потребує їх розмежування.

Для створення умов дійового захисту прав людини від несанкціонованої комерційної діяльності з даними необхідно долучити безпосередньо її до процесу захисту своїх персональних даних за визначеними законом умовами. Це можливо, якщо надати людині право власності на її персональні дані (до теперішнього часу відповіді на запитання – кому належать персональні дані конкретної особи? – взагалі не маємо). Підкреслимо, зазначене право стосується лише будь-якої комерції з персональними даними фізичних осіб – збирання даних з різних джерел, створення баз персональних даних та їх поширення на комерційних засадах, здійснення чого повинно в обов'язковому порядку враховувати добре відоме оголошення: "Стій! Приватна власність. Вхід заборонено".

Діяльність держави, зокрема функціонування її правоохоронних органів, не є можливою без персональних даних. Для органів влади фізична особа виступає як "громадянин", використання даних якої повинно здійснюватися лише у межах наданих законом повноважень.

Така постановка справи, з одного боку, надає проекту стрижень (системність, логічність та перспективність), на який, як нитка на веретено, мають "накручуватися" правові формули щодо захисту персональних даних (детальне обґрунтування див. у [198]), а з іншого – ця новація у повному обсязі відповідає положенню статті 11 Конвенції РЄ № 108: "Жодне з положень цієї глави (Глава II – Основоположні принципи захисту даних – від авт.) не тлумачиться як таке, що обмежує або іншим чином перешкоджає можливості Сторони забезпечувати суб'єктам даних більший ступінь захисту, ніж передбачений цією Конвенцією" [81, с. 68];

- по-четверте, закон повинен мати чіткість у визначеннях видів діяльності та їх узгодженість. Крім цього, закон повинен мати визначення узагальнюючого терміна щодо будь-якої діяльності із захисту персональних даних (у міжнародних стандартах – це "обробка");
- по-п'яте, закон повинен бути таким, щоб його положення надавали можливість застосовувати їх до файлів персональних даних у зв'язку з автоматизованою обробкою даних за умов застосування інформаційно-комп'ютерних технологій та мереж як у державному, так й у приватному секторах;
- по-шосте, закон повинен бути базою для внесення змін та доповнень у галузеве законодавство за умов запровадження до них у подальшому відповідних положень Рекомендацій РС, а також Директив та Рекомендацій СС. Саме їх положення становлять умови деталізації у регулюванні відносин у тій або іншій галузі. Виконання цього етапу можна вважати кінцевою метою у створенні правового фундаменту, який спирається на світові принципи приведення усього законодавства із захисту персональних даних в Україні у відповідність до вимог законодавства європейських інституцій;
- по-сьоме, після введення закону в дію є необхідним запровадження спеціального уповноваженого органу, який повинен відповідати за остаточне приведення галузевого законодавства до європейських стандартів та, у подальшому, здійснювати нагляд за діяльністю у сфері захисту персональних даних, що також передбачено європейськими стандартами [175].

До кінця 1999 р. проект Закону України "Про захист персональних даних" був розроблений, пройшов експертизу юристів 11 міністерств і комітетів та завізований їх керівниками (за виключенням Мін'юсту України)*. На той час проект мав 23 редакції, завдяки чому враховано понад 250 зауважень та пропозицій.

Для ознайомлення широкої громадськості з сутністю законопроекту була видана книга "Права человека и защита персональных данных" [68], кошти на яку надала Харківська правозахисна група (С. Захаров), що могло свідчити про те, що на той час українські представники Гельсінського правозахисного руху претензій до проекту не мали.

У 2000 р. проект Закону України "Про захист персональних даних" був спрямований до Кабінету Міністрів України (вих. Держкомзв'язку України від 20.12.2000 р. № 9141/17-02-09).

Але у КМ України проект затримали (незважаючи на те, що раніше у профільних відділах його вивчали та претензії не виказували); уряд не виступив ініціатором внесення його до Верховної Ради України. Одна з причин цього – створення іншого, аль-

* Зміст проекту та деяка інформація про хід експертизи надана у [177].

тернативного законопроекту під назвою "Про інформацію персонального (!? *від авт.*) характеру ". Цей проект був внесений головою парламентського Комітету з питань правової політики Верховної Ради України третього скликання зареєстрований у секторі реєстрації законопроектів апарату Верховної Ради України від 12.11.2001 р. № 7432 на заміну переробленої першої версії, зареєстрованої від 25.06.2001 р. № 7432. Проект неодноразово розглядався в комітетах Верховної Ради України, але так і не був внесений на пленарне засідання. До нього було багато принципових зауважень (зокрема, від Комісара Ради Європи з питань захисту даних доктора Вольтраут Кочі), незважаючи на те, що він переробляся та перереєстровувався. Остаточне рішення Комітету Верховної Ради України з питань свободи слова та інформації – відхилити та зняти з розгляду. З сутністю деяких зауважень до вказаного законопроекту можна ознайомитися у [178, с. 52-64]. Про що може йти мова, коли автори законопроекту вважають, що "інформація" має "характер"? З будь-якого словника відомо, що останнє поняття властиво біологічним істотам. Використання його у юриспруденції – це помилка "онімії", коли одне й теж слово позначає різні речі.

Проте, навіть після зняття з розгляду вищезгаданий проект не тільки перебував на сайті ВР України у Переліку законопроектів з питань інформаційної політики, що перебувають на розгляді у ВР України, але й був розміщений за № 1 у розділі "Інформаційні ресурси". У публікаціях ЗМІ та окремих офіційних документах проект також продовжував фігурувати як єдиний та перспективний, наприклад, див. [179].

У січні 2003 р. народні депутати України Родіонов М.К, Ніколаєнко С.М., академіки НАН України Юхновський І.Р., Толочко П.П. та Ситник К.М. виступили з правом законодавчої ініціативи щодо проекту Закону України "Про захист персональних даних (вих. Держкомзв'язку України від 20.12.2000 р. № 9141/17-02-09). Законопроект був зареєстрований (від 10.01.2003 р. № 2618), розглянутий у першому читанні та прийнятий за основу Постановою ВР України від 15.05.2003 р. № 784-IV. Узагальнюючий висновок Головного науково-експертного управління Апарату Верховної Ради України: "За результатами розгляду в першому читанні проект Закону України "Про захист персональних даних" може бути взятий за основу з урахуванням викладених вище зауважень і пропозицій".

Проте, у 2005 р. у Міністерстві юстиції України створюється робоча група, до якої запросили представників недержавних організацій, що працюють у сфері захисту права на приватність. Група отримала завдання створити альтернативний, але однойменний проект Закону України "Про захист персональних даних". Протягом двох років ця група розробляла проект, але він так і не був внесений до парламенту. Громадська рада з питань інформаційно-комунікаційних технологій у доповіді Президенту України під назвою "Про невідкладні заходи щодо розвитку інформаційного суспільства в Україні" повідомляла: "Міністерством юстиції України розроблено новий законопроект з аналогічною назвою ("Про захист персональних даних" – від авт.), при цьому ігнорується законопроект № 2618, вже прийнятий Верховною Радою України. Законопроект Міністерства юстиції України розкритикований правозахисниками та професійними організаціями як корупційно небезпечний та такий, що не відповідає нормам європейського законодавства".

16 березня 2006 року Верховна Рада України у другому читанні розглянула проект Закону України "Про захист персональних даних" від 10.01.2003 р. № 2618. За результатами законопроект був прийнятий в цілому як закон. Згідно з поіменним голосуванням: "за" законопроект – 287, "проти" – 0, "утримались" – 1, "не голосувало" – 108. Рішення прийнято. Закон набирає чинності з 1 січня 2007 р. На той час проект врахував уже понад 600 зауважень та пропозицій. Безпосередньо його підтримали 18 докторів та 19 кандидатів наук.

Але… 11 квітня 2006 р. Президент України повертає закон на доопрацювання. "Серед недоліків, які унеможливили підписання закону, була концепція права власності особи на власні персональні дані, яка, на думку (радників – від авт.) Президента, суперечить Конституції України" [181].

На наш погляд, по-перше, вищезазначене формулювання не враховує положення статті 11 Конвенції РС № 108, яка, хочемо ми того чи ні, буде колись ратифікована Верховною Радою України та стане складовою частиною національного законодавства.

По-друге, слід намагатися дивитися у майбутнє електронно-інформаційного простору, де регуляція суспільних відносин має деякий інший зміст та форму, що потребує від юриспруденції нетрадиційних підходів щодо розуміння змісту права власності, у тому числі права власності на інформацію.

По-третє, щоб зрозуміти категорію "права власності особи на особисті персональні дані", треба просто запитати самого себе: що ти хочеш – щоб держава монопольно захищала твої особисті дані (що вона завжди робила, але персональні дані використовують так, як кому та де заманеться), або ти бажаєш отримати реальну юридичну нагоду самому їх захистити від свавілля чиновників та несанкціонованої комерції? Відповідає така постановка питання, зокрема, букві та духу статті 3 Конституції України чи ні? Якщо з відповіддю виникають складнощі, пропонуємо звернутися до аргументів, що зазначені, зокрема, в [175, 198].

Повернемось до хронології.

З метою оцінки зауважень у Верховній Раді України було створено робочу групу. Але ніякої оцінки не було. Було "програмування" у напрямі – про право власності людини на свої персональні дані не йдеться; персональні дані відносяться тільки до "особистих немайнових прав". Закон доопрацювали (прибрали "право власності людини на саму себе" та збільшили кількість термінів щодо інформатизації), перечитували та відправили на третє читання.

9 січня 2007 р. Третє читання та повторне голосування в цілому як закон після врахування пропозицій Президента: "за" законопроект – 329 народних депутатів України.

Але… 30 січня 2007 р. закон знову повертається до Верховної Ради України з новими зауваженнями – невідповідність закону положенням статті 32 Конституції України та міжнародно-правовим актам [215].

У статті 32 Конституції України мова йде про поняття "конфіденційна інформація про особу" (з англ. confidence – довіра). У законопроекті "Про захист персональних даних" мова йде про поняття "персональні дані" (personal data), обсяг якого більший, ніж обсяг поняття "довірча інформація" ("персональні дані" можуть бути довірчі, не довірчі, обмеженої обробки, поширення та використання, таємні тощо). Поняття "персональні дані" застосовують у міжнародних стандартах та у національних законодавствах щодо їх захисту.

Враховуючи курс країни на євроінтеграцію та виходячи з того, що правозастосовна практика повинна орієнтуватися на "букву" положень міжнародних стандартів, стаття 32 Конституції України (до речі, й ЦКУ теж) потребує коригування та приведення у відповідність до юридичної термінології, яку застосовують у зазначених стандартах.

Стосовно зауваження щодо "…невідповідності закону …міжнародно-правовим актам". Взагалі не є зрозумілим – яким конкретно положенням міжнародно-правових актів закон не відповідає? Зазначена теза не має конкретних посилок та обґрунтування, що не надає їй логічної завершеності в доказах.

На жаль, подібний стан справ щодо звичайної відсутності аргументів та доказів має та продовжує мати місце всі роки оцінки законопроекту. Так, зокрема, до 2000 р. представники Харківської правозахисної групи не виказували до нього зауважень, навіть надали кошти на видання книги щодо захисту персональних даних [68], а у серпні 2007 р. зазначають, що законопроект "абсолютно не враховував європейські стандарти із захисту персональних даних, часом плутаючи це з технічним захистом баз даних. У проекті не існувало жодних істотних гарантій збереження приватності в автоматизованих системах. Багато організацій звернулося до Президента з проханням застосувати право вето, що і було зроблено" [180].

Виникає питання – яку мету може переслідувати зазначене зауваження? Мабуть – появу "панацеї" – закону із захисту персональних даних, яка надасть відповіді на всі випадки життя, передусім щодо необмеженої свободи. Та навряд чи це можливо. Крім прав особи, є інтереси суспільства та держави, які слід враховувати, а не робити з поняття "свобода" абсолют.

Якщо є бажання "обійняти неосяжне", то слід просто переписати та консолідувати всі документи Ради Європи та Європейського Союзу щодо захисту персональних даних в один закон. Приблизні розрахунки свідчать про те, що в зазначеній сфері вже є більш як 100 спеціалізованих документів (середня кількість аркушів одного з них – 20-30), не враховуючи інших євростандартів, що опосередковано стосуються захисту персональних даних. Що це буде за нормативний акт, хто його буде читати та як ним користуватися? – ось у чому питання.

Щодо тезису Харківської правозахисної групи – "у проекті не враховано питання телекомунікацій". Хто сьогодні може знати, який розвиток матиме так зване е-середовище у майбутньому? Поява нових інформаційно-комп'ютерних технологій, телекомунікаційних засобів чи нових засобів комунікації на базі біо-, біохімічних- (зокрема, на амінокислотах), нанотехнологій, суміші зазначених та невідомих поки що технологій буде завжди вимагати внесення змін у базовий закон, хоча питання може бути вирішено значно простіше – завдяки змінам у галузевому законодавстві, зокрема щодо телекомунікацій.

Тобто мова в нас іде про базовий закон, а опоненти нескінченними зауваженнями за відсутності чіткості уявлення про те, що самі хочуть, схиляють законопроект у бік створення галузевого підзаконного акту.

Усьому свій час. Насамперед необхідно визначитися з принципами та видами діяльності у сфері захисту персональних даних, які затвердить Верховна Рада України. Потім усе інше, зокрема щодо створення механізму реалізації принципів, завдяки діяльності спеціально визначеного органу (нагляду) із захисту персональних даних. Тільки за таких умов можна отримати загальнодержавну системність у роботі щодо приведення законодавства України у відповідність до законодавства співтовариств Європи.

Підсумовуючи долю та стан справ із Законом України "Про захист персональних даних", підкреслимо те, що він був двічі підтриманий народними депутатами України і двічі повертався із зауваженнями Президента України (11.04.2006 р та 30.01.2007 р.), зміст яких наданий вище. Після останнього повернення закону до Верховної Ради України його підкорегували та відправили на експертизу до Головного науково-експертного управління Апарату ВР України. І знову, управління у своєму Висновку посилається на ЦКУ, ЦПКУ та Конституцію України, в яких поняття "персональні дані" не існує взагалі (аналіз зауважень та авторські висновки див. у [214]). Із змісту зауважень є можливим зробити висновки про те, що Закон України "Про захист персональних даних" (особливо його передостання версія, у якій кожній людині надано право

власності на свої персональні дані, що надає більше можливостей для застосуванн поширеного у Європі так званого "права людини на самовизначення" і більше можли востей для реального захисту від несанкціонованої комерції її даними) сьогодні не ду же потрібен або упорядкування відносин у сфері персональних даних згідно з європей ськими стандартами не відповідає якимось політичним уявленням.

Виходячи із аналізу сучасних європейських поглядів та підходів у національному регулюванні інформаційних відносин у сфері захисту персональних даних, можна зро бити висновок, що всі європейські країни мають окремий, базовий закон щодо сфери захисту персональних даних. І Україна у цьому питанні не може бути винятком, тим більше, що це питання є складовим щодо європейської інтеграції та виконання зо бов'язань перед Радою Європи.

Структура Закону України "Про захист персональних даних" від 10.01.2003 р. № 2618 має наступні складові частини:

Преамбула.

Розділ 1. Загальні положення:

сфера дії Закону;

визначення термінів;

суб'єкти відносин, пов'язаних з персональними даними, та їх основні зо бов'язання;

об'єкти захисту;

загальні вимоги до виконання дій з персональними даними;

джерела і бази персональних даних.

Розділ 2. Власність на персональні дані:

право власності на персональні дані;

користування персональними даними.

Розділ 3. Дії з персональними даними:

використання персональних даних;

підстави виникнення права на використання персональних даних;

збирання персональних даних;

накопичення персональних даних;

зберігання персональних даних;

поширення персональних даних.

Розділ 4. Доступ до персональних даних:

режим доступу до персональних даних;

доступ до персональних даних, які становлять державну або іншу визначену зако ном таємницю;

відстрочення та відмова у задоволенні доступу до персональних даних;

оскарження рішення про відстрочення чи відмову в задоволенні запиту на досту до персональних даних;

додаткові права власника персональних даних;

оплата доступу до персональних даних.

Розділ 5. Внесення змін і доповнень:

зміни і доповнення до персональних даних.

Розділ 6. Забезпечення захисту персональних даних:

право на захист персональних даних;

уповноважений орган з питань захисту персональних даних;

технічний захист при обробці персональних даних;

обмеження дії окремих статей цього Закону.

Розділ 7. Відповідальність:
види відповідальності;
оскарження протиправних дій.
Розділ 8. Міжнародне співробітництво:
співробітництво з іноземними суб'єктами;
міжнародні договори;
передача персональних даних іноземним суб'єктам;
підтримка громадян України, які проживають за кордоном.
Прикінцеві положення.

Розгорнуту і детальну аргументацію щодо правових формул і змісту статей, що пропонуються, додаткові авторські пропозиції щодо внесення окремих доповнень та змін до редакції деяких статей Закону, механізми реалізації положень щодо створення єдиної системи захисту персональних даних в Україні див. у [175; 198, с. 10-86 та с. 178-211].

3.2.3. Електронна комерція

До законів України, які стосуються сфери електронної комерції (далі – е-комерція) відносяться:

Конституція України від 1996 р. (ст. ст. 42, 67, 91);
Цивільний кодекс України від 2003 р.;
Господарський кодекс України від 2003 р.;
Закон України "Про захист прав споживачів" від 1991 р.;
Закон України "Про обмеження монополізму та недопущення недобросовісної конкуренції у підприємницькій діяльності" 1992 р.;
Закон України "Про захист від недобросовісної конкуренції" від 1996 р.;
Закон України "Про систему оподаткування" 1991 р.;
Закон України "Про державну підтримку малого підприємництва" від 2000 р.;
Закон України "Про засади державної регуляторної політики у сфері господарської діяльності" від 2003 р. та інші акти, що зазначені в [95].

В сучасних умовах широке застосування інформаційно-комп'ютерних технологій та мереж у комерційній діяльності завдяки, зокрема, електронному обміну даними та укладенням за допомогою електронних засобів договорів у підприємництві стає реальністю. Проте в електронно-інформаційній сфері публічно-правове регулювання підприємницької діяльності має свої особливості, що потребує створення спеціальних юридичних норм і правил, адресованих безпосередньо електронній комерції. У зв'язку з цим у законодавстві й торгових звичаях розвинених країн, а також у міжнародному праві порівняно швидко були введені в юридичну практику такі базові поняття, як: "електронна комерція" ("електронна торгівля"), "електронний обмін даними", "електронний (цифровий) підпис" і значне число інших пов'язаних з ними правових конструкцій: "електронна операція", "електронні документи", "електронні платежі і розрахунки" тощо, про що детально йдеться у монографії [222].

Юридична сфера електронної комерції дуже широка. За визначенням Типового закону ООН "Про електронну торгівлю" 1997 р. (ЮНСІТРАЛ) [216], вона охоплює питання, що виникають у зв'язку з всіма відносинами комерційного змісту, які включають, але не обмежуються такими операціями: покупка/продаж, поставка, угода про розподіл продукції, торгове представництво (агентство), факторинг, лізинг, проектування, консалтинг, інжиніринг, інвестиційні контракти, страхування, угоди про експлуатацію і концесію, банківські послуги, спільну діяльність та інші форми промислової і ділової співпраці.

Також за кордоном розроблені та застосовуються нормативні положення, що відносяться до електронних комерційних операцій нового покоління, так званих "послуг інформаційного суспільства". Вони визначають правовий статус постачальників послуг; регламентують обов'язки постачальників надавати клієнтам відомості про порядок дій щодо укладання договору або відміну замовлень, забезпечення клієнтам можливості заздалегідь ознайомитися з умовами договору, зокрема, за допомогою технологічного відсилання до іншого документа.

У державах-членах Європейського Союзу та Ради Європи існує значна кількість нормативних документів (стандартів), які прямо або опосередковано визначають підходи до правового регулювання відносин у сфері електронної комерції [81]. Головним стандартом (рамковим актом) щодо сфери електронної комерції є Директива 2000/31/СС Європейського Парламенту і Ради "Про правові аспекти інформаційних послуг щодо електронної комерції на внутрішньому ринку" ("Про електронну комерцію") від 08.06.2000 р. [59]. Вона була розроблена на базі рекомендацій Комісії ЄС 1998 р., які визначили основні проблеми правового регулювання у сфері електронної комерції (див. Таблицю) [217].

Порівняно з Типовим законом ООН "Про електронну торгівлю" 1997 р. Директива 2000/31/СС є достатньо обширним документом, що регулює значне коло суспільних відносин у сфері електронної комерції. Так, зокрема, врегульована діяльність провайдерів та інших постачальників інформаційних послуг; встановлюється принцип, що виключає необхідність отримання попередніх санкцій або дозволів для здійснення діяльності подібних організацій; встановлені правила відповідальності провайдерів та інших інформаційних посередників; визначені умови, при настанні яких на вимогу національних органів судової влади на ці організації може бути покладено обов'язок по контролю і пошуку фактів або обставин, що вказують на незаконний зміст діяльності. Детально врегульовано механізм укладення електронних договорів, визначені вимоги, яким вони повинні відповідати, встановлені правила визначення моменту укладення договору.

Метою застосування згаданих спеціальних норм в окремому нормативно-правовому акті є створення відповідного правового поля щодо гармонізації національних законодавчих актів за умов вільного надання інформаційних послуг та забезпечення підвищених юридичних гарантій всім учасникам підприємницької діяльності, у першу чергу малим та середнім підприємствам, які здійснюють ділові операції за допомогою Інтернету.

Важливо підкреслити, що в Директиві 2000/31/СС окремо визначається, що захист осіб у зв'язку з обробкою персональних даних регулюється виключно Директивою 95/46/СС від 24.10.1995 р. "Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних" та Директивою 97/66/СС від 15.12.1997 р. "Про обробку персональних даних та захист прав у телекомунікаційному секторі", які повною мірою можуть бути застосовані до інформаційних послуг. Ці директиви вже визначають правову структуру в сфері обробки персональних даних. Таким чином, немає потреби роз'ясновати цю проблему в Директиві 2000/31/СС з тим, щоб забезпечити ефективне функціонування внутрішнього ринку, зокрема, вільне переміщення персональних даних між державами-членами. Запровадження та застосування цієї Директиви 2000/31/СС має бути здійснене у повній відповідності з принципами, що стосуються захисту персональних даних, зокрема, стосовно надсилання комерційного повідом-

лення без згоди одержувача та відповідальності посередників. Конфіденційність повідомлень гарантується статтею 5 Директиви 97/66/СС, згідно з якою держави-члени повинні заборонити будь-який вид перехоплень чи контроль повідомлень іншими суб'єктами, окрім винадків дозволу на таку діяльність згідно із законом.

Таблиця

Проблеми	Основні питання в рамках проблеми
Регулювання діяльності провайдерів послуг інформаційного суспільства (сервіс-провайдерів)	Порядок визначення місця надання послуги "он-лайну". Порядок початку діяльності з надання послуг "он-лайну" (дозвільний або повідомний). Рамки застосування принципу "свободи установи" (freedom of establishment), закріпленого ст. 52 Договору про створення СС.
Комерційні повідомлення	Визначення поняття "комерційні повідомлення". Правила надання послуг особами так званих регульованих професій (адвокати та ін.). Забезпечення добросовісної конкуренції. Забезпечення прозорості умов надання послуг. Виключення практики "нав'язування послуг".
Укладення договорів з застосуванням електронних засобів	Визнання дійсності договорів, що укладаються в електронний спосіб. Юридична сила дій сторін при укладенні договору.
Відповідальність посередників	Відповідальність посередників за передачу незаконної інформації. Здатність посередників контролювати інформацію, що передається.
Вирішення спорів в області електронної комерції	Засоби механізмів правового захисту, які були б найбільш швидкодійними (з урахуванням географічної віддаленості контрагентів) і ефективними (з урахуванням особливостей електронного бізнесу). Ступінь застосування позасудових механізмів урегулювання спорів. Поліпшення співпраці між регулюючими і судовими органами країн.
Реалізація норм Директиви 2000/31/СС в законодавстві держав-членів СС	Визначення принципів наглядової юрисдикції тієї або іншої держави при транскордонній електронній комерції. Введення уніфікованих правил надання інформації про провайдерів. Надання одноманітних гарантій діяльності сервіс-провайдерів.

Щодо реалій застосування у практиці електронної комерції, то у 1998 р. організація "Азіатсько-Тихоокеанське економічне співробітництво" (Asia Pacific Economic Cooperation), до якої входять Австралія, Бруней, В'єтнам, Індонезія, Канада, Китай, Малайзія, Мексика, Нова Зеландія, Папуа Нова Гвінея, Перу, Росія, Сінгапур, США, Таїланд, Тайвань, Філіппіни, Чилі, Південна Корея, Японія [218], доручила компанії

Price Waterhouse Coopers (PWC) провести дослідження на тему: як розповсюджується, розвивається і використовується електронна комерція в малому і середньому бізнесі країн-членів цієї організації. Компанії цієї категорії чисельно становлять найбільшу частину гравців на полі електронної комерції типу B2B. І ті з них, хто активно використовує технології електронної комерції, мають значні конкурентні переваги. Великі і транснаціональні компанії, що реалізовують B2B-стратегію, дуже часто залучають малий і середній бізнес до своїх ланцюжків поставок. Згідно зі статистикою у вказаному регіоні налічується понад 40 млн. малих і середніх бізнесових організацій, які становлять понад 95 % усіх підприємств. Вони забезпечують зайнятість близько 84 % всієї наявної робочої сили регіону і виробляють від 30 до 60 % ВНП, а їх продукція становить понад 35 % всього експорту.

До таких, що перешкоджають ширшому розповсюдженню електронної комерції серед малих і середніх підприємств, відносяться наступні проблеми [219]:

- низький рівень застосування електронної комерції споживачами і постачальниками послуг;
- проблеми захисту даних;
- наявність правових проблем і проблем відповідальності;
- висока вартість комп'ютерних і мережних технологій;
- обмежені знання в області моделей і технологій електронної комерції;
- невпевненість компаній у можливості виграшу від електронної комерції;
- неадекватність якості телекомунікаційного сервісу для електронної комерції.

Учасниками дослідження була запропонована низка заходів, спрямованих на подолання існуючих бар'єрів, що сприятимуть ширшому запровадженню та застосуванню електронної комерції. Важливішими заходами, що підлягають ухваленню на рівні урядів, були наступні:

- розробка національної стратегії електронної комерції;
- захист даних;
- навчання електронної комерції;
- зрозуміла податкова політика;
- зменшення правових бар'єрів;
- поліпшення сервісу веб-сайтів уряду в Інтернеті.

Результати досліджень також показали, що малий і середній бізнес значною мірою переконаний у важливості урядової підтримки та дій щодо розвитку електронної комерції. Уряд повинен виконувати керівну роль у багатьох напрямах, зокрема у поліпшенні телекомунікаційної інфраструктури, підвищенні безпеки транзакцій, у розширенні доступу малих підприємств до Інтернету та у вирішенні правових і регулюючих проблем, що виникають при застосуванні електронної комерції.

У зазначеному контексті голова комітету Торговельно-промислової палати РФ з інформаційного забезпечення підприємництва О. Іоффе зазначає: "Світова практика показує, що електронна торгівля є одним з основних видів підтримки і розвитку малого і середнього бізнесу: застосування механізмів електронної торгівлі при мінімальних витратах відкриває малому і середньому бізнесу доступ до всього ринку потенційних покупців. За даними НАУЕТ (м. Москва), в 2007 р. більше 60 % операцій припало на частку малого і середнього бізнесу, в першому півріччі їх обсяг становив 2,543 млрд. дол. США, тобто менше ніж за рік обсяг електронних контрактів, одержаних малим бізнесом, виріс на 117 %. У 2008 р. малий і середній бізнес одержать контрактів на 7 млрд. дол. США, припускають експерти" [220].

Виходячи з європейської практики можна говорити про необхідність розробки окремого акту – закону України, що регулює питання зазначеної діяльності, включаючи положення про укладення договорів за допомогою електронних засобів і юридичного їх визнання, про правовий статус, обов'язки і відповідальність інформаційних посередників в електронній комерції.

Структура закону про електронну комерцію може передбачати наступні частини:

Преамбула.

Розділ 1. Загальні положення:

мета, завдання;

визначення (електронна комерція, повідомлення щодо електронної комерції тощо);

законодавство про електронну комерцію;

основні принципи;

суб'єкти електронної комерції (постачальник інформаційних послуг, інформаційні посередники, одержувач послуг, споживач).

Розділ 2. Постачальники послуг:

інформація стосовно постачальника (провайдера) інформаційних послуг щодо електронної комерції;

умови відповідальності постачальника (провайдера) інформаційних послуг за збереження, конвертацію та передачу комерційної інформації;

захист даних, зокрема, персональних.

Розділ 3. Комерційні повідомлення:

інформація щодо комерційних повідомлень;

комерційні повідомлення, що надсилаються без згоди одержувача.

Розділ 4. Договори та інші правочини в електронній комерції:

електронний договір;

умови договору;

укладення договору (оферта та акцепт);

юридична сила електронного документа;

Розділ 5. Вирішення спорів:

позасудове;

судові позови;

електронний документ у якості доказу в суді.

Розділ 6. Відповідальність.

Прикінцеві положення.

Правове регулювання електронної комерції має ґрунтуватися на принципах рівності усіх учасників, свободи договору, безперешкодного здійснення підприємницької діяльності, вільного переміщення товарів, послуг і коштів на всій території України, а також гарантіях судового захисту даних і прав споживачів.

Фізичні і юридичні особи вільні у встановленні своїх прав і обов'язків на підставі договору та у визначенні умов договору, що не суперечать чинному законодавству.

Проектом закону України необхідно передбачити, що договір в електронній комерції може бути укладений шляхом обміну електронними документами, який дозволяє чітко встановити, що документ виходить від сторони за договором. Якщо при укладанні договору застосовуються електронні документи, то умови договору та зобов'язання сторін, що випливають з них, не можуть бути оскаржені сторонами тільки з тих підстав, що він укладений шляхом обміну електронними документами.

Також необхідно передбачити можливість подання електронних документів, підписаних за допомогою електронного підпису, як доказів. Ці докази не можуть заперечуватися тільки з тих підстав, що вони надані у формі електронних документів.

У проекті закону необхідно зазначити, що в разі, якщо законом передбачається вимога нотаріального посвідчення цивільно-правової угоди, така угода, оформлена шляхом створення електронного документа, повинна бути скріплена електронним підписом нотаріуса у порядку, встановленому Законом "Про нотаріат".

При укладанні договору в електронній комерції пропозиція його укласти однієї зі сторін (оферта), прийняття пропозиції іншою стороною (акцепт) можуть бути відправлені й отримані у вигляді електронних документів.

Пропозицію укласти договір може бути спрямовано самим оферентом чи інформаційною системою, запрограмованою оферентом або від його імені і автоматично. Договір визнається укладеним з моменту одержання акцепту особою, що направила оферту.

При цьому є потреба у вирішенні питань щодо:

- надання широкого визначення терміну "електронна комерція" виходячи з того, що вона може бути обмеженою (стосується лише торгівлі – Інтернет-торгівля), частково обмеженою (стосується підприємницької діяльності – Інтернет-комерція) або спрямована на поступове впровадження електронних технологій в усі процеси бізнес-діяльності (Інтернет-бізнес);
- внесення змін до Цивільного кодексу України та Господарського кодексу України в частині, що стосується предмета закону;
- внесення змін до положень податкового законодавства, які повинні враховувати особливості електронно-комерційної діяльності.

Особливості захисту даних. Захист даних у більшості випадків економічної діяльності становить предмет комерційної таємниці. Під комерційною таємницею підприємства маються на увазі відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) яких може завдати шкоди його інтересам. Склад і обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються керівником підприємства. Порушення комерційної таємниці розглядається з точки зору недобросовісної конкуренції, яка може зашкодити діловій репутації або майну іншого підприємця, що передбачає накладення штрафу відповідно до Кодексу України про адміністративні правопорушення.

Постановою Кабінету Міністрів України від 03.08.1993 р. № 611 був встановлений перелік відомостей, що не становлять комерційної таємниці, до яких віднесені:

- 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 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 посадових осіб підприємств, кооперативів, спілок, об'єднань та інших організацій, які займаються підприємницькою діяльністю;

• відомості, що відповідно до законодавства підлягають оголошенню.

Слід звернути увагу на те, що державна таємниця не може бути комерційною таємницею, оскільки в іншому разі мала б місце торгівля державними інтересами. З іншого боку, комерційна таємниця може бути державною таємницею, і тоді вона підлягає захисту не тільки з боку підприємства, а й держави.

У СРСР відомості щодо економічного, технічного або виробничого змісту в результаті діяльності організацій та підприємств (за виключенням відомостей, які становили державну таємницю) мали узагальнюючі поняття "комерційної інформації" (наприклад, Наказ Державного комітету СРСР по винаходах і відкриттях від 27.11.1990 р. № 146, який вводив у дію Положення про комерційну таємницю у системі Держкомвинаходів СРСР).

За кордоном встановлення режиму застосування інформації щодо комерції розглядається в межах поняття "торговий секрет" (trade secret).

Торговий секрет – це цінна інформація, яка:

• є власністю фізичної або юридичної особи;

• має самостійну економічну цінність (фактичну або потенційну) в результаті того, що вона не є загальновідомою, легко встановлюваною належними засобами іншими особами, що можуть одержати економічне збагачення від її розкриття або використання;

• є об'єктом зусиль, необхідних за відповідних обставин для підтримки її секретності.

Поняття "торговий секрет" включає відомості про техніку, технологію, спосіб, формулу, модель, програму, пристрій, метод та ін., а також особливості їх створення.

В основі поняття торгового секрету лежить конфіденційність, що поширюється не тільки на виробництво й торгівлю, а й на дослідження. Тому термін "торговий секрет" є узагальнюючим поняттям для усіх секретів.

Для торгового секрету притаманним є статичність, яка відбиває аспекти власності юридичної або фізичної особи. Коли торговий секрет стає об'єктом передачі права власності він визначається динамічністю та набуває статусу "ноу-хау".

Зазначимо, що нині законодавства країн світу щодо терміну "торговий секрет" продовжують мати розбіжності.

У США, наприклад, у ще у 1979 р. питання ділових секретів виділили із законодавства щодо інтелектуальної власності та прийняли єдиний, окремий закон.

У Великобританії шляхом виділення торгових секретів в окремий закон не пішли, проте їх захист не підпадає під регулювання захисту інтелектуальної власності.

У Канаді в 1990 р. здійснили фундаментальну реформу законодавства щодо торгових секретів у напрямі деталізації відносин в окремому законі, де увага приділена процесуальним діям судів та їх рішень. Зокрема, у § 4(1) закону про ділові секрети встановлено, що суд повинен виходити з того, що торговий секрет охороняється законом, а також враховувати зміни по відношенню до права на нього. Суд має можливість врегулювати відносини сторін виходячи з того, що перевагу має та сторона, яка спочатку володіла правом власності на секрет. З іншого боку, суд може встановити строк дії права на секрет, який визнає розумним для усунення тих комерційних переваг, які інакше одержить відповідач.

У СРСР термін "торговий секрет" перекладався та трактувався по-різному: промисловий секрет, виробничий секрет, торговельна таємниця, фірмова таємниця, комерційна таємниця або комерційний секрет тощо.

Співвідношення понять "комерційна таємниця" і "комерційний секрет" різне. Найчастіше таємниця передбачає привнесення будь-чого нового в будь-який предмет (об'єкт), процес, а під секретом розуміється не тільки сам предмет (об'єкт), а й особливість його створення, наприклад:

• промисловий секрет – це предмет новації (патенту) і будь-які особливості його створення, патентування та виробництва;

• виробничий секрет – привнесення будь-чого нового в процес виробництва;

• торговельна таємниця – отримання знань із закупівлі товарів, списків покупців та ін.;

• фірмова таємниця – індивідуальні особливості виробництва і підприємництва.

У реальному житті комерційна таємниця завжди виступає у формі комерційного секрету. Тому будь-яка таємниця є секретом, але не всякий секрет є таємницею (помилкове віднесення відомостей до комерційної таємниці). Виходячи з цього можна сформулювати робочі визначення комерційної таємниці і комерційного секрету.

Комерційна таємниця – приховувані з комерційних міркувань економічні інтереси й відомості про виробничо-господарську, управлінську, науково-технічну, фінансову діяльність підприємства, захист яких обумовлений загрозами недобросовісної конкуренції. Ця таємниця виникає тоді, коли вона має інтерес для комерції.

Комерційна таємниця може виступати в наступних основних формах:

• конфіденційність (з англ. confidence – довіра);

• договірні умови;

• контрактні відносини;

• зобов'язання (підписка про зобов'язання зберігати комерційні секрети).

Комерційні секрети – форма прояву комерційної таємниці, матеріалізовані певним чином (у вигляді документів, схем, виробів та ін.) відомості, що відносяться до комерційної таємниці та підлягають захисту від посягань шляхом вивідування, заволодіння, витоку та ін.

Нерідко зарубіжні фахівці в області планування і управління виробництвом відносять збір інформації про конкуруючі фірми і компанії до звичного маркетингу разом з такими підсистемами інформації, як персональні дані потенційних споживачів, репутацію фірми, державне регулювання на ринку і т. п. При цьому, електронно-інформаційне середовище надає значно більше можливостей для збору будь-якої інформації.

Свого часу французький дослідник Ж. Бержье склав "список засобів отримання інформації про конкурентів, який застосовують американські промисловці" [221], тобто:

1. Публікації конкурентів і звіти про процеси та одержані результати.
2. Відомості, які публічно надані колишніми працівниками конкурента.
3. Огляди ринків.
4. Фінансові звіти.
5. Влаштовувані конкурентами ярмарки і виставки та брошури, які надаються.
6. Аналіз виробів (продуктів) конкурентів.
7. Звіти комівояжерів і закупівельних відділів.
8. Питання, що ставляться фахівцям конкурента на спеціальних конгресах.
9. Безпосереднє таємне спостереження.
10. Переговори з конкурентом нібито для придбання ліцензії на один з патентів.
11. Використання професійних шпигунів для отримання інформації.
12. Змушування з роботи працівників конкурента для отримання інформації.
13. Посягання на власність конкурента.
14. Підкуп співробітників закупівельного відділу конкурента або його працівників.
15. Засилання агентів до працівників або фахівців конкурента.

16. Викрадання креслень, зразків, документів тощо.
17. Підслуховування розмов у конкурента.
18. Шантаж і різні способи тиску; зрозуміло, конкурент вдається до тих же засобів.

Існують три основних види інформації про конкурентів, до яких відносяться:

1. Інформація про ринок:
- ціни, знижки, умови договорів, специфікація продукту;
- обсяг, історія, тенденція і прогноз для конкретного продукту;
- частка на ринку і тенденції її зміни;
- канали, методи збуту і плани;
- чисельність і розміщення торгових агентів;
- контингент споживачів (зокрема, дисконтні картки) і відносини з ними;
- репутація;
- програма реклами.

2. Інформація про виробництво і продукцію:
- оцінка якості й ефективності;
- номенклатура виробів;
- технологія і устаткування;
- рівень витрат;
- виробничі потужності;
- розміщення і розмір виробничих підрозділів і складів;
- доставка;
- результати проведення науково-дослідної роботи.

3. Інформація про організаційні особливості і фінанси:
- персональні дані і філософія осіб фірми, які ухвалюють ключові рішення;
- фінансові умови і перспективи;
- програми розширення і придбань;
- головні проблеми і можливості;
- програма науково-дослідної роботи.

У наш час завдяки застосуванню техніко-технологічних засобів можливості отримання комерційної інформації значно поширились, а отже, потребують більшого її захисту. Сучасні технології та мережі надають відповідні переваги в комерційній діяльності, з одного боку, а з іншого – створюють більше умов для несанкціонованого отримання будь-яких відомостей.

Так, збирання комерційної інформації може відбуватися за допомогою звичайних каналів зв'язку. Виключити ведення ділових переговорів з використанням телефону або електронної пошти, звичайно, не можна. Тому фахівцям рекомендують в процесі спілкування виявляти обережність і надійно ідентифікувати свого співбесідника. Зрозуміло, повинна використовуватися тільки інформація, що відноситься до співбесідника.

Для отримання комерційної інформації конкурента можуть застосовувати різного роду мікрофони, мініатюрні передавачі та ін. У зв'язку з цим, перед початком наради, переговорів ретельно перевіряють приміщення, в якому вони вестимуться. У західних країнах діє розгалужена мережа фірм, що виконують цю роботу за замовленням. Створені спеціальні прилади, які дозволяють встановити захисний екран, що виключає будь-яке прослуховування в таких приміщеннях.

Вважається, що значне просочування комерційної інформації відбувається в ході ведення переговорів і ділового листування. Трапляється це з різних причин: невміння правильно рекламувати свою продукцію, престиж, що невірно розуміється, і т. д. Тут велику роль мають вже згадувані виховання і навчання співробітників. Ще до початку

переговорів співробітник повинен чітко представляти, яку інформацію він має право передати партнеру по переговорах, що повинен залишити "за кадром"; необхідно вчити фахівців проводити рекламу за методом "чорної скриньки" – вхідні параметри виробу, одержаний результат, а як результат – одержаний секрет фірми. Врешті-решт, працівник, якій веде переговори, повинен усвідомлювати, що від успішно проведених переговорів залежить як процвітання підприємства, так і його особисте благополуччя.

Збирання даних за допомогою Інтернету та інших телекомунікацій сьогодні звичайне явище. Проте ця надзвичайно привабливa можливість може призвести до пошкодження даних, що обробляються на комп'ютері, а саме: ураження комп'ютера різноманітними вірусними програмами, несанкціонованого доступу до даних у локальній мережі та при роботі в Інтернеті, за допомогою так званих програм-шпигунів тощо [170, с. 93-117].

Значне зростання кількості користувачів цієї мережі призвело до поширення кіберзлочинності, в тому числі щодо використання та поширення персональних даних. Комп'ютерні технології та мережі, які є необхідними складовими міжнародної фінансової та банківської діяльності, надали можливість вчинення злочинів економічної спрямованості на національному та міжнародному рівнях. Кримінальні елементи використовують новітні технології для відмивання "брудних" коштів, фінансових махінацій, несанкціонованого доступу до інформаційних систем, поширення неправдивої інформації та інших правопорушень.

На окрему увагу заслуговують файли "cookie". Ці файли створюються веб-серверами для запису інформації про переглянуті сторінки: дату й час, паролі користувача тощо. Ця інформація використовується для аналізу статистичних даних та створення так званих профілів користувачів (які сторінки переважно переглядає користувач, які товари замовляв тощо). Тому для припинення такої діяльності використовують або знищення файлів "cookie" на вінчестері, або блокування цих файлів завдяки опціям браузерів.

Сьогодні збитки від кіберзлочинності перевищують 100 млрд. дол. США [170, с. 113]. За даними американського Інституту комп'ютерної безпеки (Computer Security Institute), хакери використовують такі найпоширеніші методи: підбір ключів, паролів – у 13,9 % злочинів; заміна IP-адрес – у 12,4 % (цей метод атаки передбачає заміну IP-адрес пакетів, що передаються в Інтернеті, так, що вони мають вигляд переданих внутрішніх повідомлень, де кожний вузол довіряє адресній інформації іншого); ініціювання відмови в обслуговуванні (denial of service) – у 16,3 % (вплив на мережу або її окремі частини з метою порушення порядку її штатного функціонування); аналіз трафіка – 11,2 % (прослуховування, дешифрування з метою збирання інформації щодо ключів, паролів тощо); сканування – у 15,9 % (передбачає використання програми, яка перебирає можливі точки входження до системи); підміна, нав'язування, переупорядкування або заміна даних, що передаються мережею, – у 15,6 %; ін. методи – 14,7 %. Таким чином, платою за користування Інтернетом є загальне зниження інформаційної безпеки.

Важливим засобом захисту комерційної інформації є встановлення порядку поводження з її носіями, такими як різні документи, креслення, магнітні носії, які застосовуються в роботі з ПК. Набутий в цій сфері досвід може бути прийнятий як рекомендації при захисті секретів і передбачає необхідність наявності на носіях комерційної інформації відмітних позначок, що розрізняються залежно від рівня секретності інформації, яка міститься в документі.

Намагатися повністю захистити комерційні відомості, накладаючи обмеження на доступ до них, навряд чи можливо. Сучасне підприємство не може дозволити собі за-

секречувати всю циркулюючу в ньому комерційну інформацію, тим більше в умовах функціонування глобальної мережі Інтернет, електронної пошти тощо. Це дуже дорого і невигідно, певна частина відомостей повинна використовуватися в рекламі, велика кількість засекречених матеріалів створює непотрібні перешкоди в роботі. Крім того, неможливо підібрати такі штати співробітників, які до всієї інформації ставитимуться як до інформації з обмеженим доступом.

Але здійснювати протидію суперникам по конкурентній боротьбі на ринку теж необхідно. Тут і має відіграти свою роль діяльність щодо визначення ключової інформації, що дійсно є комерційною таємницею підприємства, виявлення імовірних каналів витоку і пошуку можливих шляхів її захисту. Головне – при цьому слід розуміти, що техніко-технологічні засоби, якими б досконалими вони не були, не здатні забезпечити належний захист даних без чітких нормативно-правових та організаційних заходів і суворого нагляду за ними.

3.2.4. Електронний банкінг

До законів України, які стосуються сфери електронного банкінгу (далі – е-банкінг) відносяться:

Конституція України від 1996 р. (ст. 117);

Закон України "Про банки і банківську діяльність" 2000 р.;

Закон України "Про Національний банк України" від 1999 р.;

Закон України "Про порядок здійснення розрахунків у іноземній валюті" від 1994 р.;

Закон України "Про державне регулювання ринку цінних паперів в Україні" від 1996 р.;

Закон України "Про національну депозитарну систему та особливості електронного обігу цінних паперів в Україні" від 1997 р. та інші акти, зазначені у [95].

У сучасному суспільстві банки займаються найрізноманітнішими видами операцій. Їх діяльність не тільки організує грошовий обіг і кредитні відносини. Через них здійснюються фінансування господарства, страхові операції, купівля-продаж цінних паперів, оплата товарів і послуг, посередницькі операції та управління майном тощо.

Сутність банківської діяльності має два аспекти – юридичний та економічний, які все більше визначаються інформаційним аспектом завдяки появі та поширенню електронно-інформаційного середовища (е-середовища).

У *юридичному аспекті* головне значення має поняття "банківські операції". Такими вважаються операції, які відповідно до законодавства стосуються виключно банківської діяльності: з отримання грошей у внески, надання різних видів кредитів, проведення безготівкових платежів і розрахунково-касове обслуговування, комісійні операції, операції з цінними паперами та багато іншого.

Сьогодні за умови отримання письмового дозволу (ліцензії) Національного банку України банки мають право здійснювати такі операції [8]:

- надання консультаційних та інформаційних послуг щодо банківських операцій;
- депозитарна діяльність (приймання вкладів (депозитів) від юридичних і фізичних осіб) і діяльність з ведення реєстрів власників іменних цінних паперів;
- відкриття та ведення поточних рахунків клієнтів, у тому числі переказ грошових коштів з цих рахунків за допомогою платіжних інструментів та зарахування коштів на них;
- випуск платіжних карток і здійснення операцій з використанням цих карток;
- розміщення залучених коштів від свого імені, на власних умовах та на власний ризик;

- надання гарантій і поручительств та інших зобов'язань від третіх осіб, які передбачають їх виконання у грошовій формі;
- придбання права вимоги на виконання зобов'язань у грошовій формі за поставлені товари чи надані послуги, беручи на себе ризик виконання таких вимог та приймання платежів (факторинг);
- послуги з відповідального зберігання та надання в оренду сейфів для зберігання цінностей та документів;
- випуск, купівлю, продаж і обслуговування чеків, векселів та інших оборотних платіжних інструментів тощо.

Щодо валютних цінностей банки мають право здійснювати такі операції:

- ведення рахунків клієнтів (резидентів та нерезидентів) в іноземній валюті та клієнтів-нерезидентів у грошовій одиниці України;
- відкриття кореспондентських рахунків в уповноважених банках України в іноземній валюті та здійснення операцій за ними;
- відкриття кореспондентських рахунків у банках (нерезидентах) в іноземній валюті та здійснення операцій за ними;
- інші операції на валютному ринку України та на міжнародних ринках.

У плані інформатизації (пункт 7 статті 7 Закону) Національний банк України визначає напрями розвитку сучасних електронних банківських технологій, створює, координує та контролює створення електронних платіжних засобів, платіжних систем, автоматизації банківської діяльності та засобів захисту банківської інформації.

За всієї важливості юридичного аспекту головним у діяльності банків є *економічний аспект*. Не закон визначає суть банку як такого, ні операції, що дозволені йому, а економічний бік справи, природа банку, що спрямовує його на здійснення відповідних операцій.

Сьогодні діяльність суспільства активно перетворюється завдяки *інформаційному аспекту*, основу якого складають інформаційно-комп'ютерні технології та мережі. Вони сприяють появі нових методів управління та систем обробки даних, які визначаються таким поняттям, як "інформатизація", що проектує розвиток, зокрема, банківської системи та її інформаційної складової – електронного банкінгу (е-банкінгу).

Електронний банкінг – це система дистанційного банківського обслуговування клієнта (проведення фінансових операцій (платежів) за допомогою телекомунікаційних каналів (РС-банкінг) і засобів Інтернету (Інтернет-банкінг) [223, с. 5].

е-банкінг дозволяє приватним особам у будь-який слушний час, сім днів на тиждень, 365 днів на рік з будь-якої точки земної кулі здійснювати більшість банківських операцій: проводити безготівкові внутрішньо і міжбанківські платежі, відкривати рахунки, сплачувати комунальні платежі, купувати і продавати валюту, розміщувати вільні кошти на терміновому внеску, одержувати виписки по рахунках і користуватися іншими послугами.

Саме е-банкінг створює умови оперативності в обробці даних та у прискоренні розрахунків, що сприяє зростанню платіжного обігу між суб'єктами банків усіх країн світу. Тому не глобалізація фінансових ринків, не стабільність фінансово-економічних систем, не загроза глобальних монополій з олігархією визначатимуть основні напрями розвитку банків і технологій їх діяльності, а саме – інформатизація як стан та розвиток інформаційно-комп'ютерних технологій та мереж.

Інформатизація, тобто інформаційний аспект у розвитку будь-якого суспільства, дозволяє активізувати й ефективно використовувати інформаційні ресурси, що сьогодні є найбільш важливим стратегічним фактором розвитку суспільства. Це стає найважли-

вінним у підвищенні ефективності керування практично у всіх сферах людської діяльності. Інформаційні технології та ресурси перестають виконувати просто допоміжні функції в діяльності компаній, органів державної влади і місцевого самоврядування, а стають необхідним і найважливішим їх елементом. Від їх розвитку залежить здатність організацій вирішувати різні задачі: підвищувати конкурентоспроможність – для комерційних структур, більш ефективно задовольняти потреби суспільства – для систем органів державної влади і місцевого самоврядування тощо.

Головне полягає у тому, що завдяки застосуванню інформаційно-комп'ютерних технологій та мереж є можливість отримувати істотну економію будь-яких видів ресурсів: часу, фінансів, сировини, енергії, корисних копалин, матеріалів і устаткування, людських ресурсів, і не тільки в межах однієї країни. Інтернаціоналізації інформаційно-технологічних процесів сприяє глобальна інформаційно-телекомунікаційна мережа Інтернет, завдяки якій відбуваються активні процеси інтеграції світового співтовариства, інтенсивне розширення внутрішніх і міжнародних економічних та культурних зв'язків.

Банківська система та законодавство. Банківська система – це сукупність різноманітних видів банків та інших кредитних установ, інституцій у їх взаємозв'язку, яка існує в тій чи ін. країні в певний історичний період і функціонує в межах єдиного фінансового механізму та є складовою частиною кредитної системи. У світовій практиці за наявності тих чи інших особливостей у діяльності банківської системи різних країн багато спільних рис. Однією з найбільш притаманних є дворівнева побудова банківської системи. Перший рівень становить центральний банк (наприклад, в Україні – НБУ, у США – Федеральна резервна система), другий – мережа комерційних банків та інших фінансово-кредитних інституцій. Банківське законодавство розвинутих зарубіжних країн визначається високорозвинутою системою законів про банки і банківську діяльність, ретельністю правової регламентації різних аспектів банківського сектору економіки, спрямоване на інтернаціоналізацію банківського бізнесу і розвиток міжнародного співробітництва у сфері правового регулювання банківської діяльності. В таких країнах, як Великобританія, Німеччина, США, Франція діють понад два десятки законів, які забезпечують функціонування кредитних систем цих країн.

До 1988 р. банківська система України була складовою частиною своєрідного монобанку Радянського Союзу. Функціонували філії і установи таких союзних банків державної форми власності, як Держбанк, Будбанк, Ощадбанк СРСР, а також акціонерного банку Зовнішторгбанк, власниками якого були Держбанк і Міністерство зовнішньої торгівлі СРСР. Керівними органами філій цих банків в Україні були республіканські і обласні контори банків.

У 1988 – 1990 рр. відбулася певна реорганізація банківської системи СРСР, у процесі якої були створені спеціалізовані державні банки: Промбудбанк, Агропромбанк, Житлосоцбанк, Ощадбанк, Зовнішекономбанк, які мали в Україні свої філії і установи. За Держбанком СРСР залишилися функції центрального банку, який в Україні мав республіканські та обласні контори. В цей же період почали створюватися нові комерційні банки різних форм власності. Таким чином, до проголошення незалежності (1991 р.) в Україні функціонувала банківська система, до якої входили філії, відділення і установи союзних державних спеціалізованих банків і Держбанку, а також ряд нових акціонерно-комерційних банків [217, с. 7].

З прийняттям у березні 1991 року Закону "Про банки і банківську діяльність" в Україні почала складатися дворівнева банківська система. На базі Української республіканської контори Держбанку СРСР був створений Національний банк України (НБУ), державні спеціалізовані банки перетворилися на акціонерно-комерційні банки,

швидкими темпами створювалися нові ділові банки акціонерної, приватної і корпоративної форм власності, а також банки за участю іноземного капіталу.

Сучасну структуру банківської системи України, економічні, організаційні і правові засади створення, діяльності, реорганізації та ліквідації банків визначають Закон України від 07.12.2000 р. № 2121-III "Про банки і банківську діяльність" [9] та Закон України від 20.05.1999 р. № 679-XIV "Про Національний банк України" [8], які складають основу, фундамент банківського законодавства.

Банківське законодавство – це система нормативних актів, правові норми яких закріплюють і регулюють порядок організації та діяльності банків та інших фінансово-кредитних установ України, їх взаємовідносини з клієнтами (юридичними і фізичними особами), а також порядок здійснення ними банківських операцій.

За своєю сутністю, змістом та структурою банківське законодавство визначається рядом особливостей.

По-перше, це законодавство носить міжгалузевий зміст і водночас набуває самостійного значення. Воно включає не тільки норми, які безпосередньо регулюють банківські відносини, а й норми конституційного, адміністративного, цивільного та фінансового законодавства. Багатогранність банківської діяльності дає підстави включати до складу її законодавства також норми кримінального права (наприклад, встановлення кримінальної відповідальності за виготовлення, збут, підроблення грошей, цінних паперів та іноземної валюти або кримінальна відповідальність за порушення правил про валютні операції), цивільного права (наприклад, відновлення прав на втрачені цінні папери на пред'явника або про порядок стягнення за виконавчими документами з установ, підприємств та організацій на грошові суми, що знаходяться в кредитних установах).

По-друге, для банківського законодавства притаманна множинність нормативних актів, які регулюють різноманітні аспекти і питання банківської діяльності, за відсутності належної їх кодифікації. Гострою проблемою є недостатня якість законів, які регулюють суспільні відносини у сфері банківської діяльності. Це пояснюється, з одного боку, складною і тривалою процедурою прийняття законодавчих актів, а з іншого тим, що банківські відносини надто рухливі та динамічні, що вимагає постійного внесення змін, спрямованих на приведення законодавства у відповідність із суспільними потребами. Це забезпечується оперативним прийняттям підзаконних нормативних актів. У зв'язку з цим, склалася перевага підзаконних нормативних актів над законами у сфері правового регулювання банківської діяльності.

По-третє, основний масив банківського законодавства складається з актів відомчого змісту. Причому такі центральні органи державного управління, як Національний банк України, Державна комісія з цінних паперів та фондового ринку наділені функціями щодо видання підзаконних нормативних актів, які мають міжвідомчий зміст і є обов'язкові для виконання всіма юридичними і фізичними особами.

У наш час банківське законодавство в Україні склалося як великий масив різноманітних законодавчих і підзаконних актів щодо юридичної сили, форм і сфер їх дії. У своїй сукупності вони становлять ієрархічну систему: закони і постанови ВР України, укази Президента України, постанови уряду, інструкції, положення, правила НБУ, Мінфіну та Державної комісії з цінних паперів та фондового ринку, локальні нормативні акти, міжнародні конвенції та договори, ратифіковані Україною. У цій ієрархічній системі важлива роль відводиться законам, які охоплюють найважливіші питання регулювання банківської діяльності. Це насамперед закони: "Про порядок здійснення розрахунків у іноземній валюті" (1994 р.), "Про відповідальність за несвоєчасне виконання грошових зобов'язань" (1996 р.), "Про державне регулювання ринку цінних паперів в

Україні" (1996 р.), "Про національну депозитарну систему та особливості електронного обігу цінних паперів в Україні" (1997 р.) та ін.

До джерел банківського законодавства належать постанови ВР України, які приймаються як акти поточного законодавства, наприклад: "Про застосування векселів у господарському обороті України" (1992 р.), "Про норматив обігу платіжних документів в Україні" (1993 р.), "Про впорядкування оплати комерційним банком за здійснення платежів" (1993 р.). Великий за обсягом блок банківського законодавства становлять підзаконні нормативні акти – укази Президента України та постанови КМ України. Відповідно до п. 4 розділу XV Перехідних положень Конституції України Президент України видав такі укази, як "Про застосування штрафних санкцій за порушення норм з регулювання обігу готівки" (1995 р.), "Про деякі питання захисту банківської таємниці" (1998 р.), "Про заходи щодо захисту прав фізичних осіб-вкладників комерційних банків України" (1998 р.), "Про кредитні спілки" (1999 р.), "Про заходи щодо недопущення відпливу з України валютних та ін. майнових цінностей" (1999 р.).

В регулюванні банківських відносин оперативного змісту особливе місце займають постанови КМ України, які приймаються відповідно до ст. 117 Конституції України. Наприклад, "Про тимчасову спостережну раду Державного експортно-імпортного банку України" (1998 р.), "Про затвердження переліку банків, уповноважених здійснювати розміщення та обслуговування облігацій внутрішньої державної оцадної позики" (1998 р.), "Про затвердження Порядку накладення арешту на цінні папери" (1999 р.). З існуючого масиву українського банківського законодавства до числа основних регуляторів банківських відносин слід віднести постанови, інструкції, правила, положення, які приймаються НБУ, Міністерством фінансів України, Державною комісією з цінних паперів та фондового ринку, Фондом державного майна України. Наприклад, постановами Правління НБУ були затверджені Положення "Про кредитування" (1995 р.), Інструкція "Про безготівкові розрахунки в господарському обігу України" (1996 р.), Положення "Про порядок створення і реєстрації комерційних банків" (1998 р.), Інструкція "Про відкриття банками рахунків у національній та іноземній валюті" (1998 р.), "Правила здійснення операцій на міжбанківському валютному ринку України" (1999 р.) тощо.

До системи джерел банківського законодавства належать також локальні нормативні акти, прийняті суб'єктами господарської діяльності. Наприклад, Асоціація українських банків у 1995 році прийняла статут, положення якого ставлять за мету об'єднання банків для координації банківської діяльності і сприяння розвитку банківської системи України, захисту інтересів прав банків, забезпечення їх зв'язків з громадськістю та реалізації цілей комерційних банків. Слід мати на увазі, що міжнародні договори, які стосуються банківської сфери, ратифіковані ВР України, також є частиною національного банківського законодавства. Важливе значення для створення повноцінного законодавства має розроблена НБУ концепція розвитку банківської системи України, яка включає основні напрями вдосконалення банківського законодавства. Концепція передбачає створення на основі всіх чинних законодавчих і нормативних документів систематизованого Кодексу нормативних актів регулювання банківської діяльності, постійне підтримання його в актуальному стані.

Регулювання електронної банківської діяльності за кордоном. Проблема вибору правового механізму регулювання електронної банківської діяльності, зокрема, і в цілому інформаційних відносин, що формуються в процесі використання Інтернет, стає все більш актуальною як для більшості розвинених держав світу (зокрема в особі їх фіскальних органів) і міжнародних організацій, так і для споживачів різних банківських послуг.

Сьогодні мережа Інтернет досягла такого рівня розвитку і в такому ступені здатна впливати на життя суспільства, що не припускає неминучий перехід від саморозвитку до державного регулювання діяльності у мережі, тобто – регулювання економічних відносин у зв'язку із застосуванням телекомунікацій. Наприклад, невраховані обороти по реалізації товарів, робіт і послуг тільки в російському сегменті глобальної комп'ютерної мережі Інтернет в 2000 р. склали порядку 0,5 млрд. дол. США [223, с. 9].

Рішення проблеми оподаткування результатів банківської діяльності, здійсненої з використанням Інтернет, ускладнюється у всьому світі тим, що чинне національне податкове законодавство всіх країн орієнтується на регулювання традиційних правовідносин.

Крім того, необхідно вирішувати проблему юрисдикції, яка обумовлена перш за все екстериторіальністю Інтернет, що не дозволяє повною мірою здійснювати податковий контроль в межах конкретної держави. Рух даних в Інтернеті через специфіку цієї мережі часто не може бути регламентований законодавством тільки однієї країни, у зв'язку з чим виникає необхідність підготовки міжнародно-правових актів. Слід зазначити, що вирішення зазначеної проблеми на міжнародному рівні, безумовно, заслуговує на підтримку, проте це не виключає необхідності розробки адекватного національного законодавства.

Разом з тим, ще в 1998 – 1999 рр. експертами Нью-Йоркської урядової робочої групи по електронній торгівлі і ОЕСР розроблені декілька проектів міжнародних конвенцій про електронні операції і директив про оподаткуванню операцій, здійснюваних в Інтернеті. Автори проектів виходять з прив'язки електронних послуг до фактичного місця знаходження комп'ютерного серверу, який пропонується визнавати за постійне представництво. При цьому оскільки велика частина існуючих у мережі веб-сайтів (у тому числі які належать господарюючим суб'єктам, що є податковими резидентами країн Європейського Союзу) розміщені на серверах, фізично розташованих на території США, при використовуванні цієї правової конструкції і відповідне оподаткування здійснюватиметься в цій державі, що суперечить як національним інтересам країн світу, так і загальновизнаним принципам міжнародного права.

На сьогодні у світі існують 3 основних підходи до вирішення проблеми правового регулювання і оподаткування електронної економічної діяльності. Кожний з них підтримує певна група держав [223, с. 184-194].

1. **США** і держави, які займають лідируючі позиції в області нових інформаційних технологій (**Японія, Канада, Південна Корея, Австралія**), вважають за необхідне встановлення в світі режиму невтручання (або мінімального втручання) в електронний сегмент (національних і світовий) економіки (принцип саморегулювання електронної комерції) і мораторію на оподаткування електронної економічної діяльності з метою максимізації вигод від використання економічного потенціалу мережі для національних економік названих країн.

Як зазначається у [225, с. 87-89], держави цієї групи "при всіх нюансах в підходах цих країн до створення глобальних правових рамок для електронної комерції, єдині в розумінні того, що приватному сектору треба прийняти на себе провідну роль в розвитку Інтернету і електронної торгівлі. На думку вказаних країн, система саморегулювання цієї індустрії (особливо в таких областях, як встановлення стандартів, захист даних і контроль за її змістом) повинна стати нормою, за винятком тих випадків, коли, виникає потреба в реалізації державних заходів або міжнародних угод. З цією метою потрібно буде налагодити координацію діяльності урядів по лінії міжнародних організацій (СОТ, ВОІС, ЮНСІТРАЛ та ін.) з адаптації чинних торгових законів і положень".

Мова, таким чином, повинна йти про перенесення центру тяжіння з функцій державного регулювання на функції "полегшення" і "спрощення" порядку здійснення електронної економічної діяльності.

У США згідно з рішенням Верховного суду США від 1992 р. діє мораторій на введення оподаткування електронної економічної діяльності, здійснюваної з використанням Інтернет. Відповідно до цього рішення компанії, які продають товари за допомогою Інтернет за каталогами (Інтернет-магазини), були віднесені до пільгової категорії. У 1998 р. названий мораторій був продовжений до жовтня 2001 р.

Останніми роками уряди багатьох штатів стали виказувати велику занепокоєність тим, що у міру розвитку електронної комерції через наявність мораторію в першу чергу страждають бюджетні інтереси штатів. У свою чергу, представники компаній, що здійснюють економічну діяльність в Інтернеті (Інтернет-компанії), заперечують, що відміна мораторію перешкоджатиме подальшому розвитку важливого для США сектору економіки. Тих же міркувань дотримується і федеральна влада.

У 2000 р. Конгрес США ухвалив рішення про продовження чинного мораторію. Коментуючи це рішення, конгресмен від штату Техас Л. Доггет відзначив, що "даний мораторій був прийнятий з метою заохочення зростання індустрії електронної комерції і захисту молодого бізнесу від різних федеральних і місцевих податків в США. Електронна комерція все ще переживає період дитинства і може не реалізувати весь свій потенціал, якщо потрапить під податковий прес". Податковий мораторій був продовжений до 2006 р., тобто на 5 подальших років після закінчення терміну дії поточного мораторію в жовтні 2001 р. В ході розгляду питання про мораторій на оподаткування електронної комерції були скасовані поправки, що обумовлювали право одинадцяти штатів не вводити в дію такий мораторій на їх території.

Слід зазначити, що адміністрація США наполегливо рекомендує слідувати прикладу Сполучених Штатів і політичному керівництву інших індустріально розвинених держав. Разом з тим, американські економісти – супротивники мораторію відзначають, що відсутність оподаткування електронної комерції обертається для США істотними бюджетними втратами. Так, відповідно до досліджень, виконаних професором Університету Теннессі Д. Брюсом, бюджети кожного з штатів США недоотримають до мільярда доларів щорічно.

Разом з тим, як зазначалося вище, ще в 1998 – 1999 рр. експертами Нью-Йоркської урядової робочої групи по електронній торгівлі розроблені декілька проектів міжнародних конвенцій про електронні операції і директив про оподаткування операцій, здійснюваних в Інтернеті. Як передбачається проектами, бюджетні втрати, викликані чинним сьогодні мораторієм, в недалекому майбутньому можуть бути компенсовані. Проте, згідно із "задачами сьогоднішнього дня" адміністрація США здійснює реалізацію концепції "Глобальної інформаційної безподаткової інфраструктури" (GIAI) [226].

Канада. У питаннях регулювання електронних операцій дотримується позицій США.

У липні 2001 р. в Канаді оголошено про початок збору пропозицій громадян з реформи законодавства у сфері охорони авторських прав, інтелектуальної власності і податкових пільг. Очікувана реформа законодавства покликана прояснити правовий статус Інтернет-компаній, що здійснюють мережні теле- і радіотрансляції. Крім того, передбачаюсь визначити ступінь застосування даного законодавства до діяльності компаній-провайдерів, що надають третім особам послуги з підключення до Інтернету. Чинні в країні норми з охорони авторських прав багато в чому відповідають стандартам ВОІС, проте, як зазначає перший віце-директор Інституту порівняльного права і

світових економічних процесів (м. Монреаль) А. Пашканіца: "Канаді необхідне законодавство, що орієнтоване на регулювання не статичних глобальних економічних процесів, які швидко змінюються, а того, що враховує всі наші національні мікроекономічні особливості". Так, нове законодавство "повинно врахувати такий канадський феномен, як правова невизначеність з телебаченням он-лайна". Зокрема, залишається відкритим питання, чи повинні поширюватися податкові пільги, передбачені канадським законодавством для телекомпаній і інших засобів масової інформації, функціонуючих поза Інтернет, на компанії, що здійснюють свою діяльність виключно або переважно в мережі. Дана проблема останніми роками набуває особливого значення у зв'язку з тим, що чинне законодавство як Канади, так і інших держав не містить юридичних критеріїв віднесення таких телекомпаній і інших інформаційних джерел, відомості з яких поширюються за допомогою Інтернету (електронні видання та газети), до засобів масової інформації, а також порядок їх звітності по податкових пільгах.

2. Країни другої групи, що займають позиції в області нових інформаційних технологій "услід за лідерами" – в основному держави-члени СС, – зацікавлені в швидкому усуненні прогалин щодо оподаткування у сфері електронної економічної діяльності. Внутрішню і зовнішню політику вони будують виходячи з розуміння необхідності максимального державного регулювання електронних економічних відносин, грунтуючись на приматі фіскальних інтересів.

Зазначені країни в основу своєї внутрішньої і зовнішньої політики в області електронної банківської діяльності ставлять розуміння того, що стягування податків з оборотів комерційних операцій, здійснюваних за допомогою Інтернету, може стати в перспективі важливою, а на певній стадії розвитку світової електронної економіки – важливішою статтею поповнення як національних бюджетів, так і консолідованого інтеграційного бюджету СС.

Для досягнення поставлених задач пропонуються різні податково-правові конструкції. Наприклад, експерти Ешмановського інституту (**Бельгія**) пропонують "ввести так званий "побітовий податок" – поставити лічильники і стягувати гроші за обсяг переданої інформації (трафік), точніше, "перекачаних бітів", незалежно від того, які відомості вони надають і чи надають взагалі. За зробленою свого часу оцінкою бельгійського Міністерства комунікацій, при ставці такого податку 1 дол. США за 100 метабіт податкові надходження цієї країни могли становити порядку 10 млрд. дол. США в рік (становить 4 % від валового національного продукту Бельгії)" [227, с. 70].

У **Франції** в червні 2001 р. для цілей подальшого оподаткування електронної економічної діяльності розглядалася можливість обов'язкової державної сертифікації торгових і банківських Інтернет-компаній. У доповіді комісії з фінансів Національних зборів Франції пропонується ввести спеціальний "пізнавальний знак", яким слід відмічати ті торгові Інтернет-компанії, які пропонують достатні гарантії податкової прозорості і технологічної безпеки при здійсненні платежів з використанням банківських карток [228].

Разом з тим, ще в травні 2000 р. французьким користувачам Інтернет були заборонені операції з придбання товарів в Інтернет-магазинах і аукціонах, організатори яких не одержали у встановленому порядку дозвіл на торгівлю і проведення аукціонів і не стали на податковий облік для сплати податку на додану вартість. Правовою підставою введення такої заборони слугувало Рішення муніципального суду м. Парижа від 5 травня 2000 р. № 456/7/А7 "По справі про оподаткування Інтернет-аукціонів, здійснюваних в режимі реального часу". Судовий розгляд був початий після того, як компанія Nart.com приступила до продажу творів французького живопису через веб-сайт свого американського представництва.

У вересні 2001 р. у Франції введені в обіг спеціальні небанківські пластикові картки Easysmatcodes вартістю 50, 100 і 200 франків, що призначені для оплати придбаних товарів (послуг) за допомогою Інтернет. Такі картки мають індивідуальний номер і 25 кодів, які указуються при оплаті товарів (послуг), що купуються із застосуванням Інтернету. При кожній покупці використовувався один з цих кодів.

Перевагою такої системи електронних розрахунків фахівці називають її анонімність – використання картки не пов'язане з персональними даними покупця і не вимагає відкриття спеціального банківського рахунку. Власник системи – компанія SEP-Tech уклала угоду про введення такої системи оплати з рядом сайтів порнографічного змісту. З іншого боку, за оцінками податкових органів Франції, впровадження таких карт ускладнить встановлення податково-правового контролю над електронною економічною діяльністю, крім того, розвиток подібних сплачених наперед фінансових продуктів у майбутньому може істотно ослабити стабільність банківської системи і емісійної політики Франції.

У **Німеччині** у 2000 р. розглядалась можливість доповнення діючої системи податків новим фіскальним платежем – "Податком на застосування Інтернет в ділових цілях". Для цілей даного оподаткування Інтернет з економічної точки зору передбачається розглядати як засіб виробництва. В якості платників податку (суб'єктів оподаткування) можуть виступати тільки юридичні особи – податкові резиденти Німеччини, які застосовують Інтернет для отримання прибутку ("у ділових цілях"). В цьому випадку об'єктом оподаткування виступатиме час, протягом якого комп'ютер юридичної особи був підключений до Інтернет і використовувався для здійснення підприємницької діяльності. Передбачається, що при складанні відповідної податкової декларації співробітники фінансових підрозділів компаній додатково заповнюватимуть графу "Інтернет". У названій графі вказуватиметься час, проведений в мережі ("тривалість роботи в Інтернеті"), тематика відвідуваних сайтів і т.д.

При цьому найважливішою обставиною стає не вирішена поки проблема порядку здійснення відповідного податкового контролю за достовірністю відомостей, що надаються.

Аналогічні ідеї були закладені і в ряд законопроектів **Швейцарії**. Проте в липні 2000 р. парламент країни категорично виступив проти введення загальнонаціонального оподаткування електронних банківських послуг за допомогою Інтернету. Крім того, було заявлено, що реалізація нематеріальних товарів (інформації про курси валют, біржові котирування, новини та інше), що придбаваються через Інтернет, не буде оподатковуватися на додану вартість.

У **Туреччині** переважають прихильники жорсткішого підходу до правового регулювання електронного сегмента національної економіки. Відповідно до закону Туреччини від 7 червня 2001 р. в якості базової схеми, за аналогією з якою передбачається здійснення правового регулювання інформаційних обмінів в рамках турецького сегмента Інтернету, вибрана правова конструкція, що застосовується сьогодні для регулювання діяльності друкованих видань. Інтернет прирівняли до засобів масової інформації. Зазначений закон Туреччини передбачає штрафи розміром до 100 млрд. турецьких лір (близько 85 тис. дол. США) за публікацію на веб-сайті, власником якого є юридична або фізична особа – податковий резидент Туреччини, хибних новин ділового змісту, образ і інших схожих матеріалів. Проте уряд відмовився затвердити положення закону, які вимагають дозвіл місцевих властей на відкриття веб-сайту (за аналогією з процедурою створення і державної реєстрації звичайного друкованого видання або електронного ЗМІ (юридичної особи). Запроваджено м'який, повідомний порядок відкриття веб-сайтів.

3. Третю групу становлять країни, політичні системи яких вважаються демократичними лише частково. Це в першу чергу Китай, Куба, Монголія, Іран. З цілком зрозумілих причин політичні еліти названих держав прагнуть до максимального контролю над інформаційними (а не над економічними) відносинами щодо Інтернету. Електронні економічні відносини розглядаються не з погляду фіскальних інтересів, а крізь призму політики і ідеології державної монополії.

Існує достатньо поширена думка, що широкий доступ до інформації, поширюваної із застосуванням Інтернету, веде до розвитку свободи слова і демократії. Тому більшість американських політологів передрікає неминучий крах політичних режимів країн цієї третьої групи у міру проникнення нових інформаційних технологій на їх територію. Разом з тим, влада названих країн знайшла способи контролювати політичні дебати в Інтернеті у межах своїх країн. При цьому застосовуються різні стратегії для контролю над інформаційними і економічними процесами в Інтернеті.

Так, в **Китаї** уряд заохочує бажання своїх громадян виходити в мережу, ретельно контролюючи чати і веб-сторінки. 12 липня 2001 р. голова Китаю Дзянь Дзе-Мінь закликав посилити контроль за використанням Інтернету на території Китаю. В наш час у китайському сегменті глобальної комп'ютерної мережі зведена так звана "Вогненяна Китайська Стіна", що блокує доступ до небажаних веб-сайтів. Список закритих сайтів визначається спеціальною комісією Центрального комітету Комуністичної партії Китаю. Крім того, декілька кібердисидентів, що розмістили в мережі критичні зауваження на адресу уряду, були засуджені до різних строків ув'язнення. Проблема вибору механізмів правового регулювання і оподаткування електронної економічної діяльності в Китаї поки не визначена. Міністерство фінансів Китаю з квітня 2000 р. розглядає питання про можливість оподаткування електронної економічної діяльності китайських компаній.

На **Кубі**, навпаки, доступ до мережі Інтернет мають тільки університети і деякі державні установи, тобто електронна банківська діяльність з території Куби не ведеться.

Уряд **Ісламської Республіки Іран** у принципі не виступає за заборону Інтернету, проте намагається захистити себе і населення від появи в Ірані небезпечних для партії ісламізму матеріалів, а також неконтрольованої державними органами внутрішніх доходів (податковими органами Ірану) економічної (в першу чергу торгової) діяльності. До 1997 р. в Ірані Інтернет був заборонений. Після його легалізації в країні стали надзвичайно популярними заклади, де іранцям надається можливість користування Інтернетом. Проте з травня 2001 р. в країні розгорнена кампанія, спрямована на посилення контролю над використанням Інтернету і регулювання діяльності єдиної в країні провайдерської служби. З цією метою в Ірані, як і в КНР, повністю блокований доступ на деякі іноземні веб-сайти, в першу чергу аморального і фінансово-економічного змісту. Іранська телекомунікаційна компанія, яка є монополістом у сфері послуг підключення до Інтернету, відповідно до рішення уряду країни постійно фільтрує небезпечні для національної безпеки Ірану матеріали, поширювані в глобальному інформаційному просторі, і покликана припиняти комерційні наміри іранців у мережі Інтернет [229, с. 123-124].

Зростаюче значення електронної банківської діяльності і наростаюча гострота проблем, які породжені існуючими прогалинами і в праві, і в оподаткуванні цієї сфери, стають предметом пильної уваги міжнародних організацій: Світової організації торгівлі, Всесвітньої організації інтелектуальної власності, Комісії ООН з міжнародного торгового законодавства, Міжнародної торгової палати, Організації економічного співробітництва і розвитку, Міжнародної асоціації електронної комерції, Міжнародної асоціації фінансового законодавства та ін.

Наприклад, під егідою Європейського центрального банку і Міжнародної асоціації електронної комерції в червні 2001 р. в Гаазі (Голландія) пройшла міжнародна конференція країн Європейського Союзу, учасники якої спробували визначити принципи, якими потрібно керуватися при розробці міжнародних, міжурядових актів в області оподаткування електронної економічної діяльності (електронної комерції). Проте про єдину законодавчу базу в області електронної банківської діяльності домовитися поки не вдалося.

Питання, в суді якої держави і відповідно до законодавства якої країни повинен розглядатися позов у випадку, якщо позивач і відповідач зареєстровані як юридичні особи або підприємці в різних країнах, завжди було одним з найважливіших в міжнародному приватному праві. Розвиток електронної банківської діяльності загострив названу проблему. Тому основними темами обговорення на конференції стали проблеми юрисдикції, підвідомчості і підсудності справ за суперечками, що виникають в процесі електронної економічної діяльності.

Крім того, велика увага була приділена розробці основних параметрів проекту першої міжнародної міжурядової угоди (конвенції) у сфері електронної банківської діяльності із застосуванням Інтернету. Пропозиції, що безпосередньо зачіпають електронну комерцію, торкаються регулювання секторів B2B ("бізнес-бізнес"), B2C ("бізнес-клієнт", тобто – Інтернет-торгівля), див. [83, с. 81-83], відносин з працедавцями та щодо інтелектуальної власності. Відповідно до пропозицій учасників Гаазької конференції розгляд спорів, що виникають з операціями в секторі B2B, передбачається віднести до підсудності суду будь-якої обумовленої в контракті країни. Якщо країна юрисдикції не визначена, за умовчанням діє законодавство країни місцезнаходження постачальника товару (послуг).

Операції в секторі B2C запропоновано відносити до юрисдикції суду держави, в якому постійно (або переважно) проживає покупець. Проте такий підхід де-факто визнаний лише Європейським Союзом. Проти цієї правової конструкції виступають США.

При цьому слід визнати важливою роботу Європейського Союзу щодо уніфікації підходів до правового регулювання і оподаткування щодо електронної економіки і, зокрема, узгодженості політики європейських країн із застосування електронно-цифрового підпису.

У зв'язку з великою кількістю невирішених проблем у сфері е-банкінгу, у технологічних питаннях електронних банківських операцій важливу роль мають нормативні (міжкорпоративні) засади електронних банківських трансакцій.

Нормативні засади електронних банківських трансакцій – це викладені в угодах правила, що регулюють права та обов'язки всіх учасників процесу виконання електронних банківських трансакцій як у нормальних умовах функціонування, так і у випадку якихось порушень, а також передбачають дійовий механізм санкцій для виконання зобов'язань. Повний комплекс цих правил має бути відомий всім учасникам та іншим зацікавленим особам. Дотримання правил виконання трансакцій може забезпечуватися шляхом судових спорів, вжиття заходів примусу з боку регулюючих установ та приватного арбітражу.

Нормативні засади електронних банківських трансакцій включають також стандарти, які допомагають зменшити витрати та ризики у банківських трансакціях, підвищити їх надійність. Існують, наприклад, операційні стандарти, стандарти стосовно документації, інструментів, форматів та реквізитів повідомлень. Норми (узгоджені правила) охоплюють й інші види порядку, процедур та практики, що застосовуються при виконанні електронних банківських трансакцій (наприклад, термінологію і мову, критерії оцінки та класифікації, форми й методи передачі платіжних документів, порядок перевірки їх справжності, терміни й методи виконання платежів, умови відкликання платежу і остаточного розрахунку тощо). Формалізація якнайбільшої кількості правил, стандартів, процедур прискорює процеси комунікації та обробки, скорочує витрати на поточний контроль і забезпечення додержання вимог. Чітко визначені правила мають важливе значення також з точки зору їх стимулюючого або стримуючого впливу на учасників трансакцій у виборі ними того чи іншого методу обробки трансакцій.

У нормативних засадах регулювання електронних банківських трансакцій різних країн існують суттєві відмінності. Разом з тим, у всіх країнах застосовуються декілька тотожних або дуже близьких основоположних принципів. Незалежно від походження правил, що регулюють такі трансакції (нормативні акти, домовленості чи угоди), всі вони повинні відповідати критерію справедливості та, в разі необхідності, мають узгоджуватися в ході переговорів усіх зацікавлених сторін і оприлюднюватися.

Нормативні засади електронних банківських трансакцій часто розробляються у вигляді окремих документів. Проте широко застосовуються і механізми, передбачені загальною правовою системою, зокрема банківське законодавство, основною метою якого є регулювання питань ліцензування банків та нагляду за ними, закони про центральні банки, законодавчі акти, що встановлюють правила використання певних фінансових інструментів (наприклад, чеків та переказних векселів), і, звичайно, такі загальні законодавчі документи, як цивільний кодекс чи комерційний кодекс будь-якої країни. Деякі закони також можуть стосуватися правил виконання електронних банківських трансакцій. Наприклад, закон про банкрутство, положення, що стосуються валютних та транскордонних трансакцій, закон про захист прав споживачів. У більшості країн спеціальним законодавством регулюються операції з банківськими пластиковими картками (кредитними картками).

Банківська таємниця. Згідно зі статтею 60 "Банківська таємниця" Глави 10 "Банківська таємниця та конфіденційність інформації" Закону України від 07.12.2000 р. "Про банки і банківську діяльність" – банківська таємниця – це "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 ...Інформація про ...клієнтів, що збирається під час проведення банківського нагляду, становить банківську таємницю" [9].

Законодавчі норми визначають перелік відомостей, коло суб'єктів, зобов'язаних зберігати в таємниці дані про вкладника, його рахунки в банку та операції, які він здійснює із вкладами, а також випадки і порядок доступу до відомостей, що становлять такого роду таємницю.

Нормами банківської таємниці регулюються три групи правовідносин: між банком та клієнтом; між банком та органами, які мають право доступу до банківської таємниці; між клієнтом банку та органами, які мають право доступу до банківської таємниці. Не розголошувати відомості про банківські операції, рахунки та вклади своїх клієнтів і кореспондентів – важливий обов'язок кожного службовця банку, передбачений ст. 60 Закону України "Про банки і банківську діяльність". Проте цей закон, як і Указ Президента України "Про деякі питання банківської таємниці" (1998 р.), не регламентує такі норми, як порядок оскарження протиправних дій, кримінального покарання за передачу, втрату конфіденційної фінансової інформації, необережне поводження з нею, а також розмір відшкодувань матеріальної та моральної шкоди, завданої власнику інформації.

У зв'язку з високим рівнем ризику банківської діяльності і тим, що ризикові незаконні дії банків здатні призвести до значних економічних потрясінь, у багатьох країнах існує тенденція до розширення числа випадків, у яких дозволяється здійснювати доступ до банківської таємниці, а також покладання на банки додаткових зобов'язань із взаємодії з органами, котрі мають доступ до банківської таємниці (інформування про "нестандартні" грошові операції клієнтів, особливо великі грошові перекази, підозрілі джерела коштів тощо). Така тенденція пов'язана з намаганням державних органів мінімізувати ухиляння від сплати податків, посилити протидію наркобізнесу, корупції та легалізації злочинних доходів.

Разом з цим, з виникненням комп'ютера розпочалися процеси проникнення в усі сфери діяльності людини, суспільства і держави інформаційно-комп'ютерних технологій та мереж. Ці процеси мають два аспекти.

З одного боку, нові технології та комунікації дозволяють "стискати" час та "скорочувати" відстані, отримувати економічні, технологічні та інші переваги як у плані досягнення інтересів окремої особи, так і в масштабах груп людей, країн, регіону, світової спільноти.

З іншого боку, все більше загострюється проблема неправомірних і несанкціонованих дій різних суб'єктів, які використовують засоби е-середовища. Активність у формуванні баз даних, обробка, поширення та використання відомостей про осіб без їх відома призвели до виникнення глобальної за своїми масштабами у часі та просторі проблеми інформаційної безпеки людини, суспільства і держави щодо захисту персональних даних.

Так, наприклад, у [230] повідомляється наступне. У березні 2007 р. деякі клієнти "Райффайзенбанку" знайшли в е-пошті прохання відвідати вказаний сайт банку і відновити свої дані. Прохання мотивувалося модернізацією системи безпеки банку. На сторінці сайта вимагалося ввести особистий ідентифікаційний код, що дозволяє управляти своїм банківським рахунком за межами банку.

Проте, посилання вело на абсолютно сторонній сайт, який зовні схожий на сторінку входу в систему он-лайн-банкінгу "Райффайзенбанку".

"Райффайзенбанк" ніяких листів не розсилав – повідомили в прес-службі банку. Його клієнти просто зіткнулися з черговим випадком фішингу (від англ. – лов риби). Так називають спроби виудити в користувачів Інтернету пароль до банківського рахунку або реквізити пластикової картки. Для цього злочинці створюють клони фінансових сайтів відомих банків або платіжних систем.

Число фішинг-атак збільшується. За даними англійської Асоціації Apacs, з січня 2005 по вересень 2006 р. на території країни число випадків фішингу зросло в 80 разів; збиток оцінюється в 23 млн. фунтів стерлінгів.

За підрахунками Антіфішингової групи (Anti-Phishing Working Group), за грудень 2006 р. було зареєстровано 23787 повідомлень про факти фішингу, при цьому виявлено 28531 підроблених сайтів, більшість з яких розташовувалось у США. За цей період атакам фішерів піддалися 146 брендів.

Але, на думку засновника сервісу E-Secure-IT (Арджена де Ландграфа), найбільшу небезпеку становлять російські "рибалки", які не тільки займаються виуджуванням інформації у клієнтів банків, а й загрожують атаками на сайти кредитних установ, що намагаються їм протидіяти. Він наводить приклад одного австралійського банку, нормальне функціонування якого було порушене протягом трьох днів. Доходи цього невловимого російського угруповання оцінюються в 150 млн. дол. США.

За інформацією консультантів групи Trend Micro, вартість інформації про номер кредитної картки і PIN-код, які дозволяють виготовити копію картки і зняти гроші через банкомат, становить 250 фунтів стерлінгів. А просто за номер, код безпеки і термін дії картки, які дозволяють проводити платежі через Інтернет, – від 3 до 12 фунтів стерлінгів.

Сайт підкреслює, що перший рубіж боротьби з фішингом знаходиться в банку. Банк повинен зберігати інформацію про своїх клієнтів в абсолютній таємниці. Зловмисники не повинні знати про існування у вас рахунків і пластикових карток у тому або іншому банку.

Але це ще не все. Фішери розсилають листи всім підряд, і клієнти банку виявляються серед одержувачів випадково.

Сайт рекомендує:

• знайшовши в електронній пошті лист з банку, в якому ви тримаєте свої гроші, з проханням звірити паролі і номер рахунку, не поспішайте слідувати його вказівкам. Справжнім автором послання можуть бути шахраї, що вимагають персональні дані ваших банківських рахунків і кредиток;

• у разі щойменших підозр (ви одержали підозрілий лист або знайшли операцію по рахунку, яку ви не здійснювали), негайно зверніться в банк і перешліть даний лист за електронною адресою в службу інформаційної безпеки банку.

Одержавши сигнал, банк може перевірити підозрілі операції, зокрема особисто зв'язуючись з клієнтом. Крім того, атаковані банки можуть застосовувати й інші заходи захисту: припинення ряду операцій, наприклад, грошових платежів і валютних переказів, генерації ключів.

Корпорація Microsoft на своєму сайті рекомендує перевіряти наявність шифрування даних при введенні через Інтернет персональної або фінансової інформації, користуючись перевіреними, а не надісланими поштою адресами.

Сайт також повідомляє про можливості програмного захисту, хоча вони не дуже надають оптимізму – у нову версію браузера Internet Explorer 7.0 вбудований спеціальний фішинг-фільтр, що дозволяє автоматично перевіряти відвідуваний сайт на добросовісність. Втім, перевірку можна відключити, та і розпізнаються, на жаль, не всі підроблені сторінки.

Розвиток міжнародно-правової, економічної, фінансової, банківської, правоохоронної та інших форм співробітництва, що передбачає вільний рух інформаційних ресурсів щодо товарів, капіталів і послуг за умов застосування інформаційно-комп'ютерних технологій та мереж, збільшення потоків персональних даних і підтримання суверенітету держави визначають об'єктивну необхідність захисту персональних даних.

Враховуючи активність застосування інформаційно-комп'ютерних технологій та мереж і загрозу несанкціонованої автоматизованої обробки персональних даних, більшість європейських країн прийняли спеціальні закони та підписали Конвенцію РС № 108 від 28.01.1981 р. "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних". Принципи Конвенції були конкретизовані у Директиві 95/46/СС Європейського Парламенту та Ради від 24.10.1995 р. "Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних", а також у Директиві 97/66/СС Європейського парламенту та Ради від 15.12.1997 р. "Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі". Ці акти є міжнародними стандартами, що визначають принципи гармонізації національних законодавств у сфері захисту персональних даних як для європейських, так й інших країн світу.

Як зазначалося у підрозділі 3.2.2 цього дослідження – питання запровадження в Україні міжнародних принципів із захисту персональних даних практично не вирішене.

Зокрема, у банківському законодавстві такі поняття, як "персональні дані" та "захист персональних даних", що є основними поняттями європейських стандартів, не використовуються. Це передбачає внесення відповідних змін у банківське законодавство.

Системи електронного банкінгу. Будь-яка система банківської діяльності передбачає здійснення операцій із фінансових повідомлень та розрахунків.

Поява інформаційно-комп'ютерних технологій та мереж привела до запровадження електронних систем обробки даних та сприяла у змінах щодо технологій вирішення питань банківських справ та торговельної діяльності, зокрема щодо електронно-фінансових повідомлень та електронних розрахунків (далі – е-платежів).

Сьогодні фінансові установи вдосконалюють не тільки системи е-платежів між банками, але й системи "банк-клієнт", що дозволяють клієнтам банку управляти своїми рахунками по телефонній лінії, мережах мобільного зв'язку та через Інтернет. Вже є понад 20 технологій щодо е-банкінгу, які дозволяють здійснювати е-платежі через телекомунікаційні канали (мережі) обслуговування [57, с. 89].

Канали обслуговування та допоміжні системи. Електронний банкінг має наступні канали обслуговування [223, с. 18]:

- Інтернет-банкінг;
- РС-банкінг;
- Mobile-банкінг (мобільний банкінг, або м-банкінг).

Інтернет-банкінг використовується для роботи в режимі "он-лайн", тобто дозволяє управляти своїми рахунками в режимі реального часу з будь-якої країни світу. Для роботи клієнту потрібен сучасний комп'ютер з будь-якою операційною системою (Windows, Linux і ін.), будь-яким веб-браузером (Internet Explorer, Netscape і ін.) і доступом до Інтернету.

В Інтернет-банкінгу для корпоративних клієнтів вбудовані функції обміну документами з бухгалтерськими програмами клієнтів. Підтримується імпорт і експорт всіх типів документів через обмін файлами в текстовому форматі.

РС-банкінг використовується для роботи в режимі "офф-лайн". Робота з документами, довідниками, імпорт документів з бухгалтерських програм, підпис документів, отримання виписок не вимагають підключення до Інтернету.

У функціональному плані РС-банкінг повністю ідентичний Інтернет-банкінгу – підтримується єдиний призначений для користувача інтерфейс, єдині типи документів, єдині екранні і друковані форми, єдина бізнес-логіка, єдині довідники, єдині механізми взаємодії з бухгалтерськими програмами, єдині механізми захисту інформації.

Клієнти з не швидкісним і неякісним доступом до Інтернету, а також клієнти, які не бажають працювати через Інтернет, можуть завдяки своєму модему підключитися безпосередньо до банківського модемного пулу. Час, що витрачається клієнтом на передачу-прийом 50 платіжних документів, становить понад 40 – 60 секунд.

Синхронізація з банком – передача до банку фінансових документів, завантаження виписок, синхронізація довідників, завантаження оновлень клієнтської компоненти РС-банкінгу – відбувається через захищене з'єднання по TCP/IP (протокол передачі даних, або протокол Інтернету) [83, с. 60].

РС-банкінг забезпечує гарантований рівень безпеки, містить механізм е-підпису під фінансовими документами. Всі дані шифруються із застосуванням криптографічних алгоритмів, здійснюється контроль цілісності даних, що передаються.

Mobile-банкінг реалізує концепцію "банк на долоні" і забезпечує цілодобовий, мобільний і повнофункціональний доступ до послуг е-банкінгу.

Mobile-банкінг призначений для роботи в "он-лайні" та дозволяє корпоративним клієнтам управляти банківськими рахунками з персонального комп'ютера або мобільного телефону з доступом до Інтернету.

Клієнти можуть формувати і відправляти до банку платіжні доручення, працювати з довідником, відстежувати статуси документів, одержувати виписки за рахунками за будь-який період, обмінюватися з банком листами.

Mobile-банкінг містить механізм е-підпису під фінансовими документами, забезпечує гарантований рівень безпеки. Дані шифруються із застосуванням криптоалгоритмів, забезпечується контроль цілісності даних, що передаються. Секретні ключі е-підпису клієнта зберігаються у зашифрованому вигляді в пам'яті комп'ютера або на відчужуваних носіях.

Версії е-банкінгу. Слід зазначити: скільки банків, стільки і версій е-банкінгу, які бувають "важкі" і "легкі".

"Важка" версія. Користувачу потрібно на свій комп'ютер встановити програму і підключити до системного блоку комп'ютера спеціальний адаптер. Кожного разу для підтвердження проведення будь-якої операції потрібно притуляти до цього адаптера електронну "пігулку", схожу на ту, що використовується для замка під'їзного будинкофону. Проблема може виникнути при установці програми на робочому місці в офісі, де адміністратори мережі забороняють відкривати IP-порти.

"Легка" версія. Користувачу системи для доступу до своїх коштів потрібно зайти через Інтернет на сайт банку, ввести номер своєї банківської пластикової картки і PIN-код.

До допоміжних систем е-банкінгу відносяться:

а) системи доступу.

Клієнтам можуть на вибір пропонуватися варіанти систем доступу.

Простіший доступ – система на основі сесійних ключів, коли для проведення кожної операції користувачем вводиться окремий ключ (послідовність символів) відповідно до запропонованого системою номера.

Складніший і безпечніший доступ – система на основі електронного цифрового підпису, який користувач зберігає на зручному для себе носії (комп'ютер, дискета, CD або флеш-карта) і використовує його для підпису розпоряджень, що відправляються до банку;

б) тарифи.

Від банку до банку вони сильно відрізняються. Включають три складові:

- плата за підключення;
- абонентна плата;
- комісії за проведення різного виду платежів.

Плата за підключення все рідше використовується банками і стягується переважно за надання технологічних складових системи.

Абонентна плата практикується всіма банками. В окремих банках вона стягується за пакет послуг, що включає оплату за послуги Інтернет-банкінгу та пластикову картку.

Комісія за здійснення е-платежів включає відсоток від суми платежу, але не менш визначеної банком мінімальної суми (наприклад, комісія може становити 0,2 %).

Банківська пластикова картка. Банківська пластикова картка – це іменний електронно-розрахунковий документ, що видається банком, за допомогою якого здійснюється оплата товарів і послуг [223, с. 19].

Кожна картка містить реквізити власника картки (адресу і код банку та відділення, номер його рахунку, розпізнавальний знак (ПІБ, адресу тощо, тобто – персональні дані), що відповідають персональному ідентифікаційному номеру (PIN-коду) власника,

строк її дії, максимальну суму, яку має в розпорядженні власник картки і яка зменшується при кожному знятті коштів з рахунку). Це мінімально необхідний перелік даних, що дозволяє ідентифікувати та встановити платоспроможність клієнта. Потім здійснюється звичайна банківська операція, і гроші з одного банківського рахунку переводяться на інший. Після того, як продавець одержить підтвердження про переведення грошей на його рахунок, товар передається покупцеві.

Існують різні види карток, які розрізняються за функцією, технологічними особливостями і механізмом розрахунків.

За функціональними ознаками розрізняють кредитні картки і дебетові картки, які у свою чергу можуть бути "звичайними" або "золотими". Останні призначаються для осіб з високою кредитоспроможністю і передбачають пільги для користувачів.

За технологічними особливостями найпоширеніші картки двох видів – з магнітною смугою і з вбудованою мікросхемою. Картки з магнітною смугою мають декілька доріжок для фіксації в закодованій формі даних, необхідних для ідентифікації особи власника картки при її використанні в банківських автоматах і електронних терміналах торговельних закладів.

За механізмом розрахунків виділяють двосторонні і багатосторонні системи. Двосторонні картки виникли на базі двосторонніх угод між учасниками розрахунків, які можуть використовувати картки для купівлі товарів у замкнутих мережах, контрольованих емітентом карток (універмаги, бензоколонки тощо). Кредит надає сама компанія, вона ж отримує процент за позичками.

Дістали поширення також банківські приватні та корпоративні картки, за допомогою яких можна здійснити купівлю зі знижкою в окремих магазинах, але випуск карток, видачу кредиту за покупками і розрахунки за оплатою торгових рахунків здійснює банк-учасник угоди. Іноді такі картки випускаються для членів певних професійних груп (пілотів, адвокатів) або осіб, пов'язаних спільними інтересами (наприклад, філателістів), їх називають "клубними" картками. У багатосторонній системі широко використовуються картки міжнародних кредитно-фінансових груп VISA, EuroCard, Master Card, American Express, які дають можливість купувати товари в різних точках земної кулі у різних торговельних мережах і організаціях сервісу, котрі визнають ці картки як платіжний засіб.

При, здавалося б, плюсах карткової форми розрахунків відомі фінансові структури Visa, Master Card не радять клієнтам здійснювати платежі через Інтернет. Головна проблема полягає в тому, що інформація передається у відкритому вигляді і може бути скопійована, змінена чи перехоплена. Крім того, покупець може опротестувати будь-яку операцію з його карткою при відсутності первинних документів. Ця проблема передбачає необхідність створення первинних паперових документів, щоб потім можна було використовувати їх як доказ здійснення операції, навіть у суді.

Смарт-картка – це картка з мікросхемою, що має здатність змінювати її стан в інтерактивному режимі. Такі картки називають також "інтелектуальними" картками. Вбудована в картку мікросхема (чіп) складається з пристроїв для збереження інформації та процесора, який сам по собі є комп'ютером і здатний обробляти інформацію, записану в запам'ятовуючих пристроях. На основі записаних у мікросхемі відомостей трансакція з використанням картки може здійснюватись в автономному режимі (off-line), тобто без безпосереднього зв'язку з центральним процесором банківської комп'ютерної системи в момент здійснення трансакції. Оскільки картка сама зберігає в пам'яті суму коштів, які перебувають на банківському рахунку, то авторизації тут не потрібно: якщо ліміт перевищений, трансакція не відбудеться. Якщо ж сума трансакції менша від суми ліміту, то в момент її здійснення сума вільного ліміту буде зменшена і запишеться новий залишок, який може бути використаний при наступній покупці. При внесенні грошей на рахунок ліміт поновлюється, про що робиться новий запис у мікросхемі.

Інформаційні можливості картки з мікросхемою значно ширші, ніж у карток з магнітною смугою (якщо картка з магнітною смугою дозволяє зберігати інформацію обсягом в 1 тис. біт, то картка з мікросхемою – 8 тис. біт). Якщо картка з магнітною смугою є лише пасивним засобом зберігання інформації, то картка з мікросхемою може реагувати і записувати у свою пам'ять дані про раніше виконані трансакції. Важливою перевагою картки з мікропроцесором є також її висока надійність. Злочинці швидко навчилися розпізнавати секретні коди карток з магнітною смугою, викрадати їх або виготовляти фальшиві картки і використовувати їх в автоматах для видачі готівки. Мікросхему імітувати важче. Вона має декілька ступенів захисту, і підробити інформацію, записану в ній, важко або взагалі неможливо. Якщо картка викрадена і привласнювач захоче скористатися нею для одержання грошей в автоматі, то при неправильному введенні PIN-коду мікросхема руйнується, і картка не може більше використана.

Кредитні та дебетні картки можуть існувати як на основі карток з магнітною смугою, так і на основі карток з мікросхемою, але "електронний гаманець" потребує використання смарт-картки. Більшість емітентів замінюють існуючі картки з магнітною смугою на картки з мікросхемою, щоб усі види карткових послуг можна було надавати з використанням однієї картки. Щоправда, картки з мікросхемою мають відносно високу вартість (у 5 – 7 разів більшу порівняно з магнітною карткою). Крім того, їх введення в обіг у країнах, які з початку створення системи карткових розрахунків орієнтувались на магнітні картки, ускладнене, оскільки заміна обладнання, сумісного зі смарт-картками, вимагає великих капіталовкладень.

Електронно-цифровий підпис. Усі проблеми електронної економіки й інших договірних відносин нерозривно пов'язані з підтвердженням правомірності угод, що укладаються за допомогою засобів забезпечення інформаційної взаємодії різних суб'єктів у е-середовищі. Основою правомірності зобов'язань сьогодні вважається юридичне закріплення е-підпису [232].

У державах-членах ЄС узгодження і гармонізація національних законів, постанов і адміністративних положень здійснюється згідно з Директивою 99/93/ЄС Європейського Парламенту і Ради "Про систему електронних підписів, що застосовується в межах Співтовариства" від 13.12.1999 р. [81, с. 345]. Метою цієї Директиви є сприяння застосування електронних підписів та їх юридичному визнанню. Вона закладає правову основу для здійснення певних послуг з сертифікації з метою забезпечення належного функціонування внутрішнього ринку. Директива не охоплює аспектів, що стосуються укладання і чинності контрактів чи інших правових зобов'язань, якщо мають місце вимоги, передбачені формою, визначеною внутрішнім законодавством чи законодавством держав Співтовариства, так само як вона не впливає на правила і обмеження застосування документів, що містяться у внутрішньому законодавстві чи законодавстві держав Співтовариства.

В Україні правовий статус електронного цифрового підпису та регулювання відносин, що виникають при його застосуванні, визначається згідно із Законом України "Про електронний цифровий підпис" від 22.05.2003 р. [34].

Головна відмінність е-підпису від звичайного підпису полягає в тому, що цифровим підписом завіряється не папір чи носій, а сам зміст документа, тобто відомості, що містяться в ньому. Саме е-підпис є тим інструментом, що дозволяє створити правові основи для:

- електронного (цифрового) документообігу в мережах;
- становлення платіжних систем нового типу і цінних електронних паперів;
- укладання угод за допомогою мереж.

Фізична сутність е-підпису полягає в наступному.

Зміст документа (файла) в комп'ютері подано як послідовність байтів і тому може бути однозначно описано визначеним (довгим) числом чи послідовністю декількох коротших чисел. Щоб скоротити цю послідовність, не втративши її унікальності, застосовують спеціальні математичні алгоритми, такі як контрольна сума або хеш-функція. Якщо кожен байт файла помножити на його номер (позицію) у файлі й отримані результати підсумувати, то вийде коротше порівняно з довжиною файла число. Зміна будь-якого байта у вихідному файлі змінює підсумкове число. На практиці застосовуються більш складні алгоритми, що виключають можливість введення такої комбінації перетворень, за якої підсумкове число залишилося б незмінним. Хеш-функція визначається як унікальне число, отримане з вихідного файла шляхом його "обрахування" за допомогою складного алгоритму.

Щодо технічного аспекту одержання е-підпису. Давно відомий криптографічний метод за допомогою симетричного ключа (названий симетричним шифруванням), при використанні якого для шифрування і розшифровування служить той самий ключ (шифр, спосіб). Головною проблемою симетричного шифрування є конфіденційність передачі ключа від відправника до одержувача. Розкриття ключа в процесі передачі рівносильне розкриттю документа і наданню зловмисникові можливості його підробити.

У 1970-х рр. був винайдений алгоритм асиметричного шифрування. Суть його полягає в тому, що зашифровується документ одним ключем, а розшифровується іншим, причому по першому з них практично неможливо вирахувати другий, і навпаки. Тому якщо відправник зашифрує документ секретним ключем, а публічний, чи відкритий, ключ надасть адресатам, то вони зможуть розшифрувати документ, зашифрований відправником, і тільки ним. Ніхто інший, не володіючи секретним ключем відправника, не зможе так зашифрувати документ, щоб він розшифровувався парним до секретного відкритим ключем.

Відправник, обчисливши хеш-функцію документа, зашифровує її значення своїм секретним ключем і передає результат разом з текстом документа. Одержувач за таким же алгоритмом вираховує хеш-функцію документа, потім за допомогою наданого йому відправником відкритого ключа розшифровує передане значення хеш-функції і порівнює вирахуване і розшифроване значення. Якщо одержувач зміг розшифрувати значення хеш-функції, використовуючи відкритий ключ відправника, то зашифрував це значення саме відправник. Чужий чи перекручений ключ нічого не розшифрує. Якщо вирахуване і розшифроване значення хеш-функції збігаються, то документ не був змінений. Будь-яка зміна змісту (навмисна чи ненавмисна) документа в процесі передачі дасть нове значення хеш-функції, що вираховується одержувачем, і програма перевірки підпису повідомить, що підпис під документом невірний.

Таким чином, на відміну від власноручного підпису, е-підпис нерозривно пов'язаний не з певною особою, а з документом і секретним ключем. Якщо дискетою з вашим секретним ключем заволодіє хтось інший, то він, природно, зможе ставити підписи за вас. Однак ваш е-підпис не можна перенести з одного документа на який-небудь інший, його неможливо скопіювати, підробити – під кожним документом він унікальний. Процедури збереження, використання, відновлення і знищення ключів досить детально розписані в різних методичних рекомендаціях до систем е-підпису.

Процес шифрування інформації асиметричними ключами здійснюється в такий спосіб. Якщо поміняти ключі місцями, іншими словами, секретним зробити ключ розшифровування, а відкритим ключ шифрування, то відправник може зашифрувати лист відкритим ключем одержувача, і тоді прочитати лист зуміє лише той, у кого є секретний парний ключ, тобто тільки сам одержувач. Велика перевага асиметричної схеми шифрування полягає в тому, що відпадає необхідність у конфіденційній передачі ключів. Відкритий ключ можна зробити доступним на веб-сайті, передати е-поштою і т. п., не побоюючись наслідків доступу до нього третіх осіб.

Для зручності шифрування і застосування е-підпису в корпоративних системах із великою кількістю абонентів застосовують довідники відкритих ключів. Кожен ключ має тіло і номер, однаковий для секретної і відкритої частин ключа й унікальний для кожного абонента. Номер передається відкрито в заголовку зашифрованого документа чи в заголовку е-підпису. Одержувач по цьому номеру з відповідного довідника вибирає сам ключ, що підставляється в процедуру розшифровування або перевірки підпису. Виконується така вибірка, як правило, за допомогою спеціальних програм, і вся процедура займає частки секунди.

Важливу роль у системі діловодства, що застосовує е-підпис, відіграє адміністрація системи. Вона забезпечує контроль за дотриманням абонентами єдиних правил роботи, бере участь в аналізі конфліктних ситуацій, керує ключовою системою ключів і, що важливо, підтримує у всіх абонентів довідники відкритих ключів в актуальному стані. Довідники змінюються регулярно: при будь-якій зміні списку учасників, при заміні ключів. Необхідність заміни ключів виникає, скажімо, у випадку їх компрометації – мається на увазі ряд подій, за яких ключова інформація стає недоступною чи виникає підозра несанкціонованого доступу. До таких подій відносяться: утрата дискет з ключами, їх ушкодження, звільнення співробітника, що мав доступ до даних щодо ключів, порушення правил збереження і знищення секретних ключів та ін.

При виникненні подібної ситуації учасник системи зобов'язаний негайно повідомити адміністрацію системи (чи її підрозділ – центр керування системою ключів) про факт компрометації. Адміністрація має блокувати відкритий ключ учасника в довіднику і сповістити про це інших учасників (обновити в них довідники). Фіксація моменту повідомлення адміністрації про компрометацію ключів дуже важлива. Дійсними вважаються тільки ті документи учасника, що були отримані до цього моменту. Цей факт враховується при аналізі конфліктних ситуацій, за якого, насамперед, здійснюється перевірка, чи був ключ відправника чинним на момент одержання документа адресатом.

У тому випадку, коли в корпоративній системі передбачений обмін е-документами лише між центром (банком, брокерською фірмою, холдингом) і його клієнтами, клієнтам досить знати тільки один відкритий ключ е-підпису цього центру, останній же використовує довідник відкритих ключів усіх клієнтів. Якщо ж у системі передбачена можливість обміну е-документами між абонентами прямо, то довідники з переліками відкритих ключів мають бути у всіх учасників і обновлятися одночасно.

Електронні гроші як інструмент е-банкінгу. Електронні гроші (далі – е-гроші) – це еквівалент безготівкових коштів, виражених в електронній формі у вигляді файлів. Вони є одним з перспективних розрахункових інструментів забезпечення електронної банківської діяльності в рамках платіжних систем, що функціонують на основі банківських карток і телекомунікаційних мереж.

Загальна схема дій системи щодо е-грошей така: банк одержує від клієнта звичайні гроші і видає розписку про їх одержання, завірену е-підписом банку. Цей підпис, занесений на носій даних (на смарт-картку), є свідченням про наявність у банку клієнта

відповідної суми грошей. Дані щодо смарт-картки потім можуть бути передані через мережу. Головна технічна проблема – запобігання появі фальшивих е-грошей, тобто копіювання з одного носія на інший. Для цього використовується зв'язок у режимі реального часу з банком-емітентом.

Рівень поступової комерціалізації Інтернету почав досягати економічно значущих величин у другій половині 1990-х рр. Приблизно у цей період між основними компаніями комп'ютерної індустрії починається боротьба за створення і впровадження стандарту так званих "електронних грошей", які стали б гнучким, швидким і універсальним засобом оплати. Гроші, в якості матеріального виразу (носія) яких у наш час переважно використовуються банкноти і монети, недовговічні, схильні до природних процесів зносу (старіння), а значить, їх обіг пов'язаний з великими затратами для емітента. Наявні грошові знаки (на відміну від інформаційно-цифрових даних) доводиться періодично вилучати з обігу і замінювати новими, тієї ж номінації. Кожна банкнота і монета мають певну собівартість, причому собівартість виробництва грошових знаків нижчої вартості відносно дорожча (порівнянні з номіналом), ніж собівартість банкнот і монет вищої вартості. До того ж, для перерахунку, інкасування, перевезення і зберігання традиційних грошей потрібні додаткові витрати.

Електронні гроші є юридично значимими інформаційно-цифровими даними (імпульсами) і тому позбавлені названих недоліків. Собівартість розрахунків, що здійснюються в електронній формі, нікчемна мала.

Слід зазначити, що робота над створенням дослідних систем стандартів е-грошей провідними комп'ютерними корпораціями-розробниками програмного забезпечення здійснювалася в тісній співпраці з банками і небанківськими фінансовими структурами.

Американський банк First Virtual Holding став першою легальною кредитною установою, що приступила до банківської діяльності в Інтернеті (тобто першим віртуальним банком). У жовтні 1994 р. банк почав застосовувати електронну пошту для здійснення операцій з невеликими грошовими сумами. Фахівці комп'ютерної імперії Microsoft і міжнародної платіжної системи банківських карток Visa спільно розробили систему оплати товарів (послуг) в комп'ютерних мережах з застосуванням банківських кредитних карток. Британські банки National Westminster і Midlend реалізували на практиці систему цифрових грошей Mondeks на основі смарт-карток з вбудованим мікропроцесором, що зберігає інформацію про власника. Корпорація Netscape Communications Corp. (США) разом з компаніями Microsoft, Mastercard, Bank of America і американською телекомунікаційною компанією MCI однією з перших розробила програмне забезпечення для фінансових операцій в діловій частині мережі Інтернет [224, с. 119].

У лютому 1995 р. англійський Barclays Bank став першим великим європейським банком, що здійснював підприємницьку діяльність з застосуванням Інтернету. На спеціальному веб-сайті банку була відкрита Інтернет-вітрина (Інтернет-магазин) з продажу вин, іграшок, а також залізничних квитків. Клієнти банку змогли проглядати каталоги і використовувати номери своїх банківських кредитних карток для оплати товарів, що доставляються їм кур'єром до будинку. Проект банку Barclays вперше дозволив від рекламних перейти до повноцінних банківських операцій в Інтернеті. Покупці на основі електронних каталогів товарів заповнювали електронні бланки замовлень. Бланк з вказівкою відомостей про кредитну картку покупця шифрувався і враховувався банком. На первинному етапі з міркувань безпеки даних банк не надавав доступ до банківських рахунків клієнтів, і вони не могли здійснювати управління своїми банківськими рахунками на відстані. Потім це обмеження було скасовано.

У той час коли традиційна комп'ютеризація в банках продовжувалася, виникали і нові стратегії. Першими проектами в області кредитних послуг за допомогою Інтернету, стали розробки корпорацій Internet Corp. (програма домашніх банківських послуг), Microsoft (програма е-платежів і управління особистими фінансами) і банків – партнерів Bank of America (програмне забезпечення для управління особистими фінансами). Сьогодні господарюючі суб'єкти можуть одночасно застосовувати декілька варіантів систем е-грошей.

Сучасні е-гроші є певною послідовністю цифр, які символізують (замінюють) банкноти і монети, і в цьому полягає їх інформаційна природа. З їх допомогою можна придбати товари (послуги) в режимі реального часу з застосуванням інструментів дистанційного управління банківським рахунком (наприклад комп'ютер, підключений до мережі Інтернет, звичайний телефон (Інтернет-банкінг), мобільний телефон, що підтримує стандарт WAP (м-банкінг), банківські пластикові картки (карткові електронні банківські послуги або картковий банкінг). За прогнозами фахівців, у перспективі е-гроші, у разі певного розвитку, можуть потіснити, а потім і частково витіснити традиційні грошові знаки.

Як наголошувалося, перший віртуальний банк, що здійснював банківську діяльність виключно в мережі Інтернет, був створений в 1994 р. в рамках американського мережевого кредитно-карткового проекту First Virtual Holding. Технологічною основою здійснення банківських операцій стало застосування електронної пошти. Відповідно до технології функціонування цієї системи е-платежів номера банківських кредитних карток клієнтів заносяться до захищеної комп'ютерної системи і ніколи не виходять за межі мережі. Замість них видається ідентифікаційний персональний номер для оплати електронних покупок.

За різними оцінками, в Інтернеті функціонує понад 620 віртуальних банків. При цьому, важливою з погляду податкового права і законодавства про захист прав споживачів стає та обставина, що підприємницьку діяльність в Інтернеті здійснюють і віртуальні банки. Вони повинні мати спеціальний дозвіл (ліцензію) на ведення банківської діяльності, одержаний відповідно до порядку, встановленого національним законодавством країни їх фактичного резидентства або реєстрації First Virtual Holding.

При збереженні сьогоднішніх темпів розвитку е-платежів і електронних фінансових послуг е-гроші здатні, по-перше, змінити наше уявлення про правову і економічну природу грошових знаків. По-друге, привести до зміни статусу і ролі банків як фінансових інститутів. І, по-третє, істотно підірвати національні фінансові системи (особливо в державах із слабкою ринковою економікою) і позиції центральних банків як регуляторів національної банківської системи.

Визначаючою перспективою е-грошей стане відповідь на питання, чи зможуть цифрові грошові знаки виконувати такі основні функції традиційних грошей, як обміну і накопичення. Крім того, на сьогоднішньому рівні розвитку інформаційних технологій фахівцям поки не вдасться вирішити проблему анонімності грошових знаків, виражених в електронній формі.

Все викладене свідчить про те, що випуск і обіг е-грошей вимагає жорсткого правового регулювання на користь самих учасників цих відносин (користувачів систем е-грошей).

За кордоном великий внесок у вивчення природи і перспектив е-грошей зробив відомий уельський фахівець в області банківського оподаткування і е-платежів А. Оперкент [224, с. 198]. У 1994 р. в одній із своїх робіт він зазначав, що е-гроші, швидше за все пропонуватимуться як банками, так і небанківськими організаціями. Якщо останні

зможуть видавати е-гроші безпосередньо споживачам, то істотно підірвуть клієнтську базу традиційних банків. Тоді банки самі будуть вимушені випускати в обіг власні е-гроші. Але може трапитися, що ринок вже буде зайнятий аналогічними рішеннями небанківських фірм. Важливою проблемою стане психологічна недовіра споживачів до нового продукту. Вбачається, що для того, щоб е-грошам вірили як паперовим банкнотам, вони повинні на першу вимогу обмінюватися на національну валюту. Але тоді кожній одиниці е-грошей повинна відповідати одиниця звичних грошей, підкріплена стабільним станом економіки цієї країни. Або, якщо поглянути на ситуацію з іншого боку, в реальному світі має бути відповідне грошове покриття е-грошей, які використовують для е-платежів. Тому в такій системі не повинно існувати електронного кредиту, адже він збільшує масу е-грошей без відповідного зростання кількості звичних грошових знаків, а це викликає інфляцію.

Важливе те, що зазначене зменшує для банків вигідність операцій з е-грошима. Вони стануть нецікавим і навіть шкідливим явищем. Звичайно, банки можуть брати комісію за конвертацію е-грошей або за ліцензування їх випуску, але конкуренція напевно зробить такий бізнес малоприбутковим. Все це ставить банки перед досить складною дилемою. І потім, держава звичайно жорстко регулює ринок переміщення і обміну іноземних валютних цінностей. Прагнення створити за допомогою е-грошей якийсь новий ринок валют примушує держави світу вживати у відповідь заходи, спрямовані на зміцнення національної фінансової системи. Тому на ранніх стадіях впровадження е-грошей важливо прирівняти їх до будь-якої умовної одиниці (або валюти) і обмінювати за звичним ринковим курсом нарівні з іншими валютами.

Можна припустити, що в обхід законів ринку і грошового обігу, а можливо, і законів держави, банки або небанківські (що швидше) структури все таки ризикнуть видавати електронні гроші в кредит. В цьому випадку такий кредит матиме ціну. Тоді, якщо держави світу домовляться, конвертування в традиційні валюти перестане бути необхідною умовою існування е-грошей. Вони можуть стати тотожними за функціями із звичайними банкнотами.

З погляду загальнолюдських цінностей — це буде прорив в інший вимір свободи. Але такі гроші перестануть бути прив'язані до держави, стануть наднаціональними, стануть, за визначенням К. Маркса, "світовими грошима". Це може за певної пасивності держави "розмивати" її фінансову основу, а за найнесприятливішим сценарієм призвести до краху існуючих банківської і податкової систем (якщо будуть порушені регуляторні функції держави щодо економіки, втрачений контроль за грошовою масою і розрахунками).

Проте, можливо, держава втрутиться в процес розвитку е-платежів, і деякі з е-грошей підтримуватимуться урядом, інші — приватними особами. У будь-якому випадку потенціал е-грошей величезний і дотепер достеменно не вивчений.

Визначення електронних грошей у європейських стандартах. Чинне українське законодавство не містить згадки про е-гроші і тому, природно, не містить і легального їх визначення. Не розглядається зазначене поняття і доктриною фінансового права. В Україні термін "електронні гроші" використовується лише в економічних і публіцистичних роботах.

У зарубіжних країнах поняття "електронні гроші" було введене в науковий обіг відносно недавно. На початку 1990-х рр. почалися дослідження Європейського інституту грошей (згодом на його базі був створений Європейський центральний банк), основним завданням яких стала спроба спрогнозувати можливі шляхи розвитку платіжних систем у країнах-членах Європейського Союзу. У 1994 р. за результатами проведе-

них досліджень була опублікована доповідь "Про передоплачені картки", яка торкнулася і проблем е-грошей [224, с. 200]. Одним з найважливіших положень доповіді став висновок про необхідність обмежити коло емітентів передоплачених карток тільки кредитними установами. Ця теза відображена в проекті Директиви, опублікованої у 1998 р. у вигляді пропозиції Комісії Європейського Союзу. В остаточному тексті Директиви вказана вимога була посилена введенням норми (ст. 1, п. 4), що рекомендує державам-членам Європейського Союзу "забороняти проведення емісії е-грошей особам або підприємствам, які не є кредитними установами". Як зазначають фахівці, введення прямої заборони іншим емітентам на емісію е-грошей свідчить про прагнення європейських законодавців ввести у сфері е-грошей достатньо жорстке регулювання – аналогічне тому, яке здійснюється у сфері банківської діяльності.

У Сполучених Штатах Америки аналогічні дослідження були проведені Міністерством фінансів в 1996 р. Проте в частині введення заборони на емісію е-грошей іншими емітентами в США запанував більш ліберальний підхід – заборони на неї немає.

У зв'язку з вказаними вище обставинами у документах Європейського Союзу було істотно розширене легальне визначення поняття "кредитна установа", що міститься в Директиві 2000/12/СС Європейського Парламенту і Ради від 20.03.2000 р. "Про кредитні установи". Ця зміна у понятті була внесена одночасно з ухваленням Директиви 2000/28/СС Європейського Парламенту і Ради "Про установи у сфері електронних грошей" [224 , с. 201]. Якщо раніше кредитна установа визначалася як "підприємство, діяльність якого полягає в ухваленні депозитів або інших таких, що належать поверненню, грошових коштів від необмеженого кола осіб і наданні кредитів за свій рахунок" (п. 1 ст. 1 Директиви 2000/12/СС "Про кредитні установи" в первинній редакції), то в даний час як:

"(а) підприємство, діяльність якого полягає в прийнятті депозитів або інших таких, що належать поверненню грошових коштів, від необмеженого кола осіб і наданні кредитів за свій рахунок; або

(б) установа у сфері електронних грошей відповідно до Директиви 2000/46/СС від 2000 р." (п. 1 ст. 1 Директиви СС 2000/12/СС "Про кредитні установи" в поточній редакції).

В Директиві 2000/46/СС поняття "установа у сфері електронних грошей" формулюється таким чином (п. 3(а) ст. 1): "підприємство або будь-яка інша юридична особа (інше, ніж кредитна установа, вказана в п. 1(а) ст. 1 Директиви 2000/12/СС), яка випускає засоби платежу у формі електронних грошей". Тепер організації-емітенти е-грошей включені до складу кредитних установ разом з класичними кредитно-грошовими інститутами.

Одне з перших визначень поняття "електронні гроші" було запропоновано в публікаціях економістів департаменту нової фінансової політики і департаменту економічних досліджень Європейського центрального банку. Так, в "Доповіді про електронні гроші" від 1998 р., дається наступне визначення: "електронні гроші в широкому значенні визначаються як електронне зберігання грошової вартості за допомогою технічного пристрою, який може широко застосовуватися для здійснення платежів на користь не тільки емітента, але й інших суб'єктів і яке не вимагає обов'язкового застосування банківських рахунків для проведення трансакцій, а діє як інструмент, що передоплачений, на пред'явника".

Пізніше, у вересні 2000 р., була прийнята Директива 2000/46/СС Європейського Парламенту і Ради від 18.09.2000 р. "Про відкриття і ведення діяльності установ-

емітентів електронних грошей, а також здійснення нагляду за цією діяльністю". У ній дається наступне уточнене визначення е-грошей:

"Електронні гроші є грошова вартість, що є вимогою до емітента, яка:

1) зберігається на електронному пристрої;

2) видається при отриманні коштів на суму, не меншу за вартістю, ніж випущена грошова цінність;

3) приймається як засіб платежу підприємствами, іншими, ніж емітент" (ст. 1 Директиви).

Закріплений в Директиві підхід до поняття "електронні гроші" має велике наукове і практичне значення. Ключовою ознакою в цьому визначенні є поняття "вимога до емітента". Слід підкреслити, що правова природа цієї вимоги відмінна від правової природи банківського вкладу. Основний критерій відмінності (він вказаний у п. 3 ст. 2 Директиви) – часовий (скільки часу минає між отриманням традиційних грошей емітентом і їх обміном на е-гроші; причому у Директиві використовується саме термін "обмін", а не "емісія"). Негайний обмін виключає застосування норм Директиви щодо внесків до кредитних установ (ці положення діють тільки при обміні після закінчення певного періоду) [233].

На думку зарубіжних дослідників, в юридичних питаннях види е-грошей слід поділяти на е-гроші, які обертаються в рамках систем, що функціонують на:

а) основі банківських карток, і

б) на базі комп'ютерних мереж.

До першого виду відноситься грошова вартість, що виражена в електронній формі і зберігається на банківських пластикових картках (смарт-картках) або в електронних гаманцях, що мають вбудований мікропроцесор із записаним на ньому у результаті передоплати грошовим еквівалентом. Тобто, до е-грошей такого виду слід відносити лише багатоцільові картки (тобто картки, що запроваджені для платежів на користь не тільки самих емітентів карток, а й інших юридичних і фізичних осіб).

Поширеними е-грошима на базі пластикових карток вважаються Mondex та Viza Cash. В якості емітентів і платників за цими картками виступають банки, а основа грошового еквівалента, що зберігається і переміщується за їх допомогою, – банківські депозити.

Принципово нове явище в цій групі – картки, що випускаються телефонними, транспортними та ін. компаніями і приймаються до оплати широким колом суб'єктів (наприклад, картки Управління міського транспорту Нью-Йорка або картки деяких телефонних компаній в Росії і Японії). Якщо в майбутньому такі картки стануть приймати велика кількість фірм, то розрахунки за ними проводитимуться вже не через банки, а через бухгалтерські документи компаній-емітентів.

Як відзначають фахівці, банківські гроші (які піддаються регулюванню з боку центральних банків) використовуються лише як початкова ланка вартісного ланцюжка: покупець картки платить за неї або готівкою, або банківським чеком. При подальших трансакціях необхідність в підтримці залишків на банківських рахунках (просто в інформуванні фінансових установ про здійснення операцій) відпадає. Цим скорочується потреба комерційних банків у коштах, що зберігаються на резервних або розрахункових рахунках у центральних банках.

До другого виду е-грошей відносяться так звані "мережні гроші", при обігу яких грошова вартість зберігається в пам'яті комп'ютерів на жорстких дисках. Вони беруть участь в грошовому обігу за допомогою різних програм, що забезпечують переказ коштів по телекомунікаціях, зокрема через Інтернет. Деякі зарубіжні фахівці до цього відносять пристрої доступу – касові апарати, системи дистанційних банківських послуг через телефон або через комп'ютер.

Вважається, що з часом е-гроші першої групи можуть почати витісняти традиційну готівку і чеки, тоді як е-гроші другої групи прийдуть на зміну банківським карткам, а також візьмуть на себе розрахункові функції в обхід банків.

Сьогодні існує безліч систем е-банкінгу й інструментарію його реалізації, які впроваджуються банками повсюдно. Найбільша активність виявляється на корпоративному рівні. Разом з тим, загальноприйнятої методики забезпечення надійності, легітимності і безпеки банківського обслуговування та захисту даних завдяки відкритості мережевих систем не виявлено. Як вважається, вирішення цих питань потребує визначення базових принципів забезпечення надійності зазначених видів дистанційного банківського обслуговування.

3.2.5. Електронне урядування

До законів України, які стосуються сфери електронного урядування (е-урядування), відносяться:

Закон України "Про інформацію" від 1992 р.;

Закон України "Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації" від 1997 р.;

Закон України " Про Національну програму інформатизації" від 1998 р., а також укази Президента України:

"Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні" від 2000 р.;

"Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади" від 2002 р.;

"Про заходи щодо забезпечення інформаційної безпеки держави" від 2002 р. та інші акти, зазначені у [95].

Як зазначається у [238], за визначенням Європейської Комісії, "електронний уряд" це застосування інформаційних і комунікаційних технологій у державних адміністративних органах у поєднанні з організаційними змінами і новими методами для поліпшення послуг державного сектору і демократичних процесів, а також зміцнення підтримки політики держави. Тобто поняття "електронний уряд" означає систему електронного урядування за допомогою якої, завдяки застосуванню органами влади сучасних технологій та мереж, зокрема Інтернет-технологій, державою здійснюється інформування суспільства, надання послуг та нормативно-правове регулювання суспільних відносин.

Розвиток інформаційної інфраструктури і цільового застосування інформаційних ресурсів у країнах ЄС і США зумовив появу та певне функціонування різних модулів (складових) системи е-урядування: "уряд-громадяни" (модуль G2C, government-to-citizens), "уряд-бізнес" (модуль G2B, government-to-buiness), "уряд-уряд" (модуль G2G, government-to-government), а також універсального модуля – "уряд-демократія" (модуль G2D, government-to-democratization), про що досить докладно йдеться у [83, с. 96-103; 238, с. 81-105].

Модуль G2C. Складова "уряд-громадяни" передбачає надання органами державної влади соціально-інформаційних послуг громадянам (розгляд і відповіді на запити, скарги, пропозиції, звернення, надання і забезпечення захисту персональних даних та ін.), інформації про послуги, що сприяє взаємодії громадськості з урядовими агентствами, дозволяє здійснювати інтерактивні платежі та багато ін. Ціль модуля – відкриття для громадян структур влади шляхом вільного доступу на веб-сторінку через певні портали.

Модуль G2B. Складова "уряд-бізнес" стосується питань обслуговування приватного бізнесу, економічного розвитку, питань патентування, ліцензування. Ціль модуля – прискорення процесів діяльності приватного бізнесу шляхом спрощення процедури оформлення платежів, кредитів, ліцензій, пільг, надання можливості участі в роботі е-тендерів, що проводяться урядом і т. ін.

Модуль G2G. Складова "уряд-уряд" (е-уряд, модуль G2G) поліпшує взаємодію, якість і швидкість інформаційного обміну між різними організаціями державної влади в межах урядової структури. Ціль модуля – прискорення вирішення поточних питань, ведення діловодства на безпаперовій основі, здешевлення роботи і підтримки інформаційної безпеки держави. По суті, модуль передбачає створення урядового Інтранету - "держави в державі". Така комунікація допомагає різним державним службам використовувати урядові ресурси більш раціонально, оперативно, уникати дублювання, створити механізм аналізу того, що робиться, і (що важливо), мати прозорі бюджетні процедури.

Універсальний модуль G2D. Складова "уряд-демократія" є урядовим порталом забезпечення масштабного розвитку демократії й обслуговування суспільства у сфері захисту прав людини, екологічних аспектів, перерозподілу зон пріоритетної компетенції державних і суспільних структур, використання бюджету й ін. Ціль модуля – надання громадянам публічної інформації про діяльність органів державної влади і можливості широкого обговорення питань управління і розвитку суспільства і держави. Цей портал будується за тематичним напрямом інформаційних ресурсів, а потім – за відомчою приналежністю. Модуль G2D припускає реалізацію он-лайнового голосування (е-голосування) через Інтернет. Однак на сьогодні існують три серйозні технологічні проблеми, що перешкоджають його швидкому розгортанню, – корупція, слабкість інфраструктури всесвітньої мережі і кіберзлочинність (хакерство).

Як уже зазначалось, е-урядування має на меті забезпечити прозорість діяльності парламенту і чиновників для громадян, що повинна вийти на якісно новий рівень. Інформатизація роботи всіх органів державного управління несе із собою поліпшення якості наданих населенню послуг і сприйняття громадян як споживачів, а не як прохачів. Інтернет-доступ до інформації, якою володіють установи влади, – від законодавства, підзаконних нормативних актів і відомчих інструкцій до поточної інформації про робочі місця, продукти харчування та ін. – повинен змінити не тільки умови життя громадян, але й саме їх ставлення до влади.

У принципі, говорячи про е-урядування, необхідно розрізняти традиційні державні інститути, забезпечені он-лайновим інтерфейсом, і безпосередній е-уряд як ідею.

Он-лайновий зв'язок тією чи іншою мірою розвивається сьогодні повсюди, у тому числі й в Україні, де його проявом з певною натяжкою можна вважати інтерактивні можливості віртуальних представництв різних держструктур.

Для побудови ж е-урядування потрібна більш глибока перебудова всіх традиційних форм діяльності. Точніше, у разі успіху цієї програми зміниться сама парадигма державного управління, і механізм державної машини, хочеться сподіватися, у меншій мірі буде працювати в основному на себе. Створення е-урядування приведе не тільки до більш ефективного і менш витратного адміністрування, але й до кардинальної зміни взаємовідносин між населенням і урядом. Процес управління стане більш прозорим і відкритим для громадян. У широких мас з'явиться можливість участі в обговоренні законопроектів. Кожен житель зможе висловити думку щодо обговорюваної проблеми і долучитися до законотворчості. Таким чином, свої інтереси зможуть відстоювати не тільки групи обранців народу, але й рядові громадяни.

Проте є ряд серйозних проблем, що вимагають певного усвідомлення і, відповідно, вирішення. Окремі фахівці продовжують додержуватися думки, що якщо Інтернет усього лише інструмент, який відповідає новим потребам суспільства, то він не змінить докорінно ні державу, ні саме суспільство. Можливо, взаємодія громадян і державних інститутів буде проходити в оптимальному режимі, аналогічно тому, як це відбувається при інформатизації управління бізнесу. Однак, якщо чиновник зловживає своїм становищем нині, то він знайде спосіб робити це й в оцифрованому світі. Саме чиновники менш за все зацікавлені в розкритті своєї діяльності (на сьогодні існує понад 30 відомчих таємниць). А відсутність прозорості в діяльності різних структур і колегіальність при прийнятті рішень дозволяє уникати персональної відповідальності.

Суспільство також не прагне встановлювати з державними інститутами прозорі відносини. З одного боку, системи е-уряду дають можливість наглядати за діяльністю чиновників і відомств. Але мало хто задумується, що без комп'ютера чиновник може погано справлятися з контролем над будь-якою діяльністю і приватним життям громадян, а з комп'ютером йому буде набагато зручніше робити це, – зауважує координатор "Московського лібертаріума" А. Левенчук. Технологія може змінити методи регулювання, але не змінює їх суті. Інформаційна відкритість не стане прямим результатом оцифровки відносин громадян і державних інститутів і навряд чи приведе до лібералізації суспільних відносин.

Сьогодні електронна революція не достатньою мірою здатна зробити державу більш відкритою. Навпаки, завдяки новим технологіям і мережам при старій ментальності окремі люди і суспільство в цілому можуть ставати надмірно прозорими для осіб, що здійснюють владні повноваження, а отже, більш контрольованими. Про небезпеку пророкував один з ідеологів інформаційного суспільства Деніел Белл – "...стає усе більш очевидною загроза політичного спостереження за індивідами із застосуванням витонченої інформаційної техніки, – писав він. – Все це елементарно підтверджує один з найстарших політичних труїзмів: коли будь-яка владна структура установлює бюрократичні норми і прагне насаджувати їх, створюється загроза зловживань. Інший не менш важливий момент полягає в тому, що контроль над інформацією найчастіше виливається у зловживання, починаючи з приховування інформації і закінчуючи її незаконним обнародуванням, і щоб запобігти цим зловживанням, необхідні інституціональні зміни, насамперед у сфері інформації.

Інтернет вперше в історії надає техніко-технологічну можливість для масового доступу до інформації. Але він не визначає необхідність робити це. "Одна з проблем прозорості державних структур – законодавча, тому що в деяких країнах, на жаль, і в Росії, немає ні традиції розкриття інформації, ні законодавчого регулювання цієї сфери", – говорить І. Атамирзян, керівник Східно-європейського відділу зі зв'язків з науково-дослідними організаціями Microsoft Research.

Існує й інша точка зору, відповідно до якої інформаційно-комп'ютерні технології кардинально змінять не тільки моделі взаємодії в суспільстві, але навіть свідомість людей. Про це з шістдесятих років минулого століття говорять теоретики постіндустріального суспільства. Як і всяка теорія, ця теж проходить перевірку зіткненням із реальністю і не завжди її витримує. Досить спірний момент – образ постіндустріальної людини: передбачалося, що особистість буде більш вільною в самореалізації, прагнення до придбання благ поступиться місцем творчості і нова людина з високим рівнем освіти стане активним учасником державних рішень. Навіть Захід, незважаючи на всі ознаки постіндустріальності (сектор виробництва послуг превалює над промисловим, комп'ютери трансформують працю, інформація стає головним капіталом), поки що показує стабільний приклад суспільства споживання та забруднення середовища.

Багато й інших складностей у розвитку е-середовища, наприклад, відсутність масового доступу, а точніше, нерівний доступ до освітньої інформації за допомогою Інтернету. Так, на думку представників Міністерства торгівлі США, американська нація вже має проблему з розшарування суспільства за "цифровою" ознакою. Що змусило дійти настільки парадоксального висновку? Ніщо інше, як невблаганні цифри статистики. Виявляється, навіть у такій високорозвиненій країні, як США лише 40,8 % білого населення мають комп'ютери, тобто вдвічі більше, ніж серед афроамериканців (19,3 %) або американців іспанського походження (19,4 %). При цьому імовірність того, що білий американець із будинку може одержати доступ до всесвітньої мережі, набагато вища, ніж у його співгромадян з іншим кольором шкіри. У той же час серед людей, які закінчили коледж, власники персональних комп'ютерів (63,2 % від кількості населення) зустрічаються в десять разів частіше, ніж серед осіб, які не мають вищої освіти. Чи варто додавати, що навіть ці скромні і досить бентежливі цифри не йдуть ні в яке порівняння з нашими мені ніж 2 % населення, які мають персональний комп'ютер з модемом і рознарований телефон? Фахівці вважають, що тільки коли хоча б 10 % громадян мають можливість працювати в мережі, настає переломний момент, з якого і починається інтенсивний саморозвиток інформаційного суспільства.

Існує і прямо протилежна проблема – загроза так званої абсолютної демократії, коли люди почнуть влаштовувати всенародні Інтернет-голосування з усякого мало-мальськи серйозного приводу, про який вони почули (а часом і недочули) у телевізійних новинах або на базарі. У цьому сенсі пряма демократія як крайній приклад дебюрократизації є не що інше, як влада натовпу, тобто охлократія, і чим більше натовп, тим нижче рівень культури та інформованості. Тому необхідність прямої постійної політичної участі й супутньої їй дебюрократизації, приписуваних цифровому суспільству, може викликати певні сумніви.

Щодо України, то у 2003 р., на виконання постанови Кабінету Міністрів України "Про заходи щодо створення електронної інформаційної системи "Електронний Уряд" від 24.02.2003 р. № 208 Держкомзв'язку та інформатизації України видав Наказ "Про затвердження Переліку і Порядку надання інформаційних та інших послуг з застосуванням електронної інформаційної системи "Електронний Уряд" від 15.08.3003 р. № 149 (із змінами від 27.07.2004 р.), в якому визначено 202 інформаційні послуги, які плануються надавати громадянам за допомогою системи "Електронний Уряд".

Створення системи е-урядування в Україні орієнтоване на:

- надання урядових послуг без обмежень шляхом створення національної та регіональних мереж громадських пунктів доступу до інформаційних ресурсів;
- максимально ефективне управління процесами у державі шляхом автоматизації відносин між державними установами на різних рівнях, звільнення державних службовців від рутинної роботи, економії бюджетних коштів, вироблення прозорої системи звітності;
- дебюрократизацію взаємовідносин з державними органами та зменшення рівня корумпованості шляхом поступового переведення критичної кількості відносин між громадянами, підприємствами та державними органами в електронний формат. Нові схеми взаємовідносин (уряд-бізнес) та (уряд-громадяни) з застосуванням інформаційно-комп'ютерних технологій є максимально прозорими та економними;
- підвищення якості надання державних послуг шляхом створення "електронних альтернатив" проведення операцій з громадянами та підприємствами: реєстрація, ліцензування, сертифікація, оподаткування, проведення виборів, оплата платежів;
- підвищення ефективності документообігу та комерційних операцій шляхом застосування системи електронного документообігу та електронного цифрового підпису на основі чинного законодавства;

- підвищення рівня інвестування у державні проекти шляхом залучення інвестицій приватного сектору на основі проведення відкритих тендерів;
- підвищення рівня взаємодії з громадським сектором, шляхом залучення з боку держави громадських організацій до надання електронних послуг громадянам та організаціям;
- прискорення адміністративної реформи шляхом всебічного застосування можливостей електронного уряду в діяльності органів державної влади;
- підвищення конкурентоспроможності на міжнародному рівні шляхом інтерактивної взаємодії України з електронними урядами іноземних держав.

У 2004 р. громадською робочою групою Фонду "Інформаційне суспільство України" був запропонований проект "Електронна Україна" (див. //www.e-ukraine.com.ua), який звертав увагу на максимальне застосування переваг зазначеної системи як важливого фактору здійснення народовладдя в державі. Підвищення рівня взаємної довіри громадян, держави та бізнесу, якості та прозорості державних послуг рекомендувалось формувати на принципах:

- максимальна простота і прозорість (е-уряд має обслуговувати звичайних громадян, а не лише фахівців);
- єдині технічні стандарти і взаємна сумісність (електронні додатки мають відповідати принципам загальної архітектури ідентифікації, безпеки, дизайну);
- забезпечення дотримання правил інформаційної безпеки;
- беззастережна орієнтація на думку громадян при реалізації нововведень.

Резюмуючи зазначене, вважаємо однією з головних проблем електронного урядування проблему повного інформування населення про діяльність органів влади. У цьому сенсі крім списків закритої інформації, що наприклад, становить державну таємницю, необхідно створити і списки інформації що в обов'язковому порядку підлягає відкритій публікації, - не тільки вищого, конституційного рівня (законів, наприклад), але й різних підзаконних актів, відомчих інструкцій, статистичної інформації і т. д. Це буде сприяти зниженню підґрунтя для корупції й уможливить дійсну довіру та взаємодію громадян з державою.

3.2.6. Інформаційна безпека

До законів щодо сфери інформаційної безпеки, як складової національної безпеки України, відносяться:

Конституція України від 1996 р. (ст. ст. 17, 32, 92);

Закон України "Про Службу безпеки України" від 1992 р.;

Закон України "Про правовий режим надзвичайного стану" 1992 р.;

Закон України "Про державну таємницю" від 1994 р.;

Закон України "Про правовий режим воєнного стану" від 2000 р.;

Закон України "Про основи національної безпеки України" 2003 р. тощо, а також укази Президента України:

"Про Стратегію національної безпеки України" від 2007 р.;

"Про рішення Ради національної безпеки і оборони України від 17.06.1997 року "Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин" від 1997 р.;

"Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України" від 2001 р. та інші акти, зазначені в [95].

За визначенням, яке надається у Законі України "Про основи національної безпеки України" від 19.06.2003 р., національна безпека – це така 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 України. Закон визначає пріоритети національних інтересів, об'єкти національної безпеки та суб'єкти, які зобов'язані її забезпечувати, основні напрями державної політики, повноваження та основні функції державних органів у сфері безпеки.

Згідно з п. 13 Закону України "Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 09.01.2007 р. наявність інформаційної безпеки визначається станом захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання 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.

Питання інформаційної безпеки – це, насамперед, питання регламентації доступу до інформації. У цьому плані Кабінет Міністрів України видав розпорядження від 23.07.2008 р. № 990-р щодо створення проекту Конвенції про доступ до інформації. Зазначимо, до слова, що у Росії ця робота була розпочата у 1999 р., коли в Держдуму Президентом РФ було внесено проекти федеральних законів – "О праве на информацию" та "Об обязанности органов государственной власти, государственных организаций и органов местного самоуправления предоставлять информацию гражданам о своей деятельности".

Інтерес людини відчувати свою автономію в суспільстві, яка захищається правом на недоторканність приватного життя, знаходиться у діалектичному протиріччі з певними інтересами інших осіб і суспільства, зокрема у безпеці і добробуті, захисті прав і свобод інших осіб. Заради цих інтересів здійснюється боротьба із злочинністю, під час якої відбувається втручання у приватне життя. Однак це діалектичне протиріччя не може бути вирішено відкиданням одних інтересів на користь іншим. Для його розв'язання вимагається оцінка задіяних інтересів і їх узгодження.

Цей безперечний постулат відображається в конструкції деяких статей Європейської Конвенції про захист прав людини і основоположних свобод. Як і ст. ст. 9, 10 та ст. 11 Конвенції, ст. 8 складається з двох частин. Перша – вказує права, які підлягають захисту, а друга – зазначає можливі обмеження чи виключення з проголошених прав.

Ст. 8 Європейської конвенції про захист прав людини і основоположних свобод вказує на такі інтереси, що конкурують з правом особи на приватність:

- інтереси національної та громадської безпеки;
- економічного добробуту країни;
- запобігання заворушенням і злочинам;
- захисту здоров'я або моралі;
- захисту прав і свобод інших людей.

Ст. 32 Конституції України вказує на інтереси національної безпеки, економічного добробуту та прав людини як можливу підставу для обмеження права на приватність інформації персонального змісту. Це є виправданим, оскільки право на повагу до приватного життя як ширше за правовим змістом може зазнавати більших обмежень, ніж право на приватність інформації персонального змісту, яке є його складовою частиною.

Це підтверджується, зокрема, положеннями спеціальних міжнародно-правових документів, присвячених захисту персональних даних. Ст. 9 Конвенції РС № 108 "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних" передбачає, що відступ від положень, що гарантують права суб'єкта даних, дозволяється в інтересах державної безпеки та громадського спокою, грошових інтересів держави або для боротьби із злочинами та для захисту прав і свобод інших осіб. А ст. 13 Директиви 95/46/СС "Про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних і вільним обігом цих даних" 1995 р. проголошує, що обмеження можуть застосовуватися, якщо це є необхідним заходом для: державної безпеки, оборони, громадського порядку, в інтересах слідства, важливого економічного або фінансового інтересу, захисту суб'єкта даних або прав і свобод інших осіб. Цьому переліку обмежень майже тотожні за змістом положення ст. 32 Конституції України.

Як зазначається у Законі України "Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 2007 р., вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

- 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 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 розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Резюмуючи зазначене, підкреслимо, що інформаційна безпека є складовою частиною національної безпеки, а її питання – це, насамперед, регламентація доступу до інформації. Для розв'язання існуючого діалектичного протиріччя та забезпечення балансу інтересів людини, суспільства і держави потрібна оцінка задіяних інтересів і їх узгодження згідно положень ст. 8 Європейської конвенції про захист прав людини і основоположних свобод, ст. 9 Конвенції Ради Європи № 108 "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних" та ст. 13 Директиви 95/46/СС Європейського Парламенту і Ради "Про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних і вільним обігом цих даних" 1995 р.

Питання для самоконтролю

1. Загальна характеристика інститутів інформаційного права.
2. Інститут засобів масової інформації.
3. Інститут науки та освіти.
4. Інститут інформатизації та Національної програми інформатизації.
5. Інститут інтелектуальної власності.
6. Інститут захисту персональних даних.
7. Інститут електронної комерції.
8. Інститут електронного банкінгу.
9. Інститут електронного урядування.
10. Інститут інформаційної безпеки.

Розділ 4. НАПРЯМИ УПОРЯДКУВАННЯ ІНФОРМАЦІЙНИХ ВІДНОСИН

4.1. Діяльність у інформаційній сфері

Згідно зі статтею 12 Закону України "Про інформацію", інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави [4]. У будь-якій державі зазначена діяльність спрямовується відповідною державною політикою. Під державною інформаційною політикою мається на увазі регулююча діяльність державних органів, спрямована на розвиток інформаційної сфери суспільства, що охоплює всю сукупність відносин, пов'язаних зі створенням, отриманням, збереженням, обробкою, використанням і поширенням інформації у всіх її видах та секторах застосування: наукової, науково-технічної, науково-освітньої, виробничої, ділової, розважальної і т. п.

До головних напрямів в упорядкуванні інформаційних відносин відноситься інформаційна діяльність державних органів, яка має управлінський, регулюючий зміст, що визначається адміністративним правом. Ця діяльність спрямована на забезпечення прав та інтересів суб'єктів інформаційної діяльності в Україні та взаємовигідного співробітництва України з іншими державами. Основними напрямами упорядкування відносин щодо інформаційної діяльності держави є:

- забезпечення інформаційних прав людини і основоположних свобод;
- забезпечення балансу інформаційних прав людини, суспільства і держави;
- створення, збереження, використання і поширення інформаційних ресурсів економічного, екологічного, фінансового, інформаційного й іншого призначення;
- охорона та захист інформаційних ресурсів і інформаційних послуг;
- підтримка інформаційної безпеки держави;
- експертиза проектів інформаційних систем і мереж;
- освітня робота, підготовка і підвищення кваліфікації кадрів.

Державна політика інформатизації є складовою державної інформаційної політики. Згідно з Законом України "Про Національну програму інформатизації", інформатизація – це сукупність взаємозалежних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб, реалізації прав громадян і суспільства на основі створення, розвитку, використання інформаційних систем, мереж, ресурсів і інформаційних технологій, створених на базі застосування сучасної обчислювальної і комунікаційної техніки [30].

Згідно з Законом України "Про Концепцію Національної програми інформатизації", державна політика інформатизації розглядається як складова частина соціально-економічної політики держави в цілому і спрямована на раціональне використання промислового і науково-технічного потенціалу, матеріально-технічних і фінансових ресурсів для створення сучасної інформаційної інфраструктури в інтересах вирішення комплексу поточних і перспективних задач розвитку України як незалежної демократичної держави з ринковою економікою [29].

Державна політика інформатизації передбачає нормативно-правове упорядкування інформаційних відносин щодо діяльності осіб, суспільства і держави у будь-якій галузі господарства стосовно формування та використання ринку інформаційних ресурсів, інформаційних продуктів та інформаційних послуг за допомогою інформаційно-

комп'ютерних технологій та мереж. Упорядкування відносин здійснюється шляхом реалізації таких функцій:

- юридичного закріплення відносин, встановлення норм і правил діяльності у сфері інформатизації;
- розробки концептуальних основ і механізмів реалізації державної політики інформатизації;
- перманентного формування і виконання програм і проектів Національної програми інформатизації;
- державної координації діяльності центральних, місцевих органів виконавчої влади й органів місцевого самоврядування, організацій і підприємств у сфері інформатизації;
- державної експертизи проектів інформаційних систем органів державної влади і місцевого самоврядування і контролю сумісності їх використання в інформаційному просторі України;
- стандартизації систем і засобів інформатизації;
- сертифікації засобів технічного захисту у сфері інформатизації;
- ліцензування окремих видів підприємницької діяльності у сфері інформатизації;
- розробки і реалізації взаємовигідного міжнародного співробітництва у сфері інформатизації;
- підтримки інформаційної безпеки і суверенітету України.

До загальних організаційних принципів відносяться централізація і децентралізація, саморозвиток, самофінансування і самоокупність, державна підтримка через систему пільг, кредитів, прямого бюджетного фінансування.

У зв'язку із становленням інформаційного суспільства, яке визначається розвитком інформаційно-комп'ютерних технологій та мереж, все більшої уваги потребують питання щодо наступних трьох аспектів.

По-перше, інформатизація передбачає сукупність дій та процесів для задоволення інформаційних потреб та забезпечення прав людини, а також інтересів суспільства і держави. Це стосується не тільки інформатизації але й усієї інформаційної сфери держави.

По-друге, задоволення інформаційних потреб та забезпечення прав і інтересів у сфері інформатизації здійснюється за допомогою засобів і систем автоматизованої обробки та передачі даних та у межах чинного законодавства, що упорядковує відповідні відносини. Інформаційні відносини виявляються через діяльність та взаємодію прав і обов'язків різних суб'єктів, що вимагає їх правового упорядкування у нормативно-правових актах, зокрема щодо сфери інформатизації. Згідно до статті 14 Закону України "Про інформацію", основними видами діяльності є одержання, використання, поширення та зберігання інформації. Проте зазначене не враховує таки види інформаційної діяльності, як створення, збирання, охорона, захист, знищення інформації та не має узагальнюючого терміну щодо будь-яких дій (згідно з європейськими стандартами – це обробка даних).

По-третє, особливість засобів інформатизації полягає у тому, що їх застосування розмиває бар'єри між різними секторами інформаційного середовища та вносить неузгодженість в упорядкування відносин в інформаційній сфері. Виникає потреба у системності в упорядкуванні інформаційних відносин, і юридичною базою цього є єдині принципи та їх чітке визначення у словесній форми, що розуміється як "норма права", яка відповідає принципам права. У свою чергу "норма права" є основою створення "правових норм" ("правових формул") щодо інформаційного законодавства. Іншими словами, поняття "норма права" слід застосовувати лише для дефініції (тлумачення) принципів, доктрин та цінностей, які визначають досягнення у моральному та культур-

ному розвитку світової цивілізації, і для інформаційної сфери всі вони узагальнюються таким поняттям, як "інформаційне право". Все те, що стосується суб'єктивних уявлень у підходах та створенні формулювань (так званих правових формул будь-якого законодавства) для упорядкування та регулювання відносин відноситься до поняття "правова норма", яка є тільки приблизним відображенням "норми права" щодо принципів, доктрин та цінностей людського буття, вироблених пошуками справедливості та мудрістю великих людей минулого. Підвищення узгодженості між "нормою права", яка визначає досягнення цивілізації і культури (див. [235, 236]), та "правовою нормою", що звичайно має зміст компромісу між політикою влади та прагненнями громадянського суспільства до реальної справедливості, можна вважати одним з головних завдань нової галузі права – інформаційного права.

Резюмуючи зазначене, навряд чи можна з повною впевненістю стверджувати, що з розробкою і прийняттям вказаних законів держава цілком визначилася у своїй політиці щодо упорядкування відносин у інформаційній сфері та, зокрема, у сфері інформатизації. Цього не може бути через динамічність і активність у застосовуванні інформаційно-комп'ютерних технологій та мереж. Є потреба у переосмислені концептуальних підходів і необхідності вироблення більш ефективних принципів державного регулювання не тільки у сфері інформатизації, але й у всій сфері інформаційних відносин. Це можливе завдяки єдності інформаційного законодавства. У зв'язку з цим Національна програма інформатизації має бути не тільки переліком проектів і програм щодо інфраструктури інформатизації. Все більшої уваги потребує задачі "стикування" (конгломерації) різних інформаційних систем і засобів та єдиної нормативно-правової бази для створення зрозумілого, зручного й ефективного для всіх інформаційного середовища. Це можливе на базі "відкритих систем". Концепція "відкритих систем" зводиться до стандартизації, але не в директивній, а в індикативній (рекомендаційній) формі: хочеш – дотримуйся загальноприйнятих стандартів, не хочеш – роби по-своєму, але тоді – "випадеш" з єдиного інформаційного середовища держави.

Крім зазначеного є необхідність у більш ретельному та детальному упорядкуванні інформаційних відносин та гармонізації їх з положеннями європейських стандартів у таких областях, як: інформаційні послуги, підтримка інформаційної безпеки, відповідальність суб'єктів, міжнародна діяльність та інтеграція України у світовий інформаційний простір.

4.1.1. Інформаційні послуги

Згідно зі статтею 41 Закону України "Про інформацію", інформаційна послуга – це здійснення у визначеній законом формі інформаційної діяльності по доведенню інформаційної продукції до споживачів з метою задоволення їх інформаційних потреб.

Інше визначення дано у ст. 1 Закону України "Про Національну програму інформатизації": інформаційна послуга – дії суб'єктів щодо забезпечення споживачів інформаційними продуктами.

Власник інформаційного ресурсу має право визначати зміст послуг, що надаються за допомогою його ресурсів, а також установлювати розмір плати за такі послуги і порядок її внесення.

Послуги у сфері інформатизації можуть бути платними, безоплатними і комбінованими.

Кабінет Міністрів України визначає види національних інформаційних ресурсів, що можуть надаватися за плату, і порядок використання отриманих коштів.

Надання довідок про інформаційні продукти та технології, що входять до складу національних інформаційних ресурсів, а також виготовлення довідок і копій за письмовими запитами судів, державних, правоохоронних, контрольно-ревізійних органів, органів місцевого самоврядування здійснюються безоплатно.

Надання інформаційних ресурсів державним і недержавним установам, що надалі будуть використовувати їх для надання платних послуг, здійснюється на договірних засадах.

Договірні основи надання інформаційних послуг. Інформаційні послуги можуть надаватися юридичними або фізичними особами, що мають право надавати такі послуги відповідно до законодавства, у разовому або іншому порядку.

Систематичні послуги надаються фізичними особами-суб'єктами підприємницької діяльності і юридичними особами на підставі угоди, що може укладатися в усній або письмовій формі. Анулювання угоди або зміна її умов здійснюється в результаті згоди сторін, кожна з яких повинна попереджувати іншу про такі зміни.

Особа, винна в невиконанні або неналежному виконанні договору, несе відповідальність на підставах чинного законодавства про договори.

Право споживачів інформаційних ресурсів на відшкодування збитків. Споживач має право використовувати інформаційний ресурс у межах тих прав, що установлені відповідним договором і законодавством.

Споживач має право на відшкодування збитків, що були заподіяні внаслідок недостовірної, неповної або помилкової інформації, якщо заздалегідь про це не було застереження від постачальника. Збитки відшкодовуються тим суб'єктом, що безпосередньо надав недостовірну, неповну, помилкову інформацію.

Обов'язки суб'єктів щодо якості інформаційних ресурсів. Власник (володілець) інформаційного ресурсу зобов'язаний:

- захищати інформаційні ресурси (особлива увага має приділятися захисту персональних даних);
- здійснювати розпорядження інформаційними ресурсами, що містять конфіденційну інформацію або державну таємницю, за погодженням з відповідними державними органами, зацікавленими особами або їхзаконними представниками;
- сповіщати споживачів ресурсів про наявність в інформаційному продукті (ресурсі) недостовірної, неповної, помилкової інформації;
- забезпечувати такий режим супроводу інформаційного ресурсу, що гарантує збереження, цілісність, повноту і захист даних.

Споживач зобов'язаний використовувати наданий інформаційний ресурс у відповідності до положень угоди з власником або володільцем цього інформаційного ресурсу, а також згідно з вимогами законодавства.

4.1.2. Підтримка інформаційної безпеки

Підтримка інформаційної безпеки – одна з найважливіших функцій держави. Система забезпечення інформаційної безпеки є складовою частиною забезпечення національної безпеки держави.

Інформаційна безпека – це стан захищеності людини, суспільства і держави, за якого здійснюється охорона і захист інформаційних ресурсів, мінімізація шкоди від негативних інформаційних впливів, небажаних наслідків використання інформаційних продуктів і інформаційних технологій.

Об'єктами інформаційної безпеки є інформаційні права людини й основоположні свободи, національні інформаційні ресурси, інформаційна інфраструктура в політичній,

економічній, соціальній, військовій, екологічній, науково-технологічній й інших сферах діяльності суспільства.

Держава створює необхідні умови і здійснює правові, організаційні, соціально-економічні, науково-технічні й інші заходи, спрямовані на підтримку інформаційної безпеки.

Інформаційна безпека системи національних інформаційних ресурсів. Підтримується системою заходів правового, організаційного і техніко-технологічного змісту щодо нейтралізації зовнішніх і внутрішніх загроз, що передбачає:

- розвиток нормативно-правової бази;
- застосування інформаційних технологій, безпечних для інформаційних ресурсів;
- підтримка цілісності інформаційних продуктів і інформаційних технологій;
- охорону та захист інформаційних продуктів і інформаційних технологій від несанкціонованих доступу, модифікації, блокування або знищення;
- здійснення постійної актуалізації резервних копій інформаційних продуктів і інформаційних технологій;
- здійснення моніторингу стану інформаційної безпеки.

Безпечні інформаційні технології. В усіх складових частинах системи національних інформаційних ресурсів повинні застосовуватися безпечні інформаційні технології, за допомогою яких обробляють дані. Ці технології обов'язково повинні мати відповідний атестат.

В усіх без винятку складових частинах системи національних інформаційних ресурсів повинна функціонувати система заходів, що підтримує цілісність і збереження інформаційних продуктів.

Здійснення відповідних заходів щодо цілісності інформаційних продуктів покладають на адміністратора організації, що визначає систему доступу до ресурсів на основі нормативно-правових актів організації.

Захист інформаційних продуктів. Електронні депозитарії й автоматизовані системи обробки даних, що містять відомості, які становлять передбачену законом таємницю і розголошення якої може завдати шкоди людині, суспільству або державі, обов'язково повинні мати систему технічного захисту від несанкціонованих доступу, модифікації, блокування або знищення інформаційних продуктів.

Відповідність електронних депозитаріїв і автоматизованих систем вимогам захисту даних і підтримання цілісності ресурсів має бути підтверджена сертифікатом центрального державного органу у сфері технічного захисту інформації.

Контроль за дотриманням вимог з інформаційної безпеки здійснюють адміністратори системи національних інформаційних ресурсів, а також — центральних органів державної влади, органів місцевого самоврядування у межах, визначених законом.

4.1.3. Відповідальність суб'єктів

Порушення законодавства України у сфері інформатизації передбачає дисциплінарну, адміністративну, цивільно-правову або кримінальну відповідальність згідно з законодавством України.

Відповідальність настає за будь-які діяння щодо інформаційних, у тому числі комп'ютерних мереж і систем, технічних і програмних засобів, а також щодо інформації, даних та інформаційних продуктів, технологій і ресурсів, якщо такі дії завдають матеріальної або моральної шкоди іншим особам, а також унаслідок порушення положень законодавства.

Провайдери, а також постачальники доступу і послуг мережі Інтернет не несуть відповідальності за контент (зміст відомостей), доступ до якого вони забезпечують, але вони несуть відповідальність за якість наданих інформаційних послуг, тобто за трафік, інтенсивність потоку й обсяг переданих відомостей.

4.1.4. Інтеграція України у світовий інформаційний простір

Міжнародна діяльність України у світовому інформаційному просторі базується на законодавстві і визнаних Україною міжнародних актах. Ця взаємодія здійснюється з урахуванням національних інтересів і економічної доцільності, підтримки належного рівня інформаційної безпеки і захисту екології.

Україна підтримує міжнародні ініціативи, спрямовані на розвиток і ефективне використання світової інформаційної інфраструктури, проведення узгодженої науково-технічної політики, раціональне використання природних ресурсів і збереження навколишнього середовища.

У сучасному суспільстві інформаційні ресурси, які є основою майже всіх управлінських, економічних та соціальних процесів, набувають домінуючого значення. Постає завдання практичного створення та впровадження реальних механізмів міждержавної координації і кооперації, комплексу заходів раціонального впровадження сучасних інформаційних технологій, систем та побудови на їх основі міждержавної взаємодії у світовому інформаційному просторі.

Для забезпечення рівноправного та скоординованого включення України до світового інформаційного простору необхідно визначити головні принципи міжнародної взаємодії у цій сфері, до яких можна віднести:

- використання світового досвіду з інтеграції правового, організаційного і техніко-технологічного змісту;
- створення нормативно-правової бази інформатизації різних суб'єктів на основі системи дво- і багатосторонніх міжнародних договорів і угод;
- правове і технологічне забезпечення доступу різних суб'єктів до закордонних інформаційних ресурсів;
- впровадження міжнародних стандартів для забезпечення пошуку, збору, зберігання і використання інформації;
- активне використання закордонних інформаційних продуктів для формування власних інформаційних ресурсів України;
- придбання ліцензій, створення спільних підприємств у сфері інформатизації;
- експорт інформаційних ресурсів України і збільшення національної присутності у світовому інформаційному просторі;
- участь України як повноправного члена міжнародних програм і проектів у зв'язку з формуванням світового інформаційного простору, створенням інформаційних технологій;
- моніторинг форм і методів впливу міжнародних засобів комунікацій на процеси формування суспільної свідомості в Україні.

Інформаційний простір України повинен формуватись як органічна складова світового та європейського інформаційних просторів з урахуванням національних інтересів України та підтримки її інформаційної безпеки.

Щодо взаємодії в інформаційному просторі з державами-членами Співдружності Незалежних Держав, то ця співпраця має відбуватися на взаємовигідній основі в погоджених сферах діяльності. Основними напрямами співробітництва можуть бути:

- створення механізму постійного інформаційного обміну;

• інформаційне забезпечення органів міждержавного співробітництва;

• сприяння поглибленню і зміцненню інтеграційних процесів у погоджених сферах діяльності, розвиток взаємодії в соціально-гуманітарній і екологічній сферах;

• сприяння забезпеченню єдиних підходів до регулювання ціноутворення, оподаткування і стягнення мита на інформаційні і телекомунікаційні послуги;

• стандартизація й уніфікація міждержавного електронного документообігу на основі відповідних міжнародних стандартів;

• правове, організаційне і технологічне забезпечення використання багатомовного середовища Співдружності.

Доцільною є розробка нормативних документів щодо діяльності у сферах:

• спільне виробництво засобів обчислювальної техніки, телекомунікацій та інших засобів інформатизації;

• розроблення і впровадження засобів захисту інформації і даних, систем кодування і спеціальних технічних засобів;

• планування і реалізація довгострокових науково-технічних програм досліджень в області нових інформаційних технологій.

4.2. Інформаційні ресурси

Поняття ресурсу (від фр. "ressource" – допоміжний засіб) трактується в словниках, зокрема С.І. Ожегова, як "запасы, источники чего-нибудь, средства, к которому обращаются в необходимом случае" [140, с. 676]. Звідси виникла дефініція "інформаційний ресурс".

Згідно зі статтею 1 Закону України "Про Національну програму інформатизації" від 1998 р., інформаційні ресурси – це сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних та ін.).

Інформаційні ресурси – це організована сукупність документованої інформації, інформаційних продуктів і інформаційних технологій, призначених для забезпечення визначених економічних, екологічних, фінансових, інформаційних та інших потреб людини, суспільства і держави. Можна сказати і так, що інформаційні ресурси – це сукупність інформаційних продуктів одного або декількох тематичних напрямів, що згруповані за змістом. Інформаційні ресурси можна визначити й у такий спосіб – це організовані в базах і банках даних інформаційні продукти, необхідні для задоволення інформаційних потреб людини, суспільства і держави.

Інформаційний продукт – це документована інформація, що підготовлена і призначається для задоволення потреб користувача. Або інакше: інформаційний продукт – це об'єктивно закріплена на носії інформація, підготовлена для споживання, автоматизованої обробки і поширення за допомогою мереж передачі даних. Ще визначення: інформаційний продукт – це результат інформаційної діяльності, процес матеріальної реалізації якої надає продукцію.

У тій же статті Закону є визначення, що інформаційні технології – це цілеспрямовано організована сукупність інформаційних процесів із застосуванням засобів обчислювальної техніки, що забезпечує високу швидкість обробки даних, швидкий пошук інформації, розміщення даних, доступ до джерел інформації незалежно від місця їх розміщення. Можна сказати простіше: інформаційні технології – це цілеспрямовано організована сукупність інформаційних процесів із застосуванням засобів автоматизованого пошуку, одержання, обробки і передачі даних, до яких пристосована інформація або інформаційний продукт. Чи інакше: інформаційна технологія – це комплекс методів, способів і засобів пошуку, збору (придбання), реєстрації, нагромадження, збереження, поширення (реалізації), захисту і відображення інформації за допомогою автоматизованих систем і мереж передачі даних.

Будь-який інформаційний ресурс має дві складові: інформаційне сховище (для електронних інформаційних ресурсів – це бази даних і знань) і сам процес задоволення інформаційних потреб. З погляду семіотики (науки про знакові системи) процес задоволення інформаційних потреб у принципі здійснюється шляхом перетворення (обробки) даних (букв, знаків, цифр, сигналів, структур і ін.) інформаційного ресурсу в інформацію шляхом пошуку, обробки, структуризації даних, осмислення (аналітико-синтетичної переробки відомостей за запитом) і використання одержаної інформації для формування нового знання.

Складова процесу перетворення інформаційного ресурсу має три аспекти [174, с. 11]: синтаксичний, семантичний і пізнавальний.

Синтаксичний аспект відноситься до з'єднання слів і створення речення. Він є узагальненням даних фізичного каналу комунікації і комп'ютера, завдяки яким здійснюється пошук, первинна обробка і зберігання даних, але не інформації. Ці дані можуть трактуватися як інформація лише з погляду кількісної, статистичної ознаки їх обсягу (трафіку).

Семантичний аспект відноситься до розуміння мовних одиниць. Він забезпечується перетворенням даних у відомості, попереднім відбором за змістом інформаційного завдання і розуміння (осмислення) мовних одиниць людиною. Семантичний шум, що є втратами (спотвореннями) відомостей унаслідок помилок в осмисленні, згодом може сприяти їх невідповідності задачі інформаційного запиту, недостовірним результатам або неправильним висновкам.

Пізнавальний аспект відноситься до розуміння людиною суті інформаційного продукту і його відповідності запиту на отримання потрібної інформації. Результати відбору, аналітико-синтетичної обробки, структуризація і розуміння значення одержаних відомостей є приростом запасу інформації, який, проте, не завжди є "знанням".

Спроби отримання нових знань завдяки застосуванню комп'ютера до сьогодні істотних результатів не мають. Проблема не в задачі пошуку і отримання відомостей, розміщених в масивах даних, а в тому, що комп'ютер може тільки за заданими ключовими словами і завдяки пошуковому алгоритму прорахувати і знайти в масиві даних кодову послідовність знаків щодо певного слова. Іншими словами, будь-яка машина (зокрема, комп'ютер) за результатом процесу (дії) надають "дані", які завдяки мисленню людини стають "відомостями", що несуть у собі "інформацію", яка за наявності в ній новизни набуває статусу "знання". У разі розміщення "знання" в масиві даних відмічений ланцюжок логічної послідовності має наступний вигляд:

"знання" → "інформація" → "відомості" → "дані"

Головна причина не вирішення поки задачі отримання нових знань за допомогою комп'ютера полягає у тому, що категорії звичайної мови "слово" і "текст" за своєю природою значним чином відрізняються від категорій мислення "поняття" і "значення". У комп'ютері ці категорії ототожнюються з "кодовою послідовність знаків", яка має нереальний, штучний зміст, що лише умовно відповідає відображенню у мисленні людини.

Таким чином, все те, що стосується суспільних відносин у сфері застосування комп'ютерів, інформаційно-комп'ютерних технологій та мереж в нормативно-правових актах, слід прив'язувати до поняття "дані", а не до поняття "інформація". Свідченням цьому є застосування вищезазначених понять в сучасній нормативно-правовій базі європейських стандартів, див. зокрема [81].

4.2.1. Національні інформаційні ресурси

Національні інформаційні ресурси призначені для забезпечення національних інтересів України, реалізації інформаційних прав людини й основоположних свобод, інтересів суспільства, органів державної влади й органів місцевого самоврядування, юридичних осіб усіх форм власності.

Національні інформаційні ресурси є основою для забезпечення суверенітету й інформаційної безпеки держави, служать вирішенню задач суб'єктів української економіки, виробництва, науки, культури й інших сфер діяльності.

Складовими частинами національних інформаційних ресурсів є інформаційні ресурси різної приналежності і форми власності.

Національні інформаційні ресурси формують з інформаційних продуктів і інформаційних технологій різних форм власності.

Включення інформаційних продуктів до складу національних інформаційних ресурсів здійснюють на підставі експертизи відповідності їх властивостей вимогам задоволення потреб забезпечення національних інтересів України. Принципи і критерії визначення властивостей продуктів і технологій, порядок їх використання, а також порядок проведення експертизи затверджуються Кабінетом Міністрів України.

До складу національних інформаційних ресурсів включають:

- в обов'язковому порядку — інформаційні продукти, створені органами державної влади й органами місцевого самоврядування в порядку здійснення їх основної діяльності;
- на умовах державного замовлення — інформаційні продукти, створені після завершення виконання такого замовлення або відповідного його етапу;
- інформаційні продукти, що є похідними результатами інших робіт, що виконуються із залученням коштів державного бюджету, після завершення виконання таких робіт або їх окремих етапів;
- на основі угоди з власником (виробником) — інформаційні продукти, створені за рахунок позабюджетних коштів їх власників або виробників. Включення цих продуктів до складу національних інформаційних ресурсів не призводить до зміни їх власника, якщо інше не передбачене законом або умовами угоди;
- на основі відповідних міждержавних або міжнародних угод – міждержавні і міжнародні інформаційні продукти.

Інформаційні продукти, що надані в електронному вигляді, розміщують в електронному депозитарії (депозитаріях). Включення інформаційних продуктів до складу національних інформаційних ресурсів фіксується шляхом внесення їх реквізитів у національний електронний реєстр інформаційних ресурсів України. З цього моменту їх вважають складовими частинами національних інформаційних ресурсів.

Інформаційні продукти вилучають зі складу національних інформаційних ресурсів у тому випадку, коли вони перестають відповідати існуючим вимогам щодо якісних ознак, засобів доступу або коли в них зникає потреба. Складання переліку інформаційних продуктів, що підлягають вилученню зі складу національних інформаційних ресурсів, здійснюється на підставі експертизи відповідності цих інформаційних продуктів зазначеним вимогам. Принципи і критерії визначення відповідності, а також порядок проведення експертизи затверджуються Кабінетом Міністрів України.

Вилучення інформаційних продуктів зі складу національних інформаційних ресурсів фіксується шляхом обов'язкового вилучення їх реквізитів з електронних реєстрів. З цього моменту вони перестають бути складовими частинами національних інформаційних ресурсів.

Базу національних інформаційних ресурсів формують:

- інформаційні ресурси Верховної Ради України, Секретаріату Президента України, Кабінету Міністрів України, Конституційного Суду України, Верховного Суду України, Національного банку України;
- інформаційні ресурси органів державної влади й органів місцевого самоврядування, державних організацій і підприємств;
- інформаційні ресурси національної системи науково-технічної інформації;
- Національний архівний фонд;
- Музейний фонд України;
- Національний електронний реєстр інформаційних ресурсів України;
- інші організації, які створюють інформаційні продукти, що мають національний статус, визначений чинним законодавством.

4.2.2. Електронні інформаційні ресурси

Електронні інформаційні ресурси — це інформаційні ресурси, що розміщені в електронних базах даних, у комп'ютерних системах, системах автоматизованої обробки і передачі даних.

Веб-ресурси — це інформаційні ресурси у вигляді одного або декількох веб-сайтів.

Веб-ресурси можуть бути об'єктами всіх форм власності, договірних відносин відповідно до цивільного законодавства і законодавства про інтелектуальну власність.

Веб-ресурси можуть використовуватися їх власниками або іншими уповноваженими особами (власниками) в будь-яких цілях, що не заборонені законом.

Веб-сайт загального інформаційного змісту не повинен містити персональні дані або інформацію, що становить державну таємницю, і іншу інформацію, що обмежена в поширенні відповідно до закону.

Інформаційні продукти з обмеженим доступом можуть утримуватися на веб-сайті чи іншому інформаційному ресурсі лише за згодою відповідних державних органів або зацікавлених осіб чи їх законних представників.

4.2.3. Право власності на інформаційні ресурси

Право власності на інформаційні ресурси — це упорядковані законом інформаційно-правові відносини щодо володіння, користування та розпорядження інформаційними ресурсами щодо інформаційних продуктів і інформаційних технологій.

Інформаційні ресурси (документи, книги, бази даних, ілюстрації, фотографії, голограми, кіно-, відеофільми тощо) є предметом матеріального світу, можуть виступати як товар і бути об'єктами товарних відносин, які регулюються цивільним законодавством України (з питань власності та інтелектуальної власності) і законодавством України щодо захисту персональних даних, за винятком випадків, передбачених відповідними міжнародними договорами України.

Інформаційні ресурси можуть бути власністю громадян України, іноземних громадян і осіб без громадянства, органів державної влади й органів місцевого самоврядування, організацій і об'єднань громадян.

Фізичні і юридичні особи, що надають в обов'язковому порядку документовану інформацію в органи державної влади, не втрачають своїх прав на цю інформацію.

Фізичні і юридичні особи усіх форм власності, а також органи державної влади й органи місцевого самоврядування як суб'єкти діяльності у сфері інформатизації набу-

вають права власності на інформаційні ресурси у межах, що встановлені законодавством, за рахунок їх коштів, придбання на законних підставах, отримання внаслідок дарування або спадкування. Власники інформаційних ресурсів мають усі передбачені чинним законодавством повноваження, у тому числі вони мають право:

• призначати особу, що здійснює керування відповідними інформаційними ресурсами відповідно до наданих йому повноважень;

• встановлювати у межах своїх повноважень режим і правила обробки й захисту інформаційних ресурсів;

• визначати умови розпорядження документованою інформацією при її копіюванні і поширенні.

Право власності (у тому числі часткової власності) на інформаційні ресурси, що придбані суб'єктом в іншого власника або створені ним з використанням інформаційних ресурсів інших власників, набувається лише на підставі ліцензійних договорів з цими власниками.

Особа, що створила відповідний інформаційний ресурс, визнається його автором і одержує немайнові невідчужувані права (право авторства) відповідно до законодавства про інтелектуальну власність.

Особа, що створила відповідний інформаційний ресурс, а також реалізувала його в матеріальній продукції і за свій рахунок, визнається його власником і дістає майнові права згідно із законодавством про власність.

Особа, що створила інформаційний ресурс у результаті здійснення своїх трудових функцій або на підставі договору про виконання робіт, а також особа, авторство якої неможливо довести, не вважається власником. Власником інформаційного ресурсу вважається роботодавець або замовник.

Наявність у особи права власності на матеріальний об'єкт, що є носієм тієї або іншої інформації, не є підставою для виникнення у зазначеної особи права власності на сам інформаційний продукт.

Право власності на засоби обробки і захисту даних не створює права власності на інформаційні ресурси, що обробляють за допомогою цих засобів. Належність і режим використання похідної продукції, що створюється за допомогою зазначених засобів, визначається угодою між власником ресурсу і суб'єктами діяльності у сфері інформатизації.

Складові частини інформаційних ресурсів можуть відноситися до різних форм власності і виступати як товар, за винятком випадків, передбачених чинним законодавством України.

Суб'єкти діяльності у сфері інформатизації є власниками тих складових частин або компонентів об'єктів, що були створені ними, за рахунок їхніх коштів або придбані на законних підставах.

Майнові права на інформаційні ресурси можуть відчужуватися на загальних підставах, передбачених законодавством України про власність.

4.2.4. Обробка і доступ до інформаційних ресурсів

Інформаційні ресурси в Україні обробляються відповідно до Конституції України, законів України "Про інформацію", "Про державну таємницю", "Про науково-технічну інформацію" та інших законодавчих актів України.

Порядок обробки інформаційних ресурсів різних видів регламентується відповідними нормативно-правовими актами Кабінету Міністрів України.

Органи державної влади обробляють інформаційні ресурси згідно зі своїми повноваженнями.

Громадяни, органи державної влади, органи місцевого самоврядування, організації й об'єднання громадян зобов'язані надавати документовану інформацію органам і організаціям, відповідальним за формування державних інформаційних ресурсів відповідно до чинного законодавства. Переліки документованої інформації, що надають в обов'язковому порядку, а також переліки органів і організацій, відповідальних за обробку і захист державних інформаційних ресурсів, затверджуються Кабінетом Міністрів України.

Порядок надання (одержання) інформації, віднесеної до державної таємниці, персональних даних й іншої конфіденційної інформації установлюється відповідно до законодавства про ці категорії даних.

Доступ до інформаційних ресурсів здійснюється за згодою власника інформаційних ресурсів на підставі укладеної угоди або закону.

Доступ до даних, інформація яких становить державну таємницю, є обмеженим. Він може здійснюватися лише за згодою відповідних державних органів і згідно з нормами закону.

Особливості доступу до інформаційних продуктів, що входять до складу національних інформаційних ресурсів. Громадяни, органи державної влади й органи місцевого самоврядування, організації й об'єднання громадян мають рівні права доступу до інформаційних продуктів, що входять до складу національних інформаційних ресурсів. Виключення становлять інформаційні продукти, що містять інформацію, віднесену законом до категорії "з обмеженим доступом".

Порядок обробки і доступу до інформаційних ресурсів, що входять до складу національних інформаційних ресурсів, визначає адміністратор системи національних інформаційних ресурсів (центру інформаційних ресурсів).

Переліки видів послуг з інформаційного забезпечення, відомості про порядок і умови доступу до інформаційних продуктів системи національних інформаційних ресурсів надаються безкоштовно або за плату.

Для інформаційних продуктів, створених на кошти державного бюджету, встановлюється такий режим доступу :

• відкритий публічний доступ — якщо вони містять відкриту інформацію, доступ до якої гарантується чинним законодавством кожній юридичній або фізичній особі безкоштовно;

• платний доступ — у порядку, встановленому чинним законодавством;

Порядок доступу до інформаційних продуктів, що входять до складу національних інформаційних ресурсів і містять документовану інформацію, віднесену до категорії "з обмеженим доступом", регламентується відповідно до чинного законодавства.

Доступ до інформаційних продуктів, що входять до складу національних інформаційних ресурсів, інформація в яких може стосуватися законних прав і інтересів громадян, здійснюють з дозволу цих громадян або їхніх законних представників.

Зазначене обмеження не поширюється на письмові запити судів, правоохоронних органів, органів виконавчої влади, на які покладені повноваження щодо контрольно-ревізійних функцій, а також у випадках, передбачених чинним законодавством.

Порядок доступу до інформаційних продуктів, розроблених за межами України, повинен відповідати нормам міжнародного інформаційного права, ратифікованих Україною міжнародних договорів і угод, а також умовам ліцензійних угод із власником, положення яких повинні виконуватися незалежно від джерела коштів на придбання інформаційних продуктів.

Відомості, отримані на законних підставах з національних інформаційних ресурсів громадянами й організаціями, можуть використовуватися ними для створення похідного інформаційного продукту з метою його комерційного поширення (реалізації) з обов'язковим посиланням на джерело.

Особливості доступу до веб-ресурсу. Доступ до веб-ресурсу є вільним. Це передбачає можливість копіювання, використання на свій розсуд і поширення інформаційного ресурсу, але з обов'язковим урахуванням права власності, авторських, патентних прав і інтересів третіх осіб, за винятком умов, визначених чинним законодавством.

Інформація, що не підлягає розміщенню на веб-ресурсі. Власник веб-ресурсу або уповноважена ним особа (власник) має право розміщувати на ньому будь-яку інформацію, що відповідає вимогам закону і моралі.

При розміщенні інформації на веб-ресурсі власник повинен:

- не розміщувати на своєму веб-ресурсі інформацію насильницького або іншого антигуманістського змісту;
- поважати релігійні, національні, культурні, політичні, професійні, соціальні та інші права громадян і не поширювати інформацію, що може спровокувати національну або релігійну ворожнечу;
- не поширювати інформацію, що може зашкодити честі, гідності або діловій репутації окремих осіб;
- не поширювати персональні дані без згоди суб'єкта даних, а також іншу конфіденційну інформацію;
- дотримуватись норм культури і суспільної моралі;
- не поширювати заклики до насильницької зміни конституційного порядку або територіальної цілісності України;
- не пропагувати війну, насильство і жорстокість;
- не поширювати відверто неправдиву, перекручену й іншу неякісну інформацію;
- не поширювати порнографію;
- не вживати лайливих і брутальних слів при викладі інформації;
- не поширювати інформацію, що знаходиться у власності іншої особи, без її письмової згоди.

Забороняється використання веб-ресурсу для:

- втручання в особисте та сімейне життя громадян;
- розміщення персональних даних у складі бази даних загального інформаційного змісту і створення єдиної бази даних інформаційних ресурсів;
- поширення відверто помилкових, перекручених повідомлень (дезінформації).

Власник або володілець ресурсу у випадку завдання йому моральної або матеріальної шкоди в результаті поширення веб-ресурсу має право на повне відшкодування шкоди відповідно до чинного законодавства України на підставі судового рішення.

Веб-ресурси як засіб масової інформації. Власник веб-ресурсу або інша уповноважена особа може зареєструвати належний йому інформаційний ресурс як засіб масової інформації.

Право на встановлення мережного засобу масової інформації мають:

- громадяни України, громадяни інших держав і особи без громадянства;
- юридичні особи України й інших держав;
- трудові колективи організацій і підприємств при відповідному рішенні загальних зборів (конференції).

Суб'єкт, що здійснює реєстрацію засобу масової інформації, визнається його засновником і власником.

Засіб масової інформації у зв'язку із застосуванням телекомунікаційних мереж підлягає обов'язковому державному обліку і реєстрації відповідно до порядку, встановленого Кабінетом Міністрів України для друкованих засобів масової інформації.

Процедура реєстрації включає в себе надання заяви про реєстрацію до державного органу реєстрації, сплату реєстраційного збору й одержання свідоцтва про реєстрацію.

Веб-сайт персональних даних. Більшість національних законів сфери захисту персональних даних мають типову назву – закон про захист даних. В них знаходить вираз основної мети визначеної у статті 1 Конвенції № 108 Ради Європи "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних": "Метою цієї Конвенції є забезпечення на території кожної країни для кожної особи, незалежно від її громадянства або місця проживання, поваги до її прав і основних свобод і зокрема права на особисте життя у зв'язку з автоматизованою обробкою персональних даних, що її стосуються ("захист даних")".

Під захистом даних (date protection) розуміють будь-який правовий, організаційний, технічний (технологічний, криптографічний, програмний) захист інформації персонального змісту. Усі закони під зазначеною назвою забезпечують захист персональних даних. Для комплексного захисту даних на міжнародному рівні застосовується термін "безпека даних" (data security), тобто в даному випадку мова йде про інформаційну безпеку.

Для уникнення термінологічної плутанини поняття "захист даних" варто тлумачити у тому сенсі, що встановлено ст. 1 Конвенції № 108 Ради Європи.

Вимоги до веб-сайта персональних даних установлюються національним законодавством про захист персональних даних.

Головні вимоги згідно з нормами міжнародних стандартів:

- забороняється об'єднання веб-сайту персональних даних з веб-сайтами будь-яких даних загального інформаційного змісту без письмової згоди власника персональних даних;
- не допускається обробка і використання персональних даних у веб-сайтах персональних даних без письмової згоди власника персональних даних, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту і прав людини;
- відповідальним за поширення відомостей з веб-сайта персональних даних через службу зв'язку або електронну пошту вважається та особа, що відправляє дані. Провайдер послуг відповідає за додаткову обробку персональних даних, що необхідна йому для здійснення поширення;
- кожна фізична особа зобов'язана не розголошувати персональні дані, що стали відомі у зв'язку з виконанням службових обов'язків і після закінчення службових обов'язків в органах державної влади й органах місцевого самоврядування, організаціях, установах і підприємствах усіх форм власності.

На закінчення викладеного у підрозділах 4.1 та 4.2, має зазначити наступне. Суб'єктивні інтереси та уявлення про упорядкування суспільних відносин історично завжди не дуже відповідали та не відповідають потребам порядності, справедливості та правди у відносинах. Писані норми поведінки – це одне, їх застосування – інше. Звідси виникла впевненість про те, що юриспруденція не має моралі.

Як вважаємо, одне з головних завдань інформаційного законодавства є врахування такого історично феномену, як маніпулювання свідомістю людей. Цей вплив на людину має назву рефлексивного (від слова "рефлекс" – мимовільна реакція на зовнішні або внутрішні подразники, надбані в результаті неодноразової їх дії) управління думкою. Якщо

вплив на людину, зокрема, інформаційний, здійснюється свідомо та через обман щодо неправдивих, брехливих та ін. дезінформаційних відомостей, то це розглядається як маніпулювання її свідомістю у корисних інтересах, що створює умови порушення прав людини і свобод, сприяє не стабільності у суспільстві та збільшує дезорганізацію в управлінської діяльності держави. Питанню інформаційного захисту й присвячений наступний підрозділ.

4.3.5. Засоби захисту інформаційних ресурсів

4.3.5.1. Захист від маніпулювання свідомістю

Питання захисту інформаційних ресурсів безпосередньо стосується такого феномена, як рефлексивне управління суспільною думкою та захисту від маніпулювання свідомістю. Використання неправдивої, недостовірної, "перекрученої" тощо інформації робить людину, суспільство або державу вразливими для деструктивного політичного, економічного чи соціального впливу на них, що яскраво виявляється у виборчих технологіях. У зв'язку з цим і виникли такі поняття, як "інформаційна боротьба", "електронна боротьба", "інформаційне протиборство" та узагальнююче поняття "інформаційна війна", про що йшлося у підрозділі 1.3, ретельно дослідженого нами у [170]. В інформаційних війнах застосовують широкий клас засобів інформаційного нападу (інформаційної зброї) на противника, спрямованих на ведення радіоелектронної, електронно-інформаційної війн (зокрема, засоби комп'ютерної агресії, яка здійснюється завдяки файлам-вірусам, що порушують або перепрограмовують інформаційні системи) та інформаційно-психологічного впливу на людину (див. схему "Інформаційні війни: види, зміст, зброя, засоби нападу та захисту" Додаток 3). Зазначене, у сутності, спрямовано на обман та маніпулювання свідомістю людини, що здійснюється нерідко за допомогою пропаганди, агітації, дезінформації тощо.

У сучасному світі діє безліч маніпуляторів – від несумлінного продавця і ринкового шахрая, до цілих організацій, що спеціалізуються на економічних аферах і політичному інтриганстві, озброєних найсучаснішими знаннями і щонайпотужнішим апаратом інформаційної дії на психіку людини. Що може їм протиставити звичайний громадянин і чи може він встояти під цим натиском маніпуляцій, зберігши свою душу, здатність ясно мислити і орієнтуватися, зберегти свободу власного вибору і раціональної усвідомленої поведінки?

Достатньо широко відомий латинський вислів, що дійшов до наших днів, який у вигляді короткого афоризму формулюється таким чином – хто попереджений, той озброєний. У короткій і метафоричній формі він відображає одну з необхідних умов успішного захисту – своєчасне знання про небезпеку, яка загрожує людині, дозволяє їй підготуватися до захисту.

У наш час необхідно постійно бути готовим до того, що як у безпосередньому спілкуванні, так і в засобах масової комунікації (газети, телебачення, кіно, Інтернет тощо), у різних виступах перед масовою аудиторією свідомо чи ні, цілеспрямовано або мимоволі застосовуються психологічні засоби дії маніпулятивного змісту, і часто не для нашої користі, а навпаки, нам на шкоду. Людина, яка попереджена і володіє знаннями, може самостійно створити відносно простий, але достатньо ефективний механізм захисту у вигляді психологічного бар'єру недовіри до тих потоків рекламно-пропагандистської інформації, за допомогою яких йде масована обробка населення, і

сформувати установку на необхідність застосування відповідних способів аналізу інформації [103].

Люди в різному схильні до маніпулятивного впливу, в різній мірі володіють здатністю відрізняти правду від вигадки і брехні, уловлювати обман, нещирість і приховані задуми в діях інших людей. Одні – більш проникливі, інші – менш. Вважається, що проникливість не стільки природжена якість, а більшою мірою формується з часом, виробляється з роками в процесі практичної діяльності, пов'язаної з інтенсивним спілкуванням і взаємодією з людьми [138].

Чи можливо визначити і описати в достатньо простих поняттях, як людина може захищатися від маніпуляцій, різноманітних способів і засобів інформаційно-психологічної дії, що звалюються на неї в сучасних умовах? З'ясувати, яким чином це відбувається і як організувати процес свого захисту, щоб забезпечити необхідний рівень власної безпеки? Як визначити, що саме необхідно захищати, від чого конкретно і хто повинен захищати людину в сучасному суспільстві, якими засобами і в який спосіб це робити? Перш ніж спробувати відповісти на ці непрості запитання, необхідно з'ясувати, що таке захист, у чому специфіка захисту від маніпуляцій, її взаємозв'язок з інформаційно-психологічною безпекою людини.

У найзагальнішому вигляді інформаційно-психологічну безпеку людини можна розглядати як стан захищеності психіки від дії багатоманітних інформаційних чинників, що перешкоджають або утруднюють формування і функціонування адекватної інформаційне орієнтовної основи соціальної поведінки людини і в цілому життєдіяльності в суспільстві. Тобто такий стан, який дозволяє повноцінно розвиватися, своєчасно адаптуватися до змінних соціальних умов і організовувати свою поведінку (життєдіяльність), що дозволяє задовольняти основні потреби суспільства в соціально прийнятних формах з урахуванням інтересів і діяльності інших людей та діючих соціальних інститутів.

З урахуванням цих уявлень психологічна захищеність звичайно розглядається в контексті взаємозв'язку з психологічним захистом людини і механізмами, що її забезпечують. У цьому контексті під психологічною захищеністю розуміється відносно стійке позитивне емоційне переживання і усвідомлення індивідом можливості задоволення своїх потреб і забезпеченості власних прав у будь-якій, навіть несприятливий ситуації, при виникненні обставин, які можуть блокувати або утруднювати їх реалізацію.

Як основний механізм забезпечення психологічної захищеності виступає психологічний захист - спеціальна регулятивна система стабілізації особи, направлена на усунення або зведення до мінімуму відчуття тривоги, пов'язаного з усвідомленням конфлікту. Відповідно до такого підходу, як основна її функція розглядається "огорожа" сфери свідомості від негативних, травмуючих психіку особи переживань.

Існуючі підходи до психологічної оборони свідчать про те, що у людини є дві основні і достатньо автономні спеціальні регулятивні системи, які забезпечують її психологічну захищеність, відповідно, від внутрішнього психологічного дискомфорту і від зовнішньої психологічної дії. Ці системи мають складну будову і забезпечуються різними психологічними механізмами.

Психологічний захист від зовнішніх дій може реалізовуватися у наступних основних різновидах, відмінних певною специфічністю функціонування:

• по-перше, свідомий і підсвідомий психологічний захист. Він здійснюється на усвідомленому та рефлексивному рівнях завдяки життєвому досвіду, інтелектуальній підготовці, психологічному стану тощо тих, на кого спрямована дія. Другий від включається під впливом самої зовнішньої дії;

• по-друге, індивідуальний і груповий психологічний захист. "Носієм" першого з них є окрема особа, другого – соціальна група;

• по-третє, загальний і спеціальний психологічний захист (або неспецифічний і специфічний). У першому з них реалізується загальна критичність особи у відношенні до зовнішніх дій. Він відрізняється широтою і охоплює більшість зовнішніх дій, але в той же час є слабкою протидією їм, хоча і в різному ступені та у різних осіб.

Спеціальний, або приватний психологічний захист має вужчу сферу дії, аж до фіксації на конкретному суб'єкті або певному змісті дії, але в той час він володіє значно більшою силою.

Психологічному захисту від зовнішніх дій властиві такі ознаки, як селективність і динамізм. Селективність, або вибірковість реалізується в тому, що навіть один і той самий об'єкт дії знаходить різний ступінь протидії різним суб'єктам, а також різному змісту дій, які витікають від одного і того ж суб'єкта. Динамізм психологічного захисту виявляється в коливаннях його реальної дієвості як у бік збільшення, так і у бік зниження.

Таким чином, приватно-правовий захист від маніпуляцій складається з двох чинників:

• особистий (внутрішній) захист психоаналітичної орієнтації;

• міжособовий, груповий або колективний захист від зовнішніх загроз і дій.

Згідно з І. Грачовим [103] розгляд еволюції способів захисту, починаючи від тваринного світу до людини, дозволяє виділити наступні основні форми захисту.

1. *Відхід* – збільшення дистанції, переривання контакту, вихід за межі досяжності дії. Проявами цього виду захисту є:

а) у міжособових ситуаціях – зміна теми бесіди (на безпечнішу), небажання загострювати відносини (обхід "слизьких тем", "гострих кутів"), прагнення ухилитися від зустрічей з тим, хто є джерелом неприємних переживань (відмова, перенесення, ухилення від зустрічей); уникнення травмуючих ситуацій, під різними приводами переривання зустрічей, бесід і т. п.

Крайнім виразом даної тенденції може стати повна замкнутість, відчуженість, відмова від контактів з людьми;

б) у контакт-комунікаційних ситуаціях – залишення під різними приводами (для себе і оточуючих) мітингів, зборів, різних видовищних заходів і т. п. або різні форми відмови від участі і присутності на подібних заходах;

в) у мас-комунікаційних ситуаціях – відключення від певних каналів засобів масової інформації, від перегляду конкретних теле-, радіопрограм, відмова від читання деяких газет, статей, рубрик тощо.

2. Вилучення (витіснення) – збільшення дистанції, видалення, витіснення джерела дії:

а) у міжособових ситуаціях – видалення з місця мешкання, роботи, відпочинку; вигнання з будинку (ном'якшена форма – "іди, щоб я тебе не бачив" тощо), відсилання кудись під певним приводом (зокрема, звільнити з роботи тощо); приниження як трансформація знищення через духовну форму у вигляді насмішок, тощо (тобто часткове знищення особистих можливостей – рис вдачі, звичок, вчинків, намірів, схильностей тощо); образа і провокація конфлікту, сварки, що змушує перервати контакт, розірвати відносини, піти і таким чином збільшити дистанцію.

Крайніми формами тут можуть виступати конфлікти, що приводять до фізичної дії, наприклад, шляхом бійки і як граничний вираз – знищення;

б) у контакт-комунікаційних ситуаціях – "закриття" виступаючих, їх переривання, насмішки, репліки, образи, свист та інші демонстраційні дії і перешкоди, що змушують

комунікатора перервати контакт і віддалитися. Ці способи можуть трансформуватися в такі форми, як закидання різними предметами та інші види фізичної дії. Це притаманно для деяких категорій учасників видовищних заходів і спортивних уболівальників;

в) у мас-комунікаційних ситуаціях – м'якими формами аналогічними (як і у випадку з вигнанням) є відключення від каналів інформації. У крайньому вираз можуть трансформуватися в спроби фізичного знищення джерела комунікації.

3. *Блокування* (відгородження, перешкода) – контроль дії, що досягає суб'єкта захисту, виставляння перешкод, відгородження психіки від зовнішньої дії:

а) у міжособових ситуаціях – відчуженість (офіційність, ведення бесіди з застосуванням фізичних розділових перешкод, наприклад, через стіл, збільшення міжособового простору), різні психологічні бар'єри (недовір'я, настороженість, ворожість), смислові та семантичні ("я вас погано розумію", "мені важко зрозуміти, в чому суть..." тощо), ролеві ("я на роботі", "при виконанні службових обов'язків", "мені зараз ніколи, зайнятий, не зараз, потім..." тощо), приниження джерела дії ("непрофесіонал", "слабкий фахівець", "несерйозний", "безвідповідальний", "пройдисвіт", "все це і так відомо", "в цьому немає нічого нового", "не розуміє складності ситуації", "несе нісенітницю", "робить все, тільки щоб виділитися" тощо) і т. п.;

б) у контакт-комунікаційних ситуаціях – підвищення негативізму, критичності, емоційної відчуженості, також застосовуються психологічні бар'єри, приниження джерела (внутрішнє осміяння, спотворення авторитету тощо), неуважність (відвертання і переключення уваги на інші об'єкти, не пов'язані із змістом дії) тощо;

в) у масс-комунікаційних ситуаціях – аналогічно попередньому пункту "б".

4. *Управління* – контроль за процесом дії, вплив на її складові і джерело:

а) у міжособових ситуаціях – демонстрація загрози (небезпеки): "підкуп" і прагнення "вмилостивити"; стати другом, членом однієї спільності ("своїх не б'ють"); прагнення розжалобити (плач, скарги, нючі інтонації, зітхання, нещасний вигляд); ослабити або дестабілізувати активність (несподіваною відвертістю тощо); спровокувати бажану поведінку (зокрема, різні прийоми міжособових маніпуляцій як спосіб захисту).

Граничний вираз – психологічне і фізичне підпорядкування іншого, зневага ним (наприклад, в тоталітарних релігійних сектах, деяких асоціальних угрупованнях з кримінальним лідером і т. п.);

б) у контакт-комунікаційних ситуаціях – можливості управління дуже слабкі.

У деяких ситуаціях можливе застосування зворотного зв'язку як способу управління (наприклад, у видовищних заходах вираз реакції на виступ за допомогою аплодисментів, виклику на біс, різні прояви несхвалення, незадоволеність виступаючими тощо);

в) у мас-комунікаційних ситуаціях – управління практично неможливе. У деяких ситуаціях за рахунок застосування зворотного зв'язку як способу управління може досягатися певний управляючий ефект (зміни рейтингу популярності певних каналів телебачення, скорочення або збільшення розпродажу періодичних видань тощо).

5. *Затамовування* (маскування) – контроль інформації про самого суб'єкта захисту, її спотворення, приховування або скорочення подачі:

а) у міжособових ситуаціях – маскування, обман, приховування відчуттів, проявів емоцій, затримка або відмова від дій, щоб не проявляти себе (не накликати біду);

б) у контакт-комунікаційних ситуаціях – маскування, приховування відчуттів, проявів емоцій, затримка або відмова від дій (особливо при знаходженні в натовпі, щоб не піддатися "ефекту натовпу", психічному зараженню і не зробити вчинків, про які потім можна буде жалкувати);

в) у масс-комунікаційних ситуаціях – відстрочення реакцій, поспішних висновків і оцінок, затримка або відмова від дій і вчинків, що викликаються інформаційною дією (для подальшого раціонального і зваженого аналізу із залученням додаткових даних).

6. *Ігнорування* – контроль інформації про джерело дії, наявність або зміст загрози (небезпеки); обмеження кількості такої інформації або її спотворене сприйняття.

Цілком обґрунтованою є існуюча на сьогодні точка зору, що застосування даної форми приватно-правового захисту виправдано, незважаючи на наявну, на перший погляд, неефективність і навіть шкідливість для людини такого захисного механізму. Застосування такої форми захисту цілком доцільне і виправдане, якщо сама інформація і її поширення служать способом маніпулювання особою або коли решта форм захисту з будь-яких причин не задіються, а психіка потребує захисту від надмірного травмування емоційними чинниками, що викликаються зовнішньою інформацією.

У зв'язку з цим, застосування механізмів внутрішньоособистого психологічного захисту виправдане:

а) у міжособових ситуаціях – ігнорування інформації, що утруднює або перешкоджає певній діяльності (наприклад, перебільшення сили і можливості суперника, труднощів досягнення поставленої мети для того, щоб людина відмовилася від цього і т. п.); ігнорування інформації про певні дії, спрямовані на людину з боку джерела дії (наприклад, за ситуації, коли керівник, колега або близька людина знаходяться в стані емоційного збудження і адекватно відповісти їй – значить вступити в конфлікт, який пізніше важко або неможливо локалізувати); в той же час сприйняття адекватності оцінки ситуації може знижуватися, наприклад, на основі стереотипізації ("так він просто хуліганить", "переказиться, і все буде нормально" тощо), применшення ступеню загрози за допомогою пояснення позитивними намірами джерела дії ("вона бажає мені добра" тощо);

б) у контакт-комунікаційних ситуаціях – ігнорування інформації, що утруднює чи перешкоджає певній діяльності, або інформації як засобу маніпулювання особою в натовпі, в місцях масового скупчення людей (наприклад, для запобігання підвищенню емоційної сприйнятливості, тривожності, навіюваності, схильності до психічного "зараження"; для блокування емоцій, відчуттів, дій як спонтанної реакції на заклики й інші дії, що стимулюють прояв певних відчуттів, потреб, поведінки тощо);

в) у масс-комунікаційних ситуаціях – ігнорування інформації як засобу маніпулювання особою в різних аспектах (чутки, дезінформація, брехня, уявні прогнози, кон'юнктурні оцінки тощо).

Звичайно, будь-яка узагальнена модель – це завжди лише певна схематизація явищ, що відбуваються насправді. У реальному житті початкові форми захисту видозмінюються, утворюють химерні поєднання і комбінації залежно від індивідуальних особливостей людей, умов і конкретних ситуацій. Так, в управлінні процесом взаємодії, затаювання може виступати як самостійна пасивна форма або як поєднання з активними способами захисту.

При блокуванні дії ігнорування інформації виступає як один з різновидів цієї форми захисту. Її виділення в окрему самостійну форму захисту може бути виправдане тим, що в цьому випадку максимально активно задіються механізми внутрішньоособового психологічного захисту, здатні специфічно впливати на психіку людини.

В організаційному плані виділяють три основні рівні захисту людини і, відповідно, три основні напрями його формування і функціонування:

1) соціальний (у масштабах держави в цілому);

2) соціально-груповий (в межах різних соціальних груп і різноманітних форм соціальних організацій);

3) індивідуально-особовий.

На соціальному (державному) рівні психологічний захист реалізується за допомогою правового регулювання і організації інформаційних потоків (система поширення інформації в суспільстві) і розповсюдження способів і засобів, певних "алгоритмів" обробки і оцінки інформації в процесі соціальної взаємодії (від міжособового спілкування до масової комунікації). На цьому рівні як суб'єкти психологічного захисту особи виступають держава і суспільство через діяльність певних соціальних інститутів (система освіти, система розповсюдження соціокультурних цінностей, традицій, соціальних норм тощо).

На соціально-груповому рівні психологічний захист реалізується за допомогою розповсюдження і застосування внутрішньогрупових інформаційних потоків і джерел, а також специфічних для конкретних соціальних груп і організацій способів соціальної взаємодії, переробки і оцінки інформації (групових норм, орієнтації, переваг визначених комунікаторів, регламентація правил і процедур роботи та взаємодії із зовнішніми інформаційними джерелами тощо). На цьому рівні як суб'єкти психологічного захисту особи виступають групи і організації (сім'я, виробничі структури, громадські, політичні, релігійні та ін. організації).

На індивідуально-особовому рівні психологічний захист реалізується за допомогою формування специфічної регулятивної системи і комплексу захисних механізмів та алгоритмів поведінки, які утворюють індивідуальний приватно-правовий захист.

Для термінологічного розрізнення, стосовно соціального рівня, можна застосовувати термін "соціально-психологічний захист", для соціально-групового – термін "соціально-психологічний або груповий психологічний захист", що знаходить вираз у правилах суспільної моралі.

На індивідуально-особовому рівні психологічний захист реалізується в наступних різновидах: внутрішньоособовий психологічний захист і індивідуальний соціально-психологічний захист, який поділяється на міжособовий психологічний захист (при взаємодії в міжособових комунікативних ситуаціях) і захист від інформаційно-психологічних дій у масс-комунікаційних і контакт-комунікаційних ситуаціях (тобто, відповідно, при взаємодії з інформаційними джерелами або у складі певних груп).

Враховуючи, що поняття психологічного захисту достатньо широко поширилося і вийшло за межі його первинного значення як внутрішньоособового захисту, можна говорити про його загальне і конкретне розуміння.

Тому при розгляді соціального і соціально-групового рівнів було б доцільно застосовувати термін "соціально-психологічний захист особи".

При розгляді ж індивідуально-особового рівня можна застосовувати терміни "психологічний захист особи" або "психологічний самозахист", враховуючи при цьому, що він включає як складові компоненти міжособовий і внутрішньоособовий психологічний захист.

Підтримка інформаційно-психологічної безпеки припускає організацію і здійснення захисних заходів, які в найзагальнішому вигляді доцільно виділити в наступні основні групи, що визначаються певною організаційною самостійністю і застосованими заходами: приватно-правового регулювання, зокрема, обмеження інформаційних потоків; організації інформаційних потоків (зокрема, ініціація поширення певної інформації); розповсюдження способів і засобів обробки і оцінки інформації; участь у формуванні колективного або групового соціально-психологічного захисту; формування індивідуального психологічного захисту або психологічного самозахисту особи.

Перші дві з вказаних вище груп пов'язані із зміною "зовнішнього" для особи інформаційного середовища. Наступні три визначаються зміною механізмів і способів взаємодії людини з "зовнішнім" інформаційним середовищем.

Перша група захисних заходів звичайно застосовується на обмежених проміжках часу, в специфічних умовах або у відношенні до певних джерел і інформаційних каналів. Можуть, зокрема, застосовуватися такі заходи, як введення певних процедур перевірки достовірності поширюваної інформації (наприклад, такої, що впливає на ухвалення управлінських рішень); обмеження розповсюдження певних відомостей (наприклад тих, що сприяють виникненню агресивних чуток, паніки і т. д.) в надзвичайних ситуаціях; введення цензури в умовах бойових дій тощо.

За відсутності насправді демократичної культури в суспільстві ці заходи можуть застосовуватися також для маніпулювання людьми шляхом обмеження доступу до інформації, її приховування і т. п. На особовому рівні застосування захисних заходів з цієї групи пов'язане звичайно з ініціативною відмовою людини від використання певної інформації, джерел або каналів її розповсюдження (наприклад, відмова від рекламної інформації, "спаму" тощо) або повторною перевіркою значущої для неї інформації.

Друга група пов'язана з організацією інформаційних потоків, направлених на попередження) та нейтралізацію дії певних інформаційних чинників, які можуть психологічно негативно впливати на людей (так, наприклад, при виникненні чуток використовується поширення відомостей, що нейтралізують їх вплив). На особовому рівні це виявляється в ініціативному пошуку з певних тем додаткової інформації з різних джерел і в організації її надходження по інших каналах.

Третя група включає різноманітні форми поширення способів і засобів обробки та оцінки інформації (через системи освіти, підготовки і перепідготовки кадрів, розповсюдження соціокультурних цінностей, традицій, соціальних норм тощо).

Четверта група пов'язана з формуванням колективного психологічного захисту, який грунтується на механізмах ідентифікації людини з певними соціальними об'єднаннями людей. Це визначає використання особою при аналізі і відборі інформації певних групових оцінок, норм, думок тощо, також її орієнтацію на внутрішньогрупові інформаційні потоки і джерела.

З урахуванням цього для організації групового психологічного захисту можуть застосовуватися: різні прийоми і засоби формування відповідного соціально-психологічного клімату в колективах, атмосфери корпоративності; створення умов, що підвищують ефективність процесу ідентифікації особи з певною соціальною групою, і актуалізації відчуття приналежності до конкретної соціальної організації, її діяльності; підготовка неформальних лідерів, які виступають як "медіатори", авторитетних внутрішньогрупових джерел інформації тощо.

П'ята група пов'язана з формуванням у людини в процесі набуття досвіду інформаційно-комунікативної взаємодії (зокрема, навчання з застосуванням спеціалізованих форм психологічної підготовки, проведення тренінгових занять за спеціально розробленими методиками) алгоритмів психічної діяльності і захисної поведінки, які у своїй множині утворюють індивідуальну систему психологічного захисту або самозахисту особи.

З розглянутих вище напрямів підтримки інформаційної безпеки особи перші чотири залежать від зовнішніх для людини умов, діяльності інших соціальних суб'єктів, функціонування різних соціальних інститутів, інших людей. П'ятий напрям у першу чергу залежить від самої особи. Наприклад, чи хоче людина докласти певні зусилля для забезпечення власної інформаційно безпеки, для формування ефективної системи самозахисту або готова бути слухняною маріонеткою в руках численних маніпуляторів і рабом інформаційних пасток сучасного суспільства.

Головний висновок із зазначеного вище полягає в тому, що людина повинна сама захотіти навчатися та здійснювати власну, особисту інформаційно безпеку, бути постійно готовою захищати себе і близьких людей. Важливо при цьому досить обережно та уважно відноситися до будь-яких міркувань, обіцянок та завірень будь-яких політиків, виходити в своїх висновках з реальних фактів їх діяльності на благо суспільства та держави, а не з критики на адресу опонентів, тим більш, якщо для досягнення якихось цілей вони застосовують непристойність персональних даних. Ніколи не слід забувати слова одного з великих в історії інтриганів та маніпуляторів свідомістю Шарля Моріса Талейрана: "Обіцяйте, обіцяйте, обіцяйте. …Якщо хочеш вести людей на смерть, скажи що ведеш їх до слави" [89, с. 272-287; 170, с. 23].

4.3.5.2. Організаційно-технічний захист інформації

Інформаційний захист людини в умовах застосування новітніх інформаційно-комп'ютерних технологій та мереж, у зв'язку з витоком даних технічними каналами, потребує організаційних та техніко-технологічних знань та необхідності здійснити низки заходів.

Перш за все, треба проаналізувати специфічні особливості розташування будівель, приміщень в будівлях, територію навколо них і підведені комунікації. Потім необхідно визначити ті приміщення, усередині яких циркулює конфіденційна інформація, і врахувати застосовані в них технічні засоби. Далі слід здійснити такі технічні заходи:

- перевірити техніку на відповідність величини побічних випромінювань допустимим рівням;
- екранувати приміщення або техніку в приміщеннях;
- перемонтувати окремі лінії, кабелі;
- застосувати спеціальні пристрої і засоби пасивного та активного захисту.

Важливо підкреслити, що на кожен метод отримання інформації по технічних каналах існує метод протидії, часто не один, який може звести загрозу до мінімуму. При цьому успіх залежить від двох чинників – від компетентності в питаннях захисту інформації і даних та від наявності обладнання, необхідного для захисних заходів. Перший чинник важливіший другого, оскільки найдосконаліша апаратура залишиться мертвим вантажем у руках дилетанта.

У яких випадках доцільно проводити заходи захисту? Таку роботу необхідно здійснювати превентивно, не чекаючи поки "пролунає грім". Роль спонукального мотиву можуть відіграти відомості про витік інформації. Поштовхом до дії можуть стати сліди, що свідчать про проникнення в приміщення сторонніх осіб, або якісь дивні явища, пов'язані з використанням техніки (наприклад, підозрілий шум у телефоні).

Здійснюючи комплекс захисних заходів, не слід прагнути забезпечити захист всієї будівлі. Головне – обмежити доступ у ті місця і до тієї техніки, де зосереджена інформація з обмеженим доступом (не забуваючи, звичайно, про можливості і методи її дистанційного отримання). Зокрема, використання якісних замків, засобів сигналізації, хороша звукоізоляція стін, дверей, стель і підлоги, звуковий захист вентиляційних каналів, отворів і труб, що проходять через ці приміщення, демонтаж зайвої проводки, а також застосування спеціальних пристроїв (генераторів шуму, апаратури зв'язку, що засекречує (далі – ЗАС) та ін.) серйозно утруднять або зроблять безрезультатними спроби упровадження спецтехніки перехоплення інформації.

Саме тому для розробки і реалізації заходів захисту інформації від витоку технічними каналами треба запрошувати кваліфікованих фахівців або готувати власні кадри за відповідними програмами технічного захисту обробки та передачі інформації (далі ТЗОІП).

Заземлення ТЗОІІ. Однією з найважливіших умов засобів ТЗОІІ є правильне заземлення цих пристроїв. На практиці найчастіше доводиться мати справу з радіальною системою заземлення, яка має менше загальних ділянок для проходження сигнальних і живлячих струмів у зворотному напрямі (від засобів ТЗОІІ до сторонніх спостерігачів).

Шина і контур не повинні мати петель, а виконуються у вигляді дерева, що гілкується, де опір контуру не перевищує 1 Ом. Ця вимога виконується застосуванням як заземлювачів стрижнем з металу, що мають високу електропровідність, занурених у землю і сполучених з металевими конструкціями засобів ТЗОІІ. Найчастіше це вертикально вбиті в землю сталеві труби завдовжки в 2 – 3 м і діаметром 35 – 50 мм. Труби добрі тим, що дозволяють досягати вологих шарів землі, що мають найбільшу провідність і не схильні до висихання або промерзання. Крім того, використання труб не пов'язано з значними земляними роботами.

Опір заземлення визначається головним чином опором розтікання струму в землі. Його величину можна значно понизити за рахунок зменшення перехідного опору (між заземлювачем і ґрунтом) шляхом ретельного очищення поверхні труби від бруду та іржі, підсипанням в лунку по всій її висоті кухонної солі і утрамбовуванням ґрунту навколо кожної труби. Заземлювачі (труби) слід сполучати між собою шинами за допомогою зварювання. Перетин шин і магістралей заземлення для досягнення механічної міцності і отримання достатньої провідності рекомендується брати не менше 24 х 4 мм.

Магістралі заземлення поза будівлею треба прокладати на глибині близько 1,5 м, а усередині будівлі – по стінах або спеціальних каналах, щоб можна було їх регулярно оглядати. Сполучають магістралі із заземлювачем тільки за допомогою зварювання, а до ТЗОІІ магістраль підключають болтовим з'єднанням в одній точці. У разі підключення до магістралі заземлення декількох засобів ТЗОІІ сполучати їх з магістраллю треба паралельно (при послідовному з'єднанні відключення одного засобу ТЗОІІ може призвести до відключення всіх інших). При пристрої заземлення засобу ТЗОІІ не можна застосовувати природні заземлювачі: металеві конструкції будівель, що мають з'єднання із землею, прокладені в землі металеві труби та оболонки підземних кабелів.

Мережні фільтри. Виникнення заведень в мережах живлення засобів ТЗОІІ найчастіше пов'язане з тим, що вони підключені до загальних ліній живлення. Тому мережні фільтри виконують дві функції в ланцюгах живлення засобів ТЗОІІ: захисту апаратури від зовнішніх імпульсних перешкод і захисту від завад, створюваних самою апаратурою. При цьому однофазна система розподілу електроенергії повинна здійснюватися трансформатором із заземленою середньою точкою, трифазна – високовольтним знижувальним трансформатором.

При виборі фільтрів потрібно враховувати: номінальні значення струмів і напруг у ланцюгах живлення, а також допустимі значення падіння напруги на фільтрі при максимальному навантаженні; допустимі значення реактивної складової струму на основній частоті напруги живлення; необхідне загасання фільтру; механічні параметри фільтру (розмір, маса, тип корпусу, спосіб установки); ступінь екранування фільтру від сторонніх полів.

Фільтри в ланцюгах живлення можуть мати різні конструкції, їх маса коливається в межах від 0,5 кг до 90 кг, а об'єм – від 0,8 $см^3$ до 1,6 $м^3$. Конструкція фільтру повинна забезпечувати істотне зниження вірогідності виникнення усередині корпусу побічного зв'язку між входом і виходом через магнітні, електричні або електромагнітні поля.

Екранування приміщень. Для повного усунення в приміщеннях завад від техніко-електронних засобів, лінії яких виходять за межі контрольованої зони, треба не тільки

пригнітити їх у дротах, що відходять від джерела, але й обмежити сферу дії електромагнітного поля, створюваного системою її внутрішніх електропроводок. Ця задача розв'язується шляхом екранування.

Теоретично, з погляду вартості матеріалу і простоти виготовлення, перевагу на боці екранів з листової сталі. Проте застосування сітки значно спрощує вентиляцію і освітлення. Щоб вирішити питання про матеріал екрана, необхідно знати, у скільки разів вимагається ослабити рівні випромінювання засобів ТЗОІІ. Найчастіше це між 10 і 30 разами. Таку ефективність забезпечує екран, виготовлений з одинарної мідної сітки з осередком 2,5 мм або з тонколистової оцинкованої сталі завтовшки 0,51 мм і більше.

Металеві листи (або полотнища сітки) повинні бути електрично міцно сполучені між собою по всьому периметру, що забезпечується електрозварюванням або паянням. Двері приміщень також необхідно екранувати із забезпеченням надійного електроконтакту з дверною рамою по всьому периметру не рідше ніж через 10 – 15 мм. Для цього застосовують пружинну гребінку з фосфорної бронзи, укріплюючи її по всьому внутрішньому периметру дверної рами. За наявності в приміщенні вікон їх затягують одним або двома шарами мідної сітки з осередком не більше ніж 2 х 2 мм, причому відстань між шарами сітки повинна бути не менше 50 мм. Обидва шари повинні мати добрий електроконтакт із стінками приміщення за допомогою тієї ж гребінки з фосфорної бронзи або паяння (якщо сітка не знімається).

Розміри приміщення, що екранується, вибирають, виходячи з його призначення, наявності вільної площі і вартості робіт. Звичайно достатньо мати приміщення площею 6 – 8 $м^2$ при висоті 2,5 – 3 м.

Захист телефонів і факсів. Як будь-який електронний пристрій, телефон і факс, а також їх лінії зв'язку випромінюють у відкритий простір високі рівні поля в діапазоні частот до 150 мГц. Щоб повністю пригнітити всі види випромінювань від засобів, є необхідним їх відфільтрувати у виводах мікротелефону, в дротах, що відходять від апарату, а також забезпечити достатнє екранування його внутрішньої схеми. Те й інше можливе лише шляхом значної переробки конструкцій апаратів і зміни їх електричних параметрів. Іншими словами, слід захистити ланцюг мікрофона, ланцюг дзвінка і двохдротяну лінію телефонного зв'язку. Зрозуміло, що здійснити вказані заходи здатні тільки фахівці з використанням відповідного устаткування і стандартних схем. Те ж саме стосується проблеми захисту ліній зв'язку, що виходять за межі приміщень з апаратами.

Це дуже серйозна проблема, оскільки подібні лінії практично завжди безконтрольні і до них можна підключати найрізноманітніші засоби знімання інформації. Тут два шляхи: по-перше, застосовують спеціальні дроти (екранований біфіляр, тріфіляр, коаксіальний кабель, екранований плоский кабель). По-друге, систематично перевіряють спеціальною апаратурою, чи є факт підключення засобів знімання інформації. Виявлення наведених сигналів звичайно відбувається на межі контрольованої зони чи на комутаційних пристроях у кросах або розподільних шафах. Потім або визначають конкретне місце підключення, або (якщо таке визначення неможливе) влаштовують шумовий захист.

Найефективніший спосіб захисту інформації, що передається по телефону, – це застосування ЗАС. За кордоном ці пристрої називають скремблери. Один з кращих апаратів такого роду має габарити: 26,5 х 16 х 5 см, маса 1,3 кг. Споживана потужність не більше 5 Вт. В Україні застосовують ЗАС рівня найвищих міжнародних вимог.

Захист від вбудованих і вузькоспрямованих мікрофонів. Мікрофони, як відомо, перетворюють звук на електричний сигнал. У одності із спеціальними підсилювачами і

фільтрами вони можуть застосовуватися як підслуховуючі пристрої. Для цього створюється прихована дротяна лінія зв'язку, знайти яку можна лише фізичним пошуком або (що складніше) шляхом контрольних вимірювань сигналів у всіх дротах, що є в приміщенні. Методи радіоконтролю, ефективні для пошуку радіозакладок, у цьому випадку неефективні.

Окрім перехоплення звукових коливань, спеціальні мікрофони-стетоскопи дуже добре сприймають звуки, що розповсюджуються у будівельних конструкціях. З їх допомогою здійснюють підслуховування через стіни, двері й вікна. Паренті, існує ряд модифікацій вузькоспрямованих мікрофонів, що сприймають і підсилюють звуки, які йдуть тільки з одного напряму, і ослаблюючи при цьому решту звуків. Такі мікрофони мають вид довгої трубки, батареї трубок або параболічної тарілки з конусом концентратора. Вони уловлюють звуки людського голосу на відстанях до 1 км.

Для захисту від вузькоспрямованих мікрофонів рекомендують заходи:

- всі переговори проводити в кімнатах, ізольованих від сусідніх приміщень, при закритих дверях, вікнах і кватирках, щільно зашутих шторах. Стіни також повинні бути ізольовані від сусідніх будівель;
- підлоги і стелі повинні бути ізольовані від небажаного сусідства у вигляді агентів з мікрофонами й іншою апаратурою прослуховування;
- не ведіть важливих розмов на вулиці, в скверах та інших відкритих місцях, незалежно від того, сидите ви або прогулюєтеся;
- у ресторані, іншому закритому приміщенні поза офісом у разі потреби обміну конфіденційною інформацією різко (тобто несподівано для стежачих) змініть приміщення на те, яке знаходиться під надійним контролем вашої служби безпеки (наприклад, окремий кабінет, замовлений раніше через надійного партнера або помічника);
- пам'ятайте, що спроби заглушати розмову звуками води, що ллється з крана (або з фонтану) малоефективні;
- якщо вам обов'язково потрібно щось повідомити або почути, а гарантій від підслуховування немає, говоріть один одному пошепки прямо у вухо або пишіть повідомлення на листках, що спалюються негайно після прочитання.

Захист від лазерних підслуховуючих пристроїв. Лазери — це такі пристрої, в яких передача і отримання інформації здійснюються в оптичному діапазоні. Такі пристрої малогабаритні і економічні, тим паче, що як приймач нерідко застосовуються фотооб'єктиви, які дають можливість вести перехоплення сигналів з дальніх відстаней.

Принцип дії лазерного пристрою полягає в поєднанні зондуючого променя у напрямі джерела звуку і прийманні цього променя після його віддзеркалення від якихнебудь предметів. Цими предметами, що вібрують під дією навколишніх звуків як своєрідні мембрани, може бути скло вікон, шаф, дзеркала, посуд і т. п. Своїми коливаннями вони модулюють лазерний промінь. Прийнявши його через приймач, можна відновити звуки мови. Поширені нині лазерні пристрої дозволяють вільно підслуховувати людську мову крізь закриті вікна з подвійними рамами на відстанях до 250 метрів.

Найпростішим і в той же час дуже надійним способом захисту від лазерних пристроїв є створення перешкод для модуляції за допомогою п'єзоелемента, який коливає скло з більшою амплітудою, ніж голос людини, тому амплітуда вібрації скла виключає ведення прослуховування.

Пошук радіозакладок. Радіозакладки посідають провідне місце серед засобів промислового, політичного та іншого шпигунства. Вони бувають різних конструкцій — від найпростіших до дуже складних (що мають дистанційне керування, систему накопичення сигналів, систему передачі сигналів у стислому вигляді короткими серіями).

Для підвищення приховування роботи потужність передавача радіозакладки робиться невеликою, але достатньою для перехоплення високочутливим приймачем з невеликої відстані. При цьому, робочу частоту вибирають поблизу несучої частоти потужної радіостанції. Мікрофони роблять як вбудованими, так і виносними. Вони бувають двох типів: акустичними (чутливими до голосів людей) або вібраційними (що перетворюють на електричні сигнали коливання, які виникають від людської мови в різноманітних жорстких конструкціях). Радіозакладки найчастіше працюють на високих частотах (вище 300 кГц).

Проте є і такі пристрої, які працюють в низькочастотному діапазоні (50 – 300 кГц). Як канал зв'язку вони застосовують мережі електроживлення або телефонні лінії. Такі радіозакладки практично не випромінюють сигналів у навколишній простір, тобто мають підвищену прихованість. Якщо їх вмонтувати в настільну лампу, розетку, трійник, будь-який електроприлад, що працюють від мережі змінного струму, то вони, живлячись від мережі, довгий час передаватимуть по ній інформацію в будь-яку точку будівлі і навіть за її межі.

Для виявлення радіозакладок застосовують спеціальні вимірювальні приймачі, автоматично скануючи певний діапазон. За їх допомогою здійснюється пошук і фіксація робочих частот радіозакладок, а також визначається їх місцезнаходження. Дана процедура достатньо складна, вимагає відповідних знань, практичних навиків роботи з різноманітною, вельми складною вимірювальною апаратурою.

Якщо радіозакладки вимкнені у момент пошуку і не випромінюють сигнали, за якими їх можна знайти радіоприймальною апаратурою, то для їх пошуку застосовують спеціальну рентгенівську апаратуру і нелінійні детектори з вбудованими генераторами мікрохвильових коливань низького рівня. Такі коливання проникають крізь стіни, стелі, підлогу, меблі — в будь-яке місце, де захована радіозакладка, мікрофон, магнітофон. Коли мікрохвильовий промінь стикається з транзистором, діодом або мікросхемою, промінь відбивається назад до пристрою. Принцип дії в даному випадку схожий на мінішукач, що реагує на присутність металу.

У разі якщо немає приладів для пошуку радіозакладок або немає часу на пошук, можна користуватися генераторами перешкод для глушіння приймачів. Вони прості, надійні і повністю знімають інформацію з радіозакладок у широкому діапазоні частот.

Захист персональних комп'ютерів. Якщо персональний комп'ютер використовується тільки одним користувачем, то важливо, по-перше, попередити несанкціонований доступ до комп'ютера інших осіб в той час, коли в ньому знаходяться дані, що захищаються, і по-друге, забезпечити захист даних на зовнішніх носіях від розкрадання. Якщо ж ПК використовується групою осіб, то, крім вказаних моментів захисту, може виникнути необхідність запобігти несанкціонованому доступу цих користувачів до даних один одного.

У всіх випадках необхідно захищати дані від руйнування, модифікації тощо в результаті помилок програм і устаткування, зараження комп'ютерними вірусами. Проведення заходів страхування обов'язкове для всіх без виключення користувачів ПК і не відноситься безпосередньо до проблеми захисту даних від конкурентів.

Для безпеки даних застосовують:

- засоби захисту інформаційних і обчислювальних ресурсів шляхом застосування парольної ідентифікації і обмеження несанкціонованого доступу до даних;
- різні шифри, незалежні від контексту інформації.

Нагадаємо, що в ПК як обчислювальні ресурси виступають оперативна пам'ять, процесор, вбудовані накопичувачі на жорстких або гнучких магнітних дисках, клавіа-

тура, дисплей, принтер, інші периферійні пристрої. Захист оперативної пам'яті і процесора передбачає контроль за появою в ній так званих резидентних програм, захист системних даних, очищення залишків секретної інформації. Для цього достатньо мати в своєму розпорядженні програму проглядання оперативної пам'яті для контролю за складом резидентних програм і їх розташуванням.

Набагато важливіший захист вбудованих накопичувачів. Існують декілька типів програмних засобів, здатних вирішувати цю задачу:

- захист диска від запису і читання;
- контроль за зверненнями до диска;
- засоби знищення залишків даних.

Але найнадійніший метод захисту, безумовно, шифрування, оскільки в цьому випадку захищається безпосередньо самі дані, а не доступ до них (наприклад, зашифрований файл не можна прочитати навіть у разі крадіжки дискети). У ряді випадків застосування шифрування скрутне або є малоефективним, тому рекомендується застосовувати усі методи в їх єдності.

Більшість засобів захисту реалізуються завдяки програмам, що розширюють можливості стандартних операційних систем, а також систем управління базами даних.

4.3.5.3. Програмно-технологічний захист даних

Програмно-технічний захист даних – це діяльність, спрямована на забезпечення інженерно-технічними та програмними заходами конфіденційності, цілісності та непорушності даних.

Існує кілька основних можливостей пошкоджень даних, що обробляються на комп'ютері, а саме: ураження комп'ютера різноманітними вірусними програмами, несанкціонований доступ до даних у локальній мережі та при роботі в Інтернеті, так звані програми-шпигуни тощо [198, с. 115-132].

Інженерно-технічний захист. Концепцією технічного захисту інформації в Україні, затвердженою постановою Кабінету Міністрів України від 8 жовтня 1997 р. № 1126, визначено, що технічний захист інформації є складовою частиною системи національної безпеки України. У концепції, зокрема, зазначається, що прогрес у різних галузях науки і техніки призвів до створення компактних й високоефективних технічних засобів, за допомогою яких можна легко підключатись до ліній телекомунікацій та різноманітних технічних засобів оброблення інформації вітчизняного та іноземного виробництва з метою здобуття, перехоплення та аналізу розвідувальних даних. Для цього може застосовуватись апаратура радіо-, радіотехнічної, оптико-електронної, радіотеплової, акустичної, магнітометричної, сейсмічної, хімічної та радіаційної розвідок.

За таких умов створилися можливості витоку інформації, порушення її цілісності та блокування. Витік інформації, яка становить державну та іншу передбачувану законом таємницю, конфіденційної інформації, що є власністю держави, – це одна з основних можливих загроз національній безпеці України в інформаційній сфері. Відповідно до Концепції технічного захисту інформації в Україні система технічного захисту інформації – це сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними та нормативно-правовими заходами.

Указом Президента України від 27 вересня 1999 р. № 1229/99 затверджено Положення про технічний захист інформації в Україні. Положенням визначено правові та організаційні засади технічного захисту інформації – діяльності, спрямованої на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації, охорона якої забезпечується державою відповідно до законодавства.

Основні організаційно-технічні положення технічного захисту інформації викладено у Державному стандарті України "Захист інформації. Технічний захист інформації" у розділах "Технічний захист інформації. Основні положення" – ДСТУ 33960-96, "Захист інформації. Технічний захист інформації. Порядок проведення робіт" – ДСТУ 33961-96, "Захист інформації. Технічний захист інформації. Терміни та визначення – ДСТУ 33962-97", які набрали чинності з 01.01.1997 р. Загальні вимоги щодо підтримки інформаційної безпеки в установах та організаціях визначені міжнародним стандартом ISO/IEC 17799 "Управління інформаційною безпекою – практичні правила".

Органом державного управління, що реалізовує державну політику у сфері захисту державних інформаційних ресурсів у мережах передачі даних, криптографічного та технічного захисту інформації, забезпечує функціонування державної системи урядового зв'язку, є Державна служба спеціального зв'язку та захисту інформації в Україні (далі – Служба) [42].

Служба відповідно до покладених на неї завдань визначає порядок та вимоги щодо захисту інформації, необхідність охорони якої визначено законодавством, забезпечує функціонування, безпеку, розвиток і вдосконалення державної системи урядового зв'язку, встановлює порядок і вимоги щодо застосування мереж передачі даних, видає відповідно до законодавства ліцензії на право провадження окремих видів господарської діяльності у сфері криптографічного та технічного захисту інформації тощо.

Службою розроблено низку нормативних документів у галузі захисту інформації, зокрема НДТЗІ 1.1-001-99 "Технічний захист інформації на програмно-керованих АТС загального користування", НДТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу", НД ТЗІ 3.7-001-99 "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі", НДТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі", НДТЗІ 3.6-001-2000 "Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу", НДТЗІ 2.1-001-2001 "Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення", НДТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" та інші, де містяться вимоги щодо технічного захисту інформації.

Для протидії витоку інформації технічними каналами має створюватися комплексна система захисту, яка передбачає застосування фізичних, апаратних, програмних, криптографічних засобів захисту. Розглянемо докладніше її основні складові.

Міжнародний стандарт ISO/IEC 17799 передбачає створення фізичної безпеки інформаційних ресурсів. Вимоги щодо фізичної безпеки можуть мати значні відмінності залежно від масштабу організації та структури інформаційних сервісів, а також від існуючих загроз. Фізична безпека досягається формуванням її периметрів, які розташовані у стратегічних місцях. Вимоги щодо цих бар'єрів визначаються залежно від цінності ресурсів. На периметрах встановлюються різноманітні фізичні засоби захисту.

Фізичні засоби захисту – це різноманітні пристрої, конструкції, обладнання, призначені для створення перешкод на шляху руху зловмисників. До них належать механічні, електромеханічні, електронні, електронно-оптичні, радіо- і радіотехнічні й інші пристрої для перешкоди несанкціонованому доступу (входу, виходу), проносінню (винесенню) засобів та матеріалів і інших можливих видів протиправних дій.

До засобів фізичного захисту належать різні види огороджень. Практика свідчить, що огородження складної конфігурації здатні затримати зловмисника на досить тривалий термін. Особливі конструкції периметрів, проходів, віконних грат, приміщень, сейфів, сховищ є обов'язковими з погляду безпеки для будь-яких організацій і підприємств. Ці конструкції повинні протистояти будь-яким способам фізичного впливу з боку зловмисників: механічним деформаціям, руйнуванню свердлінням, термічному і механічному різанню, вибухові і т. ін.; несанкціонованому доступу шляхом підробки ключів, вгадування коду тощо. Одним із головних технічних засобів захисту приміщень, сейфів і сховищ є замки. Вони бувають механічними (із ключами), кодовими (у тому числі і з тимчасовою затримкою на відкривання) та з електронно-програмними пристроями, що відкривають двері і сейфи тільки у визначений час.

Фізичні засоби захисту застосовуються для вирішення таких завдань:

- охорона території і спостереження за нею;
- охорона будинків, внутрішніх приміщень і контроль за ними;
- охорона устаткування, продукції та інформації;
- здійснення контрольованого доступу до будинків і приміщень.

За функціональними призначеннями засоби цієї категорії можна поділити на такі групи:

- охоронні й охоронно-пожежні системи;
- охоронне телебачення;
- охоронне освітлення.

Розглянемо докладніше окремі групи цих засобів.

Охоронні системи. Охоронні системи і засоби охоронної сигналізації призначені для виявлення різних видів загроз: спроб проникнення на об'єкт захисту (наприклад, приміщення), спроб проносення (винесення) зброї, засобів промислового шпигунства, крадіжок матеріальних і фінансових цінностей та інших дій; оповіщення співробітників охорони або персоналу об'єкта про появу загроз і необхідність посилення контролю доступу на об'єкт, територію, до будинків і приміщень.

Найважливішими елементами охоронних систем є датчики, що виявляють загрози. Специфіка роботи датчиків визначається основними параметрами і практичними можливостями охоронних систем.

Датчики за допомогою тих чи інших каналів зв'язку з'єднані з контрольно-приймальним пристроєм пункту охорони і засобами тривожного оповіщення.

Каналами зв'язку в системах охоронної сигналізації можуть бути спеціально прокладені провідні або кабельні лінії, телефонні лінії об'єкта, лінії зв'язку трансляції, системи освітлення або радіоканали. Вибір каналів визначається можливостями об'єкта.

Важливим об'єктом охоронної системи є засоби тривожного оповіщення: дзвінки, лампочки, сирени, що подають сигнали про появу загрози.

За тактичним призначенням охоронні системи поділяються на такі системи охорони:

- периметрів об'єктів;
- приміщень і проходів у службових та складських будинках;
- сейфів, устаткування, основних і допоміжних технічних засобів;
- автотранспорту;
- персоналу, у тому числі й особового складу охорони.

Якщо охоронна система повідомляє про те, що відбулося певне порушення охоронної зони, то *системи відеонагляду* дають можливість з'ясувати, що саме сталося, та ідентифікувати зловмисника. Перевагою відеонагляду є можливість фіксувати порушення режиму охорони об'єкта і контролювати обстановку навколо нього та динаміку її розвитку, визначати небезпеку дій, здійснювати приховане спостереження, робити відеозапис для подальшого аналізу правопорушення як з метою аналізу, так і для залучення порушника до відповідальності.

Джерелами зображення (датчиками) у відеосистемах є відеокамери. Через об'єктив зображення зловмисника потрапляє на світлочутливий елемент камери, у якому воно перетворюється на електричний сигнал, що надходить спеціальним коаксіальним кабелем на монітор і за потреби – на відеомагнітофон. Відеокамера є найважливішим елементом системи, тому що від її параметрів залежить ефективність і результативність усієї системи контролю та спостереження. Сьогодні розроблені й випускаються найрізноманітніші моделі, що відрізняються як за габаритами, так і за можливостями та конструктивним виконанням.

Обов'язковою частиною системи захисту кожного об'єкта є охоронне освітлення. Розрізняють два види охоронного освітлення: чергове і тривожне.

Чергове освітлення застосовується у неробочий, вечірній чи нічний часи, як на території об'єкта, так і усередині будинку.

Тривожне освітлення вмикається при надходженні сигналу тривоги від засобу охоронної сигналізації. За сигналом тривоги можуть вмикатися і звукові прилади (дзвінки, сирени тощо).

Сигналізація і чергове освітлення повинні мати резервне електроживлення на випадок аварії або вимикання електроструму.

Для збереження ПК та іншої техніки випускаються спеціальні металеві шафи. Такі шафи забезпечуються надійною подвійною системою замикання: замком ключового типу і три – п'ятизначним комбінованим замком. Такі шафи відзначаються міцністю і надійністю, достатньою для захисту від промислового шпигунства.

Системи контролю доступу. Регулювання доступу в приміщення або будинки здійснюється насамперед за допомогою розпізнавання службою охорони або технічними засобами.

Контрольований доступ передбачає обмеження кола осіб, які допускаються у певні захищені зони, будинки, приміщення, і контроль за перебуванням цих осіб усередині них. Підставою допуску є певний метод особистого розпізнавання і порівняння особистих, персональних даних з дозвільними параметрами, які закладені у систему.

Є широкий спектр методів розпізнавання уповноважених осіб на право їх доступу у зони охорони, будинки, приміщення. На цій основі ухвалюються рішення про допуск осіб, які мають на це право, або заборону – для тих, хто не має його. Найбільшого поширення набули атрибутні і персональні методи розпізнавання. У основі кожного з них персональні дані, які стосуються відповідного суб'єкта даних. Згідно з Конвенцією РС № 108 –"персональні дані означають будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною" [56], тобто ідентифікованою завдяки її персональним даним.

До атрибутних належать такі засоби підтвердження (розпізнавання) особи, як документи (паспорт, посвідчення тощо), картки (фотокартки, карти з магнітними, електричними, механічними ідентифікаторами тощо) та інші засоби (ключі, сигнальні елементи тощо). Ці засоби найбільше підробляються зловмисниками.

Персональні методи – це методи визначення (розпізнавання) особи за її незалежними особистими показниками: відбитками пальців, геометрією рук, особливостями очей тощо.

Персональні дані визначаються ознаками, які бувають статичні і динамічні. До останніх належать пульс, тиск, кардіограма, мова, почерк тощо.

Персональні методи найприйнятніші. По-перше, вони повно ідентифікують окрему людину. По-друге, неможливо або вкрай важко підробити індивідуальні біологічні ознаки.

Звичайний спосіб впізнання людиною (вахтер, вартовий) не завжди надійний через так званий "людський фактор", який полягає в тому, що людина піддається впливові багатьох зовнішніх умов (втома, погане самопочуття, емоційний стрес, підкуп тощо).

Способи впізнання, що ґрунтуються на занам'ятовуванні коду, паролю тощо, можуть застосовуватися у випадках найнижчих вимог до безпеки, тому що часто інформацію записують користувачі на різних папірцях, у записниках та інших носіях, що при їх доступності іншим може звести нанівець усі зусилля з безпеки. Крім того, є реальна можливість підглянути, підслухати або одержати цю інформацію іншим шляхом (насильство, крадіжка тощо).

Тому широкого застосування набувають такі технічні засоби впізнання, як ідентифікаційні картки, впізнання за голосом, почерком тощо. Найпростіший і найбільш поширений метод ідентифікації – застосування різних карток, на яких міститься кодована або відкрита інформація про власника, його повноваження тощо.

Системи впізнання за голосом. Існують кілька способів виділення ознак мови людини і аналіз короткочасних сегментів, контрольний аналіз, виділення статистичних показників. Слід зазначити, що теоретично питання ідентифікації по голосу розроблені досить повно, але відповідні пристрої застосовують на рівні експериментальних зразків.

Системи впізнання за почерком вважаються найзручнішими для користувача. Основним принципом ідентифікації за почерком є сталість підпису кожного індивідуума, хоча цілковитого збігу не буває.

Система впізнання за геометрією рук. Для ідентифікації застосовують аналіз комбінації ліній згинів пальців і долоні, ліній складок, довжини і товщини пальців тощо. Технічно це реалізується шляхом накладення руки на матрицю.

Усі пристрої ідентифікації людини можуть працювати як окремо, так і в комплексі. Комплекс може бути вузькоспеціальним або багатоцільовим, за якого система виконує функції охорони, контролю, реєстрації і сигналізації. Такі системи називають комплексними. Комплексні системи забезпечують допуск на територію підприємства за карткою (перепусткою), з індивідуальним машинним кодом, блокування проходу при спробах несанкціонованого проходженням (проходження без перепустки, без допуску).

Комплексні системи забезпечують:

- допуск на територію за карткою, яка містить індивідуальний машинний код;
- можливість блокування проходу для порушників графіка роботи (запізнення, передчасний вихід тощо);
- відкриття зони проходу для вільного виходу за командою вахтера, перевірку кодів пропусків на затримку їх пред'явників за вказівкою оператора системи;
- реєстрацію часу перетинання прохідної і збереження його в базі даних НК;
- обробку отриманих даних і формування різних документів (табель робочого часу, добовий рапорт, відомість порушників трудової дисципліни тощо), що дає можливість мати оперативну інформацію про порушників трудової дисципліни, відпрацьований час;
- локалізація металевих та інших предметів, які мають загрозу для життя людей тощо.

З розвитком інформаційних технологій основною загрозою для інформації з обмеженим доступом стала проблема *несанкціонованого доступу*. Це визначається у несанкціонованому перехопленні даних технічними каналами, насамперед інформаційно-комунікаційних систем, що не мають виходу за межі контрольованої території. У цьому разі для зловмисників немає альтернативи, крім застосування розвідапаратури для перехоплення інформації технічними каналами витоку. Реально це можна забезпечити тільки в разі виявлення можливих загроз інформації, включаючи канали її витоку. Реалізація такого підходу потребує об'єднання різних підсистем безпеки в єдиний комплекс, оснащений загальними технічними засобами: зв'язку, програмним забезпеченням і базами даних.

Апаратний захист даних. До апаратних засобів захисту інформації належать різні за принципом дії і можливостями технічні конструкції, що забезпечують припинення розголошення, захист від витоку і протидію несанкціонованому доступові до джерел конфіденційної інформації.

Апаратні засоби захисту застосовуються для вирішення таких завдань:

- проведення спеціальних досліджень технічних засобів забезпечення виробничої діяльності на наявність можливих каналів витоку інформації;
- виявлення каналів витоку інформації на різних об'єктах і в приміщеннях;
- локалізації каналів витоку інформації;
- пошук і виявлення засобів промислового шпигунства;
- протидія несанкціонованому доступові до джерел конфіденційної інформації тощо.

Перед застосуванням апаратного захисту інформації слід проаналізувати ризики щодо її втрати та витоку, а також сам об'єкт захисту на предмет наявності технічних каналів витоку інформації. На основі цих даних формуються вимоги щодо системи захисту та здійснюється попередня оцінка співвідношення збитків від втрати інформації та вартості необхідної апаратури для її захисту.

За функціональним призначенням апаратні засоби можуть бути класифіковані на засоби виявлення (для радіопередавачів, диктофонів, інших несанкціонованих пристроїв), засоби пошуку і докладних вимірів (для виміру радіочастот), засоби активної і пасивної протидії (віброакустичні для захисту від лазерних мікрофонів, електромагнітні, акустоелектричні тощо).

При цьому за своїми технічними можливостями засоби захисту інформації можуть бути загального призначення, розраховані на застосування непрофесіоналами з метою одержання попередніх (загальних) оцінок і професійні комплекси, що дають можливість здійснювати пошук, виявлення і виміри всіх параметрів засобів промислового шпигунства. Як приклад перших можна розглянути групу індикаторів електромагнітних випромінювань, що мають широкий спектр прийнятих сигналів і досить низьку чутливість. Як другий приклад – комплекс для виявлення і пеленгування радіозакладок, призначений для автоматичного виявлення і визначення місця розташування радіопередавачів, радіомікрофонів, телефонних закладок і мережних радіопередавачів. Це вже складний сучасний професійний пошуковий комплекс.

Пошукову апаратуру можна розділити на апаратуру пошуку засобів знімання інформації і дослідження каналів її витоку.

Апаратура першого типу спрямована на пошук і локалізацію уже впроваджених зловмисниками засобів несанкціонованого доступу.

Апаратура другого типу призначається для виявлення каналів витоку інформації. Визначальними для такого роду систем є оперативність дослідження і надійність отриманих результатів. Застосування пошукової апаратури потребує високої кваліфікації.

Особливості захисту даних у комп'ютерних системах. У зв'язку з широким застосуванням для обробки даних засобів електронно-обчислювальної техніки сьогодні

особливо гострою стала проблема захисту інформації, автоматизованої обробки даних, їх передачі, яка була б адекватною існуючим загрозам. Для комп'ютерних систем і мереж існують специфічні види загроз. Передусім це пов'язано з тим, що електронно-обчислювальна техніка здатна працювати тільки за наявності електричного живлення. Іншою загрозою, притаманною для будь-яких технічних пристроїв, є вірогідність виходу з ладу через непередбачувані обставини (стихійне лихо, пожежа) або ж у результаті порушення правил користування ними. До окремої групи загроз слід віднести кіберзлочини.

Загрози, які призводять до знищення або доступності інформації, спричиняють значні фінансові збитки. Так, за даними Information Week, середня вартість простої інформаційної системи у фінансовій галузі становить 2,6 – 8,45 млн. дол. США. 43 % компаній, що втратили свої корпоративні дані, не змогли відновити свій бізнес, а 29 % припинили свою діяльність упродовж 2 років. Загальні вимоги щодо захисту інформації, умов обробки інформації, організації захисту інформації в автоматизованих системах викладено в Законі України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31.05.2005 р. № 2594-IV [36].

Стандарт ISO/IEC 17799 рекомендує розміщувати комп'ютерне обладнання таким чином, щоб зменшити ризик, пов'язаний з впливом зовнішнього середовища та несанкціонованим доступом. При цьому для ідентифікації можливих загроз рекомендується застосовувати такий контрольний список: пожежа; задимлення; затоплення; запилення; вібрація; вплив хімічних речовин; перешкоди в електроживленні; електромагнітна радіація.

Крім зазначених загроз, особливо слід відзначити так звану "комп'ютерну злочинність", або кіберзлочинність. Під цим соціальним явищем слід розуміти протиправне використання засобів обчислювальної техніки для вчинення злочинів, у тому числі тих, предметом яких є комп'ютерна інформація.

На конференції країн "Великої вісімки" щодо проблем кіберзлочинності, яка проходила у жовтні 2000 р., міністр закордонних справ Німеччини Йошка Фішер відзначив, що збитки від кіберзлочинів сягають 100 мільярдів німецьких марок щороку. А за оцінками Рахункової палати уряду США, щорічний збиток від розкрадань і шахрайств, вчинених за допомогою інформаційних технологій тільки через Інтернет, сягає 5 млрд. дол. США [198, с. 161-169].

У грудні 2002 р. в Лондоні відбувся Перший міжнародний стратегічний конгрес "E-CRIME CONGRESS 2002", присвячений проблемі електронної злочинності. У роботі Конгресу "E-CRIME" взяли участь близько 400 делегатів з усього світу, у тому числі з Австралії, Нової Зеландії, Кореї, Гонконгу, Росії, Латвії, США та ін. Вони представляли державні, комерційні, наукові та правоохоронні органи, що вирішують проблеми захисту інформації та здійснюють розслідування комп'ютерних злочинів. Своїх делегатів представляли Міністерство внутрішніх справ Великобританії, Інтерпол, Європол, ФБР, Управління "Р" (Росія), Microsoft, Symantec, IBM, Sun Microsystems Ltd., VISA, MasterCard, eBay, Bank of New York, Swedbank та ін.

На конгресі відзначалося, що високотехнологічна злочинність зростає швидкими темпами. Інтернет дає можливість організованим злочинним групам швидко отримувати прибуток з відносно невеликим ризиком бути упійманими. Знаходячись у мережі, можна порушувати закон на відстані, швидко і незалежно від громадянства та місця перебування. Злочинцям легко оплутувати людей, приховувати докази. Вони є значною загрозою для інфраструктури розвинутих держав. Так, за повідомленням інформаційного агентства Washington ProFile з посиланням на газету The Washington Times, терорист Усама Бен Ладен одержав у своє розпорядження комп'ютерну програму Promis (виробник – компанія Inslaw Inc.), що дає йому можливість проникати в урядові інформаційні мережі США.

Програми, створені на базі розробок Inslaw Inc., застосовуються, зокрема, ФБР і ЦРУ. Якщо Бен Ладен справді володіє Promis, то він може стежити за діями американських спецслужб, одержувати секретну інформацію про стратегічні об'єкти США, а також без проблем відмивати "брудні" гроші. Крім того, не виключено, що це програмне забезпечення використовувалося Аль Каїдою для підготовки терористичних атак на Нью-Йорк і Вашингтон, проведених 11 вересня 2001 р.

У доповіді віце-президент групи страхових компаній В. Барр виклав такі факти:

- 90 % організацій виявляють порушення інформаційних систем щороку;
- 80 % з них підтверджують фінансові збитки;
- тільки один вірус NIMDA спричинив збитків на суму понад 1,8 млрд. фунтів;
- у жовтні 2002 р. кібератака протягом 1 години вивела з ладу 9 з 13 головних комп'ютерів, які керують глобальним рухом у мережі Інтернет;
- щороку викрадається приватної інформації на суму понад 38 млрд. фунтів.

Притаманні наступні риси злочинності в галузі інформаційних технологій:

- міжнародний зміст злочину;
- труднощі у визначені "місцеперебування" злочинця;
- слабкі зв'язки між ланками в системі доказів;
- неможливість спостерігати і фіксувати докази візуально;
- широке використання злочинцями засобів шифрування інформації.

Громадськість дедалі більше цікавиться кіберзлочинністю, оскільки кожний власник або користувач комп'ютера, телефону, радіотелефону, модему, пластикової картки – це потенційний потерпілий, якого можуть очікувати тяжкі наслідки в разі вчинення злочину, особливо в державному, комерційному та промисловому секторі, де можливі великі фінансові збитки. Комп'ютерні злочинці за допомогою Інтернету поширюють свій кримінальний досвід попри національні кордони, що потребує відповідних кроків координації з боку правоохоронних установ, які протидіють цим злочинам.

Відповідно до рекомендацій Комітету з питань законодавства Ради Європи від 1990 р. нижче подано прийняту *Міжнародну класифікацію кодів комп'ютерних злочинів* [198, с. 163], яка передбачає:

QA - втручання або перехоплення;
QAH - незаконний доступ;
QAI - перехоплення;
QAT - викрадення часу;
QAZ - інші випадки несанкціонованого доступу або перехоплення;
QD - зміна або пошкодження інформації;
QDT - "Троянські коні";
QDW - "Черв'яки";
QDL - "Логічна бомба";
QDV - програми-віруси;
QDZ - інші випадки пошкодження інформації;
QF - комп'ютерне шахрайство;
QFC - шахрайство з автоматами з видачі готівки;
QFF - комп'ютерна підробка;
QFG - шахрайство з ігровими автоматами;

QFM - шахрайство шляхом неправильного вводу/виводу або маніпуляції програмами;

QFP - шахрайство з платіжними засобами;

QFT - телефонне шахрайство;

QFZ - інші випадки комп'ютерного шахрайства;

QR - несанкціоноване копіювання;

QRG - несанкціоноване тиражування комп'ютерних ігор;

QRS - несанкціоноване тиражування програмного забезпечення;

QRT - несанкціоноване тиражування напівпровідникової продукції;

QRZ - інші випадки несанкціонованого копіювання;

QS - комп'ютерний саботаж;

QSH - саботаж технічного забезпечення;

QSS - саботаж програмного забезпечення;

QSZ - інші види комп'ютерного саботажу;

QZ - злочини, пов'язані з комп'ютерами;

QZB - незаконне використання дошки електронних оголошень;

QZE - викрадення комерційної таємниці;

QZS - зберігання або розповсюдження матеріалів, які є об'єктом судового переслідування;

QZZ - інші випадки вчинення злочинів, пов'язаних з комп'ютерами.

Перелік (список) правопорушень становлять:

1. Несанкціонована заміна даних або комп'ютерних програм.

2. Комп'ютерне пограбування – придбання протиправними засобами або відкриття, переміщення чи використання торгової, комерційної, промислової таємниці без дозволу або інших законних підстав з метою завдання економічної шкоди особою, яка допущена до таємниці, або одержання протизаконної економічної переваги для себе чи для інших осіб.

3. Протиправне використання комп'ютера – використання комп'ютерних систем або мереж без дозволу користувача, що вчинене:

• з ризиком завдання збитків особі, якій надане право користуватися системою, або завдання шкоди самій системі чи її роботі;

• з метою завдання збитків особі, якій надане право користування, або завдання шкоди самій системі чи її роботі;

• для заподіяння збитків особі, якій надане право користуватися системою, або самій системі.

4. Несанкціоноване використання захищених комп'ютерних програм – використання без дозволу комп'ютерних програм, які захищені законом і були скопійовані без дозволу з метою отримання протизаконного економічного прибутку для себе та інших осіб, або завдання шкоди власникові програм.

Найперше, на що потрібно зважати при налагодженні комп'ютерної інформаційної системи, – це на якісну систему електроживлення. Крім заземлення, яке надійно захистить ваші дані від статичних розрядів, рекомендується передбачити аварійну систему електроживлення. Необхідним компонентом роботи серверів є блок безперебійного живлення (UPS). Сьогодні існує достатня кількість модифікацій UPS для комп'ютерів найрізноманітнішої потужності та часу роботи без основного електроживлення від декількох хвилин до доби і більше. Для окремих інформаційних систем передбачається застосування портативних електростанцій різноманітних потужностей. Для захисту комутаційного обладнання (модеми, мережні карти) від імпульсних перевантажень, які утворюються внаслідок завад, грозових розрядів тощо, застосовують імпульсні фільтри.

Важливо також звернути увагу на мережу електроживлення та кабелі передачі даних. Кабелі електроживлення і лінії зв'язку, що йдуть до інформаційних систем, повинні бути проведені під землею (за можливістю) або захищені належним чином за допомогою інших засобів.

Необхідно розглянути заходи для захисту мережних кабелів від їх несанкціонованого розкриття для цілей перехоплення даних і від ушкодження, наприклад, скориставшись екранами або прокладши ці лінії так, щоб вони не проходили через загальнодоступні місця.

Як уже зазначалося, технічні пристрої мають властивість виходити з ладу (хоча відомі випадки безперервної роботи комп'ютерів упродовж більш як десяти років). Тому необхідно у відповідні терміни, які рекомендує виробник обладнання, здійснювати технічне обслуговування. При цьому ремонт та регламентні роботи слід доручати тільки спеціальному персоналу. Усі несправності потрібно реєструвати у спеціальному журналі.

Обов'язковою процедурою захисту від втрати інформації є її регулярне *копіювання*. Копіювання можна здійснювати на дискети, вінчестери, стримери тощо. При цьому широко застосовуються такі програми для архівації даних, як WinZip, WinRar, Arj тощо, які у свою чергу мають можливість захищати створені архіви за допомогою паролів. Останнім часом набуває широкого поширення запис даних на лазерні накопичувачі та магнітооптику. Резервні копії повинні зніматися регулярно. Необхідно мати копії як даних, так і програмних засобів. Копії слід зберігати на значній відстані від основного робочого місця з метою уникнення втрат від аварій та катастроф. Вони також мають бути відповідним чином надійно захищені фізичними засобами, адже в них міститься вся виробнича інформація. Резервні дані необхідно регулярно тестувати, аби бути впевненим, що їх можна буде використати в разі аварії.

У комп'ютерних системах з підвищеною надійністю застосовуються такі технології:

• створення RAID-масивів (особливий спосіб зберігання інформації на декількох магнітних носіях з можливістю її відновлення в разі виходу з ладу одного з носіїв);

• дублювання інформації (дзеркальний сервер);

• автоматичне пересилання інформації в систему, розташовану в іншому географічному місці (на випадок катастроф чи викрадення носіїв інформації).

До категорій засобів підвищення надійності комп'ютерних інформаційних систем слід віднести різноманітні програмні та апаратні пристрої, які забезпечують відновлення інформації. Відновлення необхідно проводити, якщо певна інформація була помилково знищена або знищення відбулося внаслідок дії комп'ютерного вірусу. Відновлення можливе за допомогою загальновідомих програм, таких як Undelete, UnErase Wizard, Restorer 2000. Існують також схожі програми вітчизняного виробництва.

До апаратних засобів забезпечення захисту комп'ютерної інформації відносяться згадувані раніше системи сигналізації (аналогічні до тих, що застосовуються для охорони автомобілів), різноманітне обладнання для протидії викрадення самого комп'ютера (це найпростіший спосіб отримання відразу усієї інформації, хоча досить часто крадіжки відбуваються лише з метою використання апаратних засобів), використання ключів для блокування роботи клавіатури, розкриття корпусу системного блоку, замикання дискет з копіями файлів тощо. Останнім часом застосовуються апаратні засоби управління доступу до комп'ютера. Це може бути пластикова картка або інші пристрої, які виконують аутентифікацію користувача для роботи з комп'ютером або, наприклад, тільки з певним логічним диском вінчестера.

В установах для захисту даних слід створювати відповідний підрозділ згідно з "Типовим положенням про службу захисту інформації в автоматизованій системі" НД ТЗІ 1.4-001-2000, а також корисно сформувати групу реагування. До такої групи слід включити таких осіб: керівник; системний адміністратор чи системний програміст; аудитор; спеціаліст.

Керівник очолює команду управління і вирішує, яким чином реагувати на ситуацію. Він отримує доступ до даних, що стосуються як важливості розкритої інформації, так і потенційного збитку, завданого організації в результаті її втрати, несе відповідальність за документування всіх подій, що відбулися.

Системний оператор (системний адміністратор чи системний програміст) повинен найкраще знати всі обхідні шляхи в системі. Якщо злочин ще відбувається, він намагається вистежити злочинця в лабіринті подій системних зв'язків і контролювати всю роботу системи. Якщо ж злочин уже вчинено, системний оператор повинний спробувати реконструювати події. Незалежно від того, буде досягнуто успіху чи ні, він несе відповідальність за документування всього, що трапилось.

Аудитор виконує дві основні функції. По-перше, він допомагає системному оператору йти слідами злочину. Маючи досвід роботи з контрольними та іншими журналами системи, він може застосовувати ці інструменти, щоб отримати додаткові відомості про злочин і злочинця. По-друге, аудитор несе відповідальність за визначення економічного збитку від даного інциденту. Це важливо знати для правового обґрунтування. Нам'ятайте, що такі збитки обчислюються більшими сумами, ніж просто матеріальний збиток, завданий устаткуванню чи програмному забезпеченню. Аудитору необхідно визначити вартість інформації, що була викрадена, загублена чи пошкоджена, витрати робочого часу, втраченого системою, і часу, необхідного для оцінки збитків та обсягу ремонтних робіт.

У більшості невеликих підприємств, дослідницьких лабораторій, навчальних закладів аудиторські функції виконує керівник чи системний оператор; спеціаліст знає як комп'ютерну техніку, так і прикладне програмне забезпечення. Нажаль, для багатьох слідчих розслідування комп'ютерного злочину є маловідомим. Для них може бути зовсім не очевидним, що вимикання комп'ютера може призвести до втрати всіх доказів, а диски і стрічки можуть бути ушкоджені просто в результаті впливу тепла чи холоду і злочинця можна знайти, перехопивши його перетворювання каналом зв'язку. У цьому разі потрібен спеціаліст, що несе відповідальність за збирання доказів і їх зберігання, дає рекомендації, чи можна виключати, переміщати і транспортувати устаткування. Спеціаліст тісно взаємодіє із системним оператором при перевірці системних журналів та інших дій системи, що можуть допомогти розібратися в злочині і вивести на підозрюваного.

Існують такі *методи захисту даних* у комп'ютерних системах:

- обмеження доступу;
- розмежування доступу;
- криптографічне перетворення даних;
- контроль і облік доступу.

Останнім часом у зв'язку зі збільшенням обсягів, кількості користувачів, видів випадкових впливів збільшується імовірність несанкціонованого доступу до інформації. Тому розвиваються старі і виникають нові додаткові методи щодо захисту, тобто:

- функціонального контролю, що забезпечують діагностику і визначення збоїв апаратури, помилок людини, програмних помилок;
- підвищення вірогідності інформації;
- захисту інформації від аварійних ситуацій;

- контролю доступу до внутрішнього монтажу апаратури, ліній зв'язку і технічних органів керування;
- аутентифікації користувачів, технічних засобів, носіїв інформації, документів;
- захисту від побічного випромінювання і завад.

До фізичних способів захисту інформації належать:

Обмеження доступу. Цей метод полягає у створенні певної фізичної перешкоди навколо об'єкта захисту з організацією контрольованого доступу осіб, пов'язаних з об'єктом захисту за своїми функціональними обов'язками. Слід звернути також увагу на фізичний захист носіїв комп'ютерної інформації (магнітні диски, дискети, системна документація тощо). За дослідженням NHTCU, у 2002 р. у Великобританії в 71 % організацій було викрадено комп'ютерне обладнання, а в 76 % – портативні комп'ютери.

При зберіганні даних забороняється використовувати позначки на носіях інформації, за якими можна з'ясувати їх зміст. Зміст носіїв інформації повинен бути декілька разів знищений, якщо вони передаються за межі організації. Особливу увагу слід звертати на питання ремонту носіїв інформації, якщо це неможливо зробити в самій установі.

Для безпечної роботи з с-документами слід звертати увагу не тільки на роботу з ними, а й на їх знищення – адже відповідна інформація навіть після очищення "корзини" залишається на магнітному диску. Для знищення носіїв інформації також слід передбачити певну процедуру. Для цього потрібно застосовувати спеціальні пристрої (наприклад, для паперових носіїв – засоби подрібнення). Для "справжнього" видалення файлів використовують спеціальні програми, які можуть перезаписувати інформацію зверху знищеної.

Останніми роками дедалі частіше застосовуються комплекси для миттєвого знищення інформації, які в разі появи загрози витоку або крадіжки інформації на магнітних носіях миттєво її ліквідують. Слід також пам'ятати про ефект акумуляції, який призводить до того, що велика кількість несекретної інформації може стати більш конфіденційною, аніж невелика кількість секретної інформації.

Вірогідність втрати інформації різко зростає в разі транспортування носіїв. Тому слід особливо зважати на вибір кур'єра та транспорт, використання спеціальних контейнерів закритого типу. В окремих випадках доцільно передавати інформацію різними маршрутами з поділом її на окремі частини.

Захист робочої станції конкретного працівника розпочинається із захисту обладнання від несанкціонованого доступу. До найпростіших засобів належить блокуюча функція Keylock – невеликий замок на передній панелі комп'ютера. Проте це слабкий захист, який зловмисник може легко подолати. Наступним кроком захисту є BIOS-пароль, який необхідно ввести ще до завантаження операційної системи. Цей пароль користувач уводить у Setup комп'ютера у підсистемі Security (вхід у Setup здійснюється натисканням клавіші Esc або іншою, яка висвічується на моніторі при ввімкненні електроживлення). Для пароля передбачено два рівні – User та Supervisor. Перший рівень використовують для завантаження операційної системи, а інший – для входу в Setup. Цей бар'єр є нездоланним для звичайного користувача системи, проте не є таким для електронника середньої кваліфікації.

У повсякденній роботі користувачів обов'язковим елементом захисту повинен стати Screensaver-пароль, який легко встановлюється натисканням правої кнопки "миші" на полі робочого столу з подальшим вибором опції "Заставка". Залежно від інтенсивності роботи виставляється проміжок часу, після якого з'являється заставка на моніторі, зняти яку можна лише, увівши пароль.

Для мінімізації ризику пошкодження комп'ютерних програм слід здійснювати суворий контроль за доступом до текстів програм. Передусім вони повинні перебувати не в

робочих системах. Усі випадки доступу до бібліотек текстів програм слід фіксувати. Поновлення прикладних програм повинні здійснювати відповідальні особи за санкцією керівника.

Контроль доступу до апаратури. Доступ до комп'ютерних систем та даних контролюється виходячи з виробничої потреби. Виробничі вимоги слід чітко визначити та задокументувати. Для управління правом доступу до інформаційних систем необхідні формальні процедури, починаючи від початкової реєстрації нових користувачів та надання їм певних повноважень і закінчуючи видаленням записів для користувачів, які вже не потребують доступу до інформації.

Доступ до інформаційних систем з широким колом користувачів необхідно контролювати шляхом формальної процедури, наприклад:

- перевіряти дозвіл на використання системи;
- перевіряти достатність рівня доступу для виконання користувачем своїх функцій;
- періодично змінювати ідентифікатори та паролі;
- здійснювати формальний облік усіх осіб, які використовували систему;
- ліквідовувати права на доступ в осіб, які змінили місце роботи тощо.

З метою контролю доступу до комп'ютерних систем, внутрішнього монтажу, ліній зв'язку, технологічних органів керування застосовується техніка контролю розкриття апаратури. Це означає, що на об'єкти, які захищаються, закриваються кожухами, кришками, встановлено датчики, що спрацьовують при спробі одержати доступ до апаратури. Сигнал від датчика мережами надходить у централізований пристрій контролю.

У зв'язку з тим, що сьогодні паролі є основним засобом підтвердження повноважень доступу до комп'ютерних систем, необхідно отримати від користувачів письмові зобов'язання про необхідність зберігання їх у таємниці. У деяких випадках користувачі самі вибирають собі паролі. У таких випадках тимчасові паролі необхідно відразу замінити. Тимчасові паролі можуть надаватися користувачам, які забули свої паролі. Для унеможливлення таких ситуацій дубль паролю зберігають в опечатаному конверті в канцелярії установи. Користувачі повинні зберігати свої паролі у захищених місцях (не на клавіатурі або килимку для миші).

Парольний захист даних широко застосовують операційні системи (наприклад, Windows). Проте самі паролі перебувають у спеціальних файлах, інформацію з яких можна зчитати за допомогою спеціальних програм. Для унеможливлення цього необхідно відключити запис паролю в кеш-пам'ять за допомогою редактора реєстру.

Для виявлення паролів зловмисники використовують різноманітні програми, зокрема Brute-Force (груба сила), Software-Robbery тощо, які за допомогою перебору або спеціальних алгоритмів отримують паролі користувачів. Протидію цьому є якомога довші паролі зі спеціальними символами. Це унеможливить роботу навіть потужних комп'ютерних систем, які задіяні для виконання таких програм.

При створенні корпоративних комп'ютерних мереж виникає потреба їх адміністрування. При цьому необхідно підготовити відповідні інструкції і процедури реагування на події. Ці процедури повинні передбачати такі інциденти: відмова системи, порушення конфіденційності, неточність даних тощо. При цьому по завершенні ліквідації загроз слід проаналізувати причини інциденту, спланувати заходи щодо запобігання повторенню інциденту, здійснити реєстрацію та пошук додаткової інформації, необхідної для якісного аналізу. Усі інциденти слід реєструвати в контрольному журналі.

Нові інциденти дають можливість фіксувати засоби операційних систем. Скажімо операційна система Windows-NT, яка значно надійніша за своїх попередниць (при інсталяції системи необхідно вибрати тип файлової системи NTFS-NT File System), дозволяє застосовувати такі засоби безпеки, як організація доступу до дисковода або директорії та ін.

Операційна система Windows NT дає можливість контролювати велику кількість подій у комп'ютерній системі та протоколювати їх у базі даних. До таких подій можуть належати, скажімо, повідомлення про закінчення сеансу, робота з файлами тощо. Які саме події повинні протоколюватися, встановлює адміністратор системи. Усі події не потрібно реєструвати — адже таку базу важко буде проаналізувати. Час від часу необхідно з дозволу керівництва здійснювати контроль, наприклад, за використанням конфіденційних ресурсів або користувачем, який має привілейований доступ до системи.

Для запобігання несанкціонованому доступу до комп'ютерів у складних системах необхідно здійснювати автоматичну ідентифікацію терміналів. Ідентифікація важлива у тих випадках, коли сеанс зв'язку повинен здійснюватися з конкретного термінала. Певна надійність має бути при процедурі входу в комп'ютерну систему. Вона повинна виконувати такі функції:

- не виводити на екран ідентифікатори системи, доки не завершиться процес входу в систему;
- не надавати довідкову інформацію, яка б могла допомогти незареєстрованому користувачеві;
- перевіряти достовірність усіх реєстраційних даних тільки після завершення введення інформації;
- обмежити кількість невдалих спроб входження в систему;
- визначити якнайменшу та якнайбільшу тривалість процедури входження в систему. У разі невідповідності термінів необхідно зупинити процедуру входження;
- після завершення успішної процедури входження необхідно вивести на екран дату та час попереднього сеансу роботи та відомості про невдалі спроби входження в систему.

Розмежування доступу. Для зменшення ризику несанкціонованого доступу до інформації, особливо у фінансовій сфері, використовують розділення певних обов'язків, зокрема: введення даних, розробка та застосування систем, контроль засобів захисту тощо.

Розмежування доступу в обчислювальній системі полягає в поділі інформації, що циркулює в ній, на частини й організації доступу до цих частин посадових осіб відповідно до їхніх функціональних обов'язків і повноважень.

Завданням розмежування доступу є зменшення кількості осіб, що не мають відношення до інформації при виконанні своїх посадових обов'язків, тобто захист інформації від порушника серед персоналу, а також ідентифікація й аутентифікація об'єкта (суб'єкта).

Ідентифікація — надання якому-небудь об'єктові унікального образу, імені, числа. Аутентифікація полягає в перевірці того, чи насправді об'єкт, що перевіряється, є тим, за кого себе видає. Кінцева мета ідентифікації та аутентифікації об'єкта в системі — допуск його до інформації з обмеженим доступом у разі позитивного результату перевірок або відмови в доступі при негативних результатах. Об'єктами ідентифікації та аутентифікації можуть бути: людина (оператор, користувач, посадова особа); технічні засоби (термінал, дисплей, ЕОМ); документи; носії інформації (магнітні стрічки, диски тощо); інформація на дисплеї, табло тощо. Аутентифікацію об'єкта може здійснювати людина, апаратний пристрій, програма, система тощо.

Процедури ідентифікації можуть бути одноразовими або періодичними (особливо в разі тривалих сеансів роботи). У цих процедурах застосовуються різні методи:

• прості, складні або одноразові паролі;
• обмін запитаннями і відповідями з адміністратором;
• ключі, магнітні картки, значки, жетони;
• засоби аналізу індивідуальних ознак (голосу, відбитків пальців, геометричних параметрів рук, обличчя);
• спеціальні ідентифікатори або контрольні суми для апаратури, програм, даних тощо.

Найбільш поширеним методом ідентифікації є парольна ідентифікація.

Практика свідчить, що парольний захист даних є слабкою ланкою, тому що пароль можна підслухати або підглядіти, перехопити, а то й просто розгадати.

Для захисту самого пароля вироблено рекомендації, як зробити пароль надійним:

• пароль повинен містити принаймні вісім символів. Чим менше символів містить пароль, тим легше його розгадати;
• не застосовуйте як пароль очевидний набір символів, наприклад, ваше ім'я, дату народження, імена близьких або найменування ваших програм. Найкраще застосовувати для цих цілей невідому формулу або цитату;
• якщо криптографічна програма дозволяє, введіть у пароль бодай один нелітерний символ або прописну букву;
• не називайте нікому ваш пароль, не записуйте його;
• частіше змінюйте пароль.

Захист інформації від витоку за рахунок побічних електромагнітних випромінювань і наведень (далі — ПЕМІН). Робота обчислювальної техніки супроводжується електромагнітним випромінюванням і наведеннями на суміжні лінії (мережу електроживлення, "землю", сторонні лінії), що виникають унаслідок електромагнітних впливів у ближній зоні випромінювання. Електромагнітні випромінювання, навіть якщо вони відповідають припустимим технічним нормам, не є безпечними з погляду витоку секретної інформації і несанкціонованого доступу до неї. У деяких випадках інформацію, оброблену засобами обчислювальної техніки, можна відновити за рахунок аналізу електромагнітних випромінювань і завад. Для цього необхідно здійснити їх прийом і декодування. Певний час вважали, що неможливо розшифрувати інформацію, яка міститься у випромінюванні. Однак дослідження виявили, що відновлення інформації з випромінювання від деяких електронних засобів можливе за допомогою загальнодоступних радіоелектронних пристроїв. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і завад містяться у документі ПЕМІН-95 від 09.06.1995 р. № 25.

Програмний захист даних. Це система спеціальних програм, що включаються до складу програмного забезпечення захисту даних. Відзначимо, що надійна робота інформаційної системи залежить від якості програмного забезпечення, завдяки якому здійснюється обробка даних. Тому питання захисту даних слід вирішувати ще на початку проектування комп'ютерних інформаційних систем. Як свідчить практика, багато "латок", які створюються з метою тестування програм, застосовуються потім для несанкціонованого доступу до інформації. Для унеможливлення цього необхідно розділити процеси розробки і тестування програм.

Засоби захисту будуть дешевшими й ефективнішими, якщо їх вмонтувати у прикладні системи на стадії проектування. Усі вимоги до безпеки, включаючи необхідність переходу на аварійний режим для продовження обробки інформації, варто визначити у технічному завданні, а також обґрунтувати, погодити і задокументувати в рамках загального плану щодо створення інформаційної системи.

У прикладних програмних системах необхідно передбачити контроль при введені даних та перевірку достовірності даних після їх обробки. Для перевірки вхідних даних стандартом ISO 17799 пропонується застосовувати такі методи:

а) перевірки з метою виявлення таких помилок:
• величини, що виходять за задані межі;
• неправильні символи в полях даних;
• пропущені або неповні дані;
• перевищені верхні й нижні межі на введений обсяг даних;
• несанкціоновані або суперечливі дані;

б) періодичний аналіз змісту ключових полів або файлів даних для підтвердження їх вірогідності й цілісності;

в) огляд друкованої вхідної документації на предмет внесення несанкціонованих змін у вхідні дані (необхідно одержати дозвіл на внесення всіх змін у вхідні документи);

г) процедури реагування на помилки, пов'язані з перевіркою вірогідності вхідних даних;

д) визначення обов'язків усіх співробітників, що беруть участь у процесі введення даних.

Дані, що були введені в прикладну систему, можуть бути ушкоджені в результаті помилок обробки або навмисних дій. Щоб виявити такі випадки, необхідно вмонтувати засоби перевірки в системи. Прикладами засобів перевірки, які можна вмонтувати в системи, є:

а) контроль сеансу зв'язку і пакетної обробки для узгодження файлів даних про платіжний баланс після проведення операцій з ними;

б) контроль платіжного балансу для звірення початкового сальдо з кінцевим сальдо:
• контроль за виконанням операцій;
• підбиття підсумків з відновлення файлів;
• контроль за виконанням програм;

в) перевірка вірогідності даних, згенерованих системою;

г) перевірка цілісності даних і програм, що пересилаються між комп'ютерами;

д) підбиття підсумків з відновлення файлів.

Зазвичай в установах та організаціях прикладне програмне забезпечення постійно змінюється. Це зумовлено зміною технологій, вихідних форм, розширенням видів діяльності тощо. Щоб звести ризик ушкодження інформаційних систем при внесенні в них змін до мінімуму, варто здійснювати жорсткий контроль за цим процесом. Для цього потрібні формальні процедури контролю за внесенням змін. Ці процедури повинні гарантувати, що безпеку і процедури контролю буде забезпечено, що відповідним працівникам надано доступ тільки до тих компонентів системи, які необхідні для їх роботи, і що отримано формальний дозвіл на внесення змін. Такий процес повинен складатися з наступних етапів:

а) реєстрація погоджених рівнів повноважень, у тому числі:
• служба прийому запитів на внесення змін групою, що обслуговує інформаційні системи;
• повноваження користувачів на подачу запитів на внесення змін;
• рівні повноважень користувачів на прийняття докладних пропозицій;
• повноваження користувачів на прийняття внесених змін;

б) прийняття змін, пропонованих тільки зареєстрованими користувачами;

в) перевірку засобів керування безпекою і процедур забезпечення цілісності на предмет їх компрометації внесеними змінами;

г) виявлення всіх комп'ютерних програм, файлів даних, баз даних і апаратних засобів, що потребують внесення виправлень;

д) затвердження докладних пропозицій до початку роботи;

е) прийняття пропонованих змін зареєстрованими користувачами до їх внесення;

є) відновлення системної документації після завершення процесу внесення кожної зміни, а також архівація або знищення старої документації;

ж) здійснення контролю над версіями всіх поновлюваних програм;

з) реєстрація всіх запитів на внесення змін у контрольному журналі.

Серед особливостей програмних продуктів слід відзначити також їх тісний взаємозв'язок з апаратною реалізацією системи безпеки. На цьому етапі захисту програмні засоби практично не застосовуються окремо – як правило, їх включають в операційну систему або ж вони є у складі апаратно-програмних комплексів захисту даних. Тому при здачі комп'ютерних систем в експлуатацію слід звернути увагу на потужність комп'ютерів щодо здатності виконувати відповідні функції та підготовку персоналу до застосування нових систем, у тому числі в аварійних ситуаціях.

Спеціалізовані системи захисту даних комп'ютера класифікують на групи засобів, які здійснюють захист: завдяки загальному програмному забезпеченню; у складі обчислювальної системи; захисту із запитом інформації; активного захисту; пасивного захисту тощо.

Виділяють такі напрями застосування програм: захист даних та програм від вірусів; захист даних від несанкціонованого доступу; захист даних та програм від копіювання; програмний захист каналів зв'язку.

Основними функціями, що мають здійснюватися програмними засобами, є:

- ідентифікація суб'єктів і об'єктів;
- розмежування (або повна ізоляція) доступу до інформації та даних;
- контроль і реєстрація дій з програмами.

Що стосується доступу, який залежить від повноважень працівників, то він передбачає звернення користувача до програм, даних, устаткування залежно від наданого режиму доступу. Такими режимами можуть бути "тільки читати", "читати і писати", "тільки виконувати" та ін. В основі більшості засобів контролю доступу лежить те або інше уявлення про матрицю доступу. Інший підхід до побудови засобів захисту доступу заснований на контролі інформаційних потоків і поділі суб'єктів та об'єктів доступу на класи конфіденційності. Прикладні програми, які підтримують конфіденційну інформацію, повинні надавати користувачу тільки необхідні дані і тільки на комп'ютери, доступ до яких передбачено управлінням доступом.

Паролі. Паролі на сьогодні є основним засобом підтвердження доступу користувачів до комп'ютерної системи. Тому необхідно впроваджувати системи їх управління, які повинні виконувати такі функції:

- за потреби зобов'язувати користувачів змінювати індивідуальні паролі;
- здійснювати облік попередніх паролів користувачів (протягом року);
- змінювати паролі, які надаються постачальниками програм;
- перевіряти надійність паролів користувачів, наприклад, за такими параметрами: назва організації, імена користувачів, більш як два однакових символи підряд тощо.

Необхідно також розглянути можливість використання сигналу тривоги, який попереджає, що правильний пароль було набрано користувачем під фізичним тиском.

Програмні засоби реєстрації, як і засоби контролю доступу, належать до ефективних заходів захисту від несанкціонованих дій. Однак, якщо засоби контролю доступу призначені для запобігання таким діям, то задача реєстрації – виявити вже вчинені дії або спроби їх вчинити.

Антивірусний захист. Серед набору програм, що використовується більшістю користувачів персональних комп'ютерів, антивірусні програми займають особливе місце. Найбільшого поширення набули McAfee VirusScan, AVPKaspersky, DrWeb32, Symantec AntiVirus, Aidstest тощо. Вони є багатофункціональними продуктами, що сполучать у собі як превентивні, профілактичні засоби, так і засоби "лікування" вірусів та відновлення даних [237, с. 76-83].

Віруси – це потенційно "агресивні" шкідливі програми, що призводять до порушення роботи комп'ютера. "Отримати" вірус на свій комп'ютер можна двома шляхами: на електронному носії (дискеті або компакт-диску) або ж через Інтернет. На сьогоднішній день електронна пошта є основним засобом поширення комп'ютерних вірусів. За даними Міжнародної організації комп'ютерної безпеки, понад 60 % випадків зараження вірусами відбувається саме за допомогою електронної пошти. У цих умовах проблема надійного захисту корпоративної мережі від потоку небезпечних програм через електронну кореспонденцію стає найбільш гострою.

Найпоширенішим антивірусним продуктом можна назвати Antiviral Toolkit Pro (AVP) лабораторії Євгена Касперського (//www.avp.ru). Програма має зручний інтерфейс користувача, велику кількість настроювань, а також одну з найбільших у світі антивірусних баз, кількість даних у якій постійно збільшується. У комплект постачання включений так званий монітор – засіб, що при завантаженні операційної системи вмикається та робить перевірку файлів, до яких відбувається звертання. Додатково можливе підключення перевірки електронної пошти.

Не менш відомий Norton AntiVirus корпорації Symantec (//www.symantec.com). Це чи не єдиний на весь світ продукт, здатний виявити та видалити усі існуючі у світі макровіруси (віруси, які можуть завдавати шкоди на усіх рівнях е-середовища – чи то домашній персональний комп'ютер, робоча станція в офісі, сервер або шлюз Інтернету). Автоматичне сканування всієї пошти, наявність засобів для затримки даних гарантують захист користувачів.

Дуже поширеною є програма Doctor Web (//www.drweb.ru). Вона включає в себе інтелектуальну технологію вірусної активності, резидентний антивірусний контроль файлів та функції перевірки вірусів під час роботи у Інтернеті. Програма поширена у локальних мережах, які організують масове підключення до Інтернету. Захист від проникнення вірусів через мережу Інтернет і електронну пошту може також надати програма McAfee VirusScan (//www.mcafee.ru). При цьому скануються е-пошта на рівні поштових скриньок до її запису у файли на диск комп'ютера.

Захист даних у локальній мережі. Локальна комп'ютерна мережа складається з взаємопов'язаної множини засобів комп'ютерної техніки, програмного забезпечення, мережного та периферійного обладнання у межах одного будинку (чи сусідніх будинків) і призначена для надання працівникам однієї організації, установи тощо доступу до інформаційних ресурсів та послуг мережі.

Управління локальною мережею здійснюється адміністратором шляхом керування серверним комп'ютером, який є головним у цій мережі. Для обмеження доступу конкретного клієнта мережі до ресурсів даних інших комп'ютерів з метою попередження даних чи порушення конфіденційності адміністратор мережі виконує ряд дій над стандартними функціями операційної системи з виконання обмеження доступу. Основною задачею при цьому є настроювання "Віддаленого управління" (доступ до дискових ресурсів іншого комп'ютера), щоб адміністратор мав доступ до всіх комп'ютерів мережі, а клієнти – тільки до ресурсів свого комп'ютера або ресурсів, відкритих адміністратором для загального доступу. Це зробити легко. На кожному клієнтському комп'ютері в

"Панелі управління" оберіть пункт "Паролі". У вікні, що з'явилося, повинна бути закладка "Віддалене управління". Досить увімкнути прапорець "Дозволити віддалене управління" і ввести пароль для доступу (Рис. 4.1).

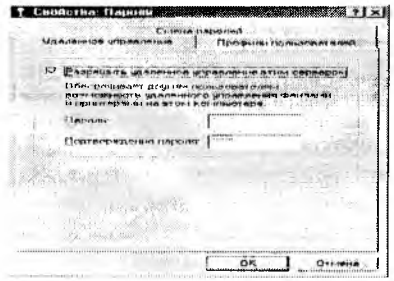


Рис. 4.1

Якщо немає закладки "Віддалене управління", перевірте, чи дозволений доступ до файлів комп'ютера в настроюваннях мережі. На комп'ютері адміністратора, щоб уникнути несподіванок, упевніться в тому, що віддалене управління відключене. Коли усе налагоджено, можна перейти до перевірки. Для одержання віддаленого управління будь-яким комп'ютером у мережі відкрийте на центральному комп'ютері "Мережне оточення", оберіть потрібний комп'ютер і, відкривши його властивості, натисніть кнопку "Управління", що знаходиться на закладці "Сервіс" (Рис. 4.2).

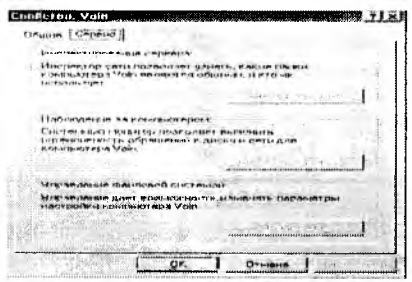


Рис. 4.2

Спочатку з'явиться вікно із запитом на введення пароля. Після цього ви дістанете доступ до всіх дисків комп'ютера незалежно від настроювань доступу до диска. На початку роботи введіть паролі до всіх комп'ютерів, і надалі ви зможете швидко відкрити доступ до всіх дисків будь-якого комп'ютера, натиснувши кнопку "Управління".

Захист даних від програм шпигунів. Для збору персональних даних про користувачів створюються програми-шпигуни, або spyware. Spyware – це програма, що посилає персональні дані з вашого комп'ютера на будь-який інший, причому, це відбувається без вашого відому і згоди. Програма пересилає дані з того моменту, як тільки комп'ютер з'єднався з Інтернетом. Передача даних здійснюється у фоновому режимі, її дуже важко прослідкувати.

Дані, що пересилаються, можуть включати усе, що знаходиться на вашому комп'ютері, тобто, на дисках вашого комп'ютера. Для багатьох фірм великий інтерес становлять адреси електронної пошти, необхідні для розсилання за ними рекламних оголошень. Іншим компаніям хочеться знати, які сторінки в Інтернеті ви відвідуєте, на які сайти в Інтернеті заходите, що купуєте в Інтернет-магазинах, ваші бажання, інтереси тощо.

Ще одна можлива дія spyware полягає в зміні настроювань вашого браузера (програми, за допомогою якої ви продивляєтеся веб-сторінки).

Існують ситуації коли програма визначає веб-сторінку, котра пропонує послуги, як таку, що завантажується "за замовченням", тобто відкривається в браузері при кожному з'єднанні з Інтернетом. Також spyware можуть погіршити з'єднання з Інтернетом або вплинути на працездатність системи в цілому. На відміну від творців "троянських копей", авторам spyware необхідно лише ваше "Ok", щоб установити свій виріб на ваш комп'ютер. Деякі програми застосовують "вікна" із сертифікатами і ліцензіями, у яких потрібно підтвердити прочитання, натиснувши "Ok". Оскільки зазначене містить складні формулювання і рідко читається користувачами – це шлях установки spyware на комп'ютер разом з вільно поширюваною програмою. Виробники, діставши згоду на установку програми на вашому комп'ютері і передачу даних з нього, заявлять, що їхній продукт – не spyware і програма була встановлена після одержання вашого дозволу. Але навряд чи будь-хто схвалить несанкціоноване використання даних з його комп'ютера.

Проникнення шпигунських програм. Є багато шляхів проникнення шпигунських програм на комп'ютери. Установлюючи сумнівну програму, обов'язково прочитайте всі коментарі в процесі установки. Частина *spyware*-додатків може встановлюватися після появи "вікна" операційної системи, наприклад, такого, як на Рис. 4.3. Не слід натискати "Ok", не прочитавши повідомлення і не переконавшись в тому, що програма, яка пропонується, дійсно потрібна.

Захист даних через настроювання параметрів Active-X. Припустімо, що ви використовуєте операційну систему Windows XP і браузер для роботи з Інтернеті Internet Explorer. Є кілька параметрів вікна перегляду, які можна налагодити так, щоб гарантувати захист при роботі в Інтернеті. Насамперед це стосується того, як ваним браузером сприймаються елементи Active.

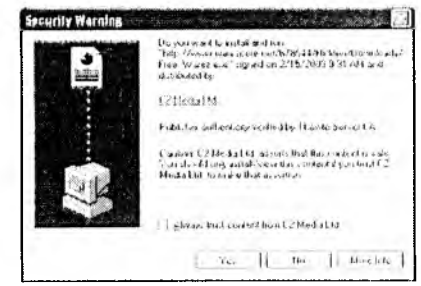


Рис. 4.3

Елементи управління Active-X є програмами, що можуть виконуватися під управлінням Windows безпосередньо на веб-сторінці. Вони можуть включати багато компонентів, таких як форми, звук і графіка. Але найбільш небезпечна функція – можливість установки програм. Багато компаній застосовують елементи управління Active-X, щоб

виконувати установку програми з веб-сайтів. За замовчуванням усі операційні системи Windows запитують у користувачів дозвіл на установку подібних додатків, але програми можуть змінити настроювання браузера, щоб обходити цей етап і автоматично запускати елементи управління Active-X. Щоб уникнути цього:

➢ У Internet Explorer натисніть на меню "Tools"(сервіс), потім "Internet options" (властивості оглядача) і виберіть закладку "Security" (безпека) (Рис. 4.4).

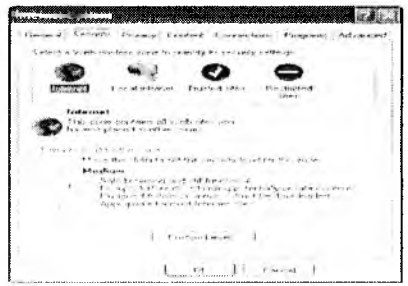


Рис. 4.4

➢ Оберіть кнопку "Custom level" (інший) (Рис. 4.5).

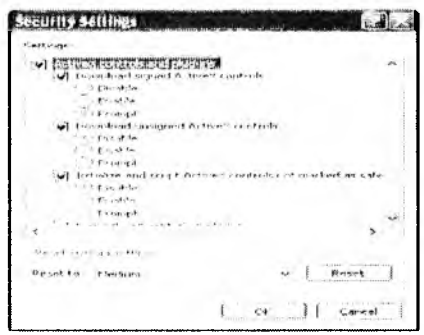


Рис. 4.5

Переконайтеся, що виключено опції "Download unsigned Active-X controls" (завантаження елементів Active, що не підписані) і "Initialize and script Active-X controls not marked as safe" (використання елементів Active, не позначених як безпечні). Для підвищеної безпеки установіть всі опції Active-X на цій сторінці в положення "Prompt" (попереджати).

Найбільш імовірна установка spyware програм (крім натискання "Ok", не переглядаючи текст у вікні) – при використанні низького рівня безпеки або неправильній установці керуючих кнопок Active-X. Якщо встановлений "низький рівень безпеки" або установки Active-X усе дозволяють, то spyware-програми зможуть встановлюватися на вашому комп'ютері без усяких попереджень або дозволів. Переконайтеся в тому, що всі опції Active-X встановлені в "Prompt" (попереджати) (Рис. 4.5), і регулярно встановлюйте поновлення від Мікрософт, що усувають виявлені проблеми в системі безпеки.

Утиліти для видалення програм-шпигунів. Якщо є підозра, що у комп'ютері є з'явилася spyware програма, то кращий спосіб позбавитися – встановити та запустити одну з програм для її виявлення та вилучення. Звісно, краще, щоб ця програма поширювалася безкоштовно. Взагалі, видалення шпигунських програм вручну – це складна та копітка робота, причому різна для кожної програми-шпигуна. Так що найбільш імовірний шлях – застосування спеціальних програм для видалення шпигуна.

Lavasoft Ad-Aware (www.lavasoftusa.com) – найвідоміша утиліта для видалення шпигунських програм (Рис. 4.6).

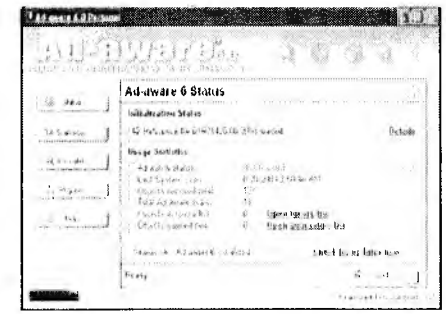


Рис. 4.6

Вона працює подібно до антивірусу шляхом сканування файлів вашого комп'ютера. Програма поширюється безкоштовно для фізичних осіб та як комерційний пакет для підприємств.

Криптографічні засоби захисту. Криптографія – це наука про захист даних за допомогою їх кодування, шифрування. Під цей термін підпадає порядок, що визначає принципи, засоби та методи, які застосовуються при трансформації даних з метою приховання їх інформаційного змісту, запобігання їх несанкціонованій зміні чи несанкціонованому користуванню.

Основні напрями застосування криптографічних методів - при передачі конфіденційних відомостей каналами телекомунікації (наприклад, е-пошта), встановлення істинності повідомлень, що передаються, зберігання даних (баз даних) на носіях у зашифрованому вигляді.

Сьогодні поширення щодо сфери захисту персональних даних отримав *засіб криптографічного захисту персональних даних – програма Pretty Good Privacy (PGP).*

Програма PGP була розроблена Філом Зімерманом (США), який зазначав про неї: "Це з самого початку був правозахисний, некомерційний проект". Сьогодні в Інтернеті існує понад 70 сайтів на 17 мовах світу, присвячені цій програмі (наприклад, у Норвегії – //www.pgpi.org; Росії – //www.pgpru.org).

Сила PGP не в тому, що ніхто не знає, як її зламати (дешифрувати) інакше, як з використанням "лобової атаки", а в продуманому і могутньому механізмі обробки ключів, швидкості, зручності й широті розповсюдження. Існують десятки не менш сильних алгоритмів шифровки, ніж той, котрий використовується у PGP, але популярність і безкоштовне поширення зробили PGP фактичним стандартом для електронного листування в усьому світі.

Звичайні засоби криптографії (з одним ключем для шифровки і дешифрування) припускали, що сторони, які вступають у листування, повинні на початку обмінятися секретним ключем, або паролем з застосуванням якогось секретного каналу ("дупло", особиста зустріч і т. ін.) для того, щоб почати обмін зашифрованими повідомленнями. Виходить замкнуте коло: щоб передати секретний ключ – потрібно секретний канал, щоб створити секретний канал – потрібно ключ.

PGP відноситься до класу систем із двома ключами – публічним і секретним. Це означає, що ви можете повідомити про свій публічний ключ усьому світові, при цьому користувачі програми зможуть відправляти вам зашифровані повідомлення, які ніхто, крім вас, розшифрувати не зможе. Ви ж їх розшифровуєте за допомогою вашого другого, секретного ключа, що тримається в таємниці.

Ви можете опублікувати свій публічний ключ на вашій веб-сторінці або послати його електронною поштою своєму другові. Ваш кореспондент зашифрує повідомлення з використанням вашого публічного ключа і відправить його вам. Прочитати його зможете тільки ви з використанням секретного ключа. Навіть сам відправник не зможе розшифрувати адресоване вам повідомлення, хоча він сам написав його 5 хвилин тому.

На сьогодні вважається, що навіть найбільш потужним комп'ютерам у ЦРУ потрібні століття, щоб розшифрувати повідомлення, зашифроване за допомогою PGP.

Найпоширеніші версії PGP:

• Aegis Shell випускається Aegis Products (//www.aegisrc.com). Серйозна програма з безліччю функцій.

• MailPGP 1.3 (//www.iki.fi). Програма з набором функцій, здатних задовольнити переважну більшість користувачів. Після завантаження має такий вигляд (Рис. 4.7).

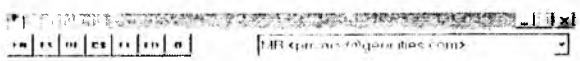


Рис. 4.7

Шифрування в зображенні і звуці. Цей клас продуктів дозволяє ховати повідомлення у файли .bmp, .gif, .wav. Він призначений для тих випадків, коли ви не хочете, щоб у когонебудь створилося враження, що ви користуєтеся засобами криптографії. Приклад подібної програми – Stools. Вона дуже легка в користуванні. Зовні графічний файл залишається практично незмінним, змінюються лише подекуди відтінки кольору. Для більшої безпеки варто застосовувати невідомі широкому загалу зображення, зміни в яких не впадуть в око з першого погляду, а також зображення з великою кількістю півтонів і відтінків. Застосовувати зображення картини "Мона Ліза" – ідея погана, тому що всі знають, як вона виглядає, і крім того, вона містить великі зони одного кольору. А от маловідома фотографія цілком підійде, наприклад щодо Рис. 4.8.

Рис. 4.8

Ліве зображення (розмір 8,9 кілобайта) не містить зашифрованої інформації, праве (розмір 11,2 кілобайта) містить текст цієї глави. Практично немає ніяких відмінностей. Співвідношення між розміром зображення і розміром текстового файла, який можна сховати, залежить від конкретного зображення. Іноді розмір текстового файла навіть перевищує розмір графічного. Програма може застосовувати кілька різних алгоритмів шифровки на вибір користувача, включаючи алгоритм 3DES.

Взагалі для програм злому використовують один із двох підходів. Вони або підбирають пароль (слово) із великого словника, або атакують навпростець (brute force), перебираючи всі можливі комбінації. Звідси простий висновок: слід завжди використовувати парольне слово, якого немає у словнику, або букви, цифри та спеціальні символи (наприклад, ?!$...).

Час, який є необхідним для обчислювання комп'ютером різних комбінацій щодо визначення пароля з 6 знаків, за умов його швидкості 200 000 комбінацій на секунду (відповідає можливостям ПК Pentium 100), представлено далі у Таблиці.

Якщо довжина пароля не шість, а 24 символи, то на розшифрування піде дуже багато часу, навіть – тисячоліччя.

Таблиця

Набір символів	Максимальний час
тільки цифри	5,0 секунд
тільки малі літери	25,7 хвилини
тільки символи	1.8 години
рядкові і заголовні букви	27.5 години
рядкові, заголовні цифри	3,3 дня
рядкові, заголовні цифри, символи	42,5 дня

Особливості захисту даних в Інтернеті. Однією з основних ознак інформаційного суспільства є широке застосування організаціями і громадянами мережі Інтернет.

Значне зростання кількості користувачів цієї мережі призвело водночас до поширення кіберзлочинності, в тому числі щодо неправомірного збору, використання та поширення персональних даних. Комп'ютерні технології та транскордонні комп'ютерні мережі, які є необхідними складовими міжнародної фінансової та банківської діяльності, надали можливість вчинення злочинів економічної спрямованості на національному та міждержавному рівнях. Організовані злочинні угруповання та кримінальні елементи використовують новітні технології для відмивання "брудних" коштів, фінансових махінацій, несанкціонованого доступу до інформаційних систем, поширення неправдивої інформації та інших правопорушень. Сьогодні збитки від кіберзлочинності перевищують 100 млрд. дол. США. За даними американського Інституту комп'ютерної безпеки (Computer Security Institute), хакери використовують такі найпоширеніші методи: підбір ключів, паролів (brute-force) у 13,9 % злочинів; заміна IP-адрес (IP-spoofing) – у 12,4 % (цей метод атаки передбачає заміну IP-адрес пакетів, що передаються в Інтернеті, так, що вони мають вигляд переданих внутрішніх повідомлень, де кожний вузол передає адресну інформацію іншому); ініціювання відмови в обслуговуванні (denial of service) у 16,3 % (вплив на мережу або її окремі частини з метою порушення порядку її штатного функціонування); аналіз трафіку (sniffer) – 11,2 % (прослуховування та дешифрування з метою збирання інформації щодо ключів, паролів тощо); сканування (scanner) у 15,9 % (передбачає застосування програми, яка перебирає можливі точки входження

до системи); підміна, нав'язування, переупорядкування або заміна даних, що передаються мережею (data didling) – у 15,6 %; інші методи – 14.7 %. Таким чином, платою за користування Інтернетом є загальне зниження інформаційної безпеки.

Один із засобів підтримки інформаційної безпеки – міжмережний екран (firewall), який виконує свої функції, контролюючи всі інформаційні потоки між внутрішньою інформаційною системою та зовнішнім інформаційним простором як "інформаційна мембрана". Тобто екран можна уявити собі як набір фільтрів, які аналізують дані, які через нього проходять, на основі певних алгоритмів, що вирішують блокувати або пересилати дані. Така система може виконувати реєстрацію подій, пов'язаних з процесом розмежування доступу, зокрема фіксувати всі "незаконні" спроби доступу до даних та сигналізувати про ситуації, які потребують негайної реакції. Відзначимо основні вимоги до таких систем:

- підтримка безпеки мережі і повний контроль над сеансами зв'язку;
- система повинна мати гнучкі засоби керування для простого та повного втілення в життя політики безпеки організації і, крім того, для забезпечення простої реконфігурації системи при зміні структури мережі;
- система повинна працювати непомітно для користувачів локальної мережі та не ускладнювати виконання ними легальних дій;
- система повинна працювати досить ефективно і встигати обробляти весь вхідний і вихідний трафік у "пікових" режимах. Це необхідно для того, щоб Firewall не можна було перевантажити великою кількістю викликів, що призвели б до порушення її роботи;
- система підтримки безпеки повинна бути сама надійно захищена від будь-яких несанкціонованих впливів, оскільки вона є ключем до конфіденційної інформації в організації;
- якщо в організації є кілька зовнішніх підключень, у тому числі й у віддалених філіях, система керування екранами повинна мати можливість централізовано забезпечувати для них проведення єдиної політики безпеки.

Система Firewall повинна мати засоби авторизації доступу користувачів через зовнішні підключення. Система повинна вміти надійно розпізнавати легальних користувачів і надавати їм необхідний доступ до інформації.

У багатьох організаціях обмін даними за допомогою Інтернету централізовано контролюється брандмауером, суміщеним з маршрутизаторами, наприклад, Solstice FireWall-1. Незважаючи на це, через непрофесіоналізм адміністраторів приблизно 30 % зломів відбувається після встановлення захисних систем. При цьому складається помилкове враження захищеності. Останнім часом застосовуються персональні брандмауери, які дають можливість здійснювати контроль за даними, що передаються в мережу (Norton Personal Firewall 2001, PGP Desktop Security 7.0, Sandbox Secure 4U Professional). При роботі з брандмауерами необхідно перш за все заблокувати всі порти комп'ютера і після цього відкрити тільки ті, які справді необхідні для роботи. Потрібно також активізувати протоколювання сигналів тривоги. При цьому, прочитавши Log-файл, можна дізнатись про всі спроби встановлення з'єднань.

Для блокування інформації, яка заборонена законом (порнографія, насильство, расистські заклики), використовують такі фільтруючі програми, як Arlington Custom Browser, Cyberpatrol, Web-broker тощо. Проте вони не завжди адекватно блокують певні сайти через недосконалі механізми визначення забороненої інформації.

Надзвичайно важливе значення в Інтернеті мають засоби ідентифікації, адже, отримавши їх, зловмисник має можливість прочитати будь-чию е-пошту, відправити листа від вашого імені, здійснити фінансові операції у віртуальному просторі.

Так, у листопаді 2002 р. американські правоохоронці заарештували трьох осіб, які здійснювали електронні крадіжки грошей. Було доведено, що трійця пограбувала близько 30 тисяч американців на суму 2.700 тис. дол. США. Хакери вираховували коди фінансових установ та банків, підробляли кредитні картки, виписували чеки та брали кредити. Слідчі вважають, що в історії США це найбільша афера з кредитними картками.

Тому особисті паролі в жодному разі не можна повідомляти ні усно, ні е-поштою. Забороняється запуск програм, вкладених в е-пошту, якщо ви їх спеціально не замовляли. У них можуть бути вкладені троянські програми для отримання ідентифікаторів користувачів.

Про компрометацію паролів можна дізнатися, якщо вам прийдуть несплачені рахунки. Тому, якщо провайдер надає засоби для контролю над входами та виходами з системи, то їх рекомендується регулярно застосовувати. Якщо провайдер сповіщає про велику кількість помилок при вході в систему, це означає, що хтось намагається розпізнати ваш пароль.

Якщо пароль скомпрометовано, необхідно негайно його змінити. Якщо самостійно це зробити неможливо, зверніться за допомогою до вашого провайдера.

Крім захисту паролю, при роботі в Інтернеті необхідно якнайменше надавати особистої інформації (номери телефонів, домашню адресу тощо), адже цією інформацією можуть скористатися зовсім незнайомі вам люди. Також відомі випадки реальних кримінальних подій після віртуального знайомства.

Декілька слів слід сказати про конфіденційність роботи в Інтернеті. Адже програми, пристосовані для полегшення роботи, можуть надавати інформацію про те, що ви робили в глобальній мережі. Передусім усе це стосується журналу браузера, який зберігає список Інтернет-адрес, які ви відвідували. Тому необхідно час від часу "очищати" цей перелік (General, History, Clear). Для того щоб записи взагалі не фіксувалися, необхідно застосовувати опцію браузера "Відкрити сторінку" ("Open page"), у вікні якого і вказати потрібну адресу.

Для прискорення завантаження Інтернет-сторінок браузери зберігають їх на магнітному диску. Для того щоб видалити зазначені файли, необхідно в меню "Сервіс" ("Tools") браузера на вкладці "General" натиснути клавішу "Delete Files".

На окрему увагу заслуговують файли "cookie". Вони створюються веб-серверами для запису інформації про переглянуті сторінки: дату, час, пароді тощо. Ця інформація використовується для аналізу статистичних даних та створення так званих профілів користувачів (які сторінки переважно переглядає користувач, які товари замовляв тощо). Тому для припинення такої діяльності використовують або знищення файлів "cookie" на вінчестері, або блокування цих файлів завдяки опціям браузерів (Edit>Preferences>Advanced>Disable Cookies).

Питання для самоконтролю

1. Інформаційна діяльність та основні напрями її упорядкування.
2. Упорядкування інформаційних відносин та гармонізації їх з положеннями європейських стандартів у сфері інформатизації.
3. Інформаційні послуги.
4. Підтримка інформаційної безпеки.
5. Відповідальність суб'єктів.
6. Інтеграція України у світовий інформаційний простір.
7. Поняття "інформаційний ресурс", "інформаційний продукт" та "інформаційні технології".

8. Національні інформаційні ресурси.
9. Електронні інформаційні ресурси.
10. Право власності на інформаційні ресурси.
11. Обробка і доступ до інформаційних ресурсів.
12. Види засобів захисту інформаційних ресурсів та їх коротка характеристика.
13. Захист від маніпулювання свідомістю.
14. Організаційно-технічний захист інформації.
15. Програмно-технологічний захист даних.

Розділ 5. СИСТЕМАТИЗАЦІЯ ВІДНОСИН В ІНФОРМАЦІЙНІЙ СФЕРІ

5.1. Реформування інформаційного законодавства

5.1.1. Створення системи інформаційного законодавства

Дослідження питань зі створення системи інформаційного законодавства, у напрямі систематизації відносин в інформаційній сфері та кодифікації інформаційного законодавства, здійснюється в Україні з 1997 р., після виходу у світ книги В.А. Копилова "Информационное право" [91].

Ще наприкінці 1990-х рр. за результатами виконання дослідних робіт у Науково-дослідному центрі правової інформатики Академії правових наук України (далі НДЦПІ АПрН України) із застосуванням комп'ютерної інформаційно-аналітичної системи "Законодавство" (у період розробки Концепції реформування законодавства України у сфері інформаційних відносин [54]) було визначено, що інформаційне законодавство становить значний масив нормативно-правових актів (понад 260 законів, 295 постанов Верховної Ради, 380 указів і 90 розпоряджень Президента, 1160 постанов і 210 розпоряджень Кабінету Міністрів, 1500 актів міністерств і відомств, тобто – понад 4000 актів). Цей масив уже тоді вимагав узгодженості, зокрема, у визначенних понятійного апарату, гармонізації норм вітчизняного інформаційного законодавства з відповідними нормами європейських стандартів тощо. Більш того, створення нових нормативно-правових актів постійно вимагало наявності "інформаційного фундаменту", тобто базового, комплексного нормативно-правового акта для всієї інформаційної сфери, який визначав би принципи єдиної системи інформаційного законодавства. Це зумовлювало необхідність систематизації інформаційного законодавства на рівні кодифікації. Така систематизація передбачає не лише зовнішню обробку сукупності існуючого нормативного матеріалу, розташування його у певному порядку та ін. У процесі кодифікації переглядають і виключають застарілі норми, вносять виправлення і усувають протиріччя, заповнюють прогалини у правовому регулюванні, створюють нові правові формули і конструкції, які враховують перспективи розвитку відносин в інформаційній сфері. Тобто кодифікація передбачає можливість оцінити необхідність і намітити напрями правового регулювання, що надає законодавству нової якості та сприяє підвищенню ефективності, зокрема, щодо інформаційно-аналітичного забезпечення діяльності органів влади.

Дослідження нормативно-правових актів щодо інформаційної сфери виявили ряд недоліків, зокрема таких:

- мають місце розбіжності в розумінні структури системи норм у сфері інформаційних відносин. В окремі закони включаються норми, що носять підзаконну нормативно-правову сутність. Відсутність легальної чіткості ієрархічної єдності законів викликає суперечливе трактування і застосування норм у практиці правозастосування, створює колізії та порушення норм закону на користь норм підзаконного акта. Продовжуються дискусії щодо підходів до формування єдиної структури системи правових норм в інформаційному законодавстві;
- чинні нормативно-правові акти у сфері суспільних інформаційних відносин не повною мірою взаємопов'язані між собою і недостатньо гармонізовані з європейськими та іншими міжнародними стандартами;
- нові правові акти нерідко не узгоджені концептуально з раніше прийнятими, що призводить до правового хаосу;

• різні закони і підзаконні акти, що регулюють суспільні відносини, об'єктом яких є інформація, приймалися в різний час без узгодження понятійного апарату. Вони мають ряд термінів, які не досить коректні, не викликають відповідну інформаційну рефлексію або взагалі не мають чіткого гносеологічного наповнення. Наприклад, щодо інформаційних відносин укажемо такі, як юридичні співвідношення: "інформатика" та "інформатизація"; "інформація" і "дані"; "документ" і "документована інформація"; "використання" і "застосування"; "таємна інформація" і "конфіденційна інформація"; "майно" і "власність"; "володіння" і "користування" тощо. Існує законодавча невизначеність дефініцій нових термінів, наприклад, "сайт", "веб-сайт", "веб-сторінка", "портал", "веб-сервер" і т. д. Термінологічна неузгодженість, різне трактування однакових за назвою і формою категорій призводять до їх неоднозначного розуміння і застосування на практиці;

• з погляду проблем інтелектуальної свободи, тобто свободи створювати і поширювати нову інформацію, відсутнє поняття "нова інформація" і відповідна регуляція відносин;

• потребують подальшого осмислення і удосконалення норми авторського права та патентного права у аспекті права промислової власності для е-середовища;

• норми права, які визначають захист персональних даних, потребують гармонізації з положеннями відповідних європейських стандартів, а також розробки і введення правових механізмів реалізації людиною права власності на її персональні дані;

• відсутнє спеціальне законодавче регулювання питань діяльності, пов'язаних із застосуванням Інтернету в комерційних цілях та надання відповідних послуг. Зазначена обставина істотно підвищує інвестиційний ризик і провокує відставання від темпів розвитку електронно-мережної економіки країн, які вже знаходяться в інформаційному суспільстві;

• велика кількість законів і підзаконних актів у сфері інформаційних відносин ускладнює їх пошук, аналіз, правову експертизу і узгодження для практичного застосування та ін.

У середовищі фахівців уже давно сформувалася думка, що сукупність правових норм у сфері суспільних інформаційних відносин, визначених у законах і підзаконних актах, дозріла за кількістю до критичної маси, яка дозволяє здійснити перехід законодавства до нової якості. Це зумовлює можливість виділення їх не тільки в окрему самостійну наукову дисципліну, але й в умовно автономну галузь публічного права — інформаційне право, відповідну легальну її систематизацію на рівні кодифікування усього інформаційного законодавства.

У червні 2000 р. НДЦПІ АПрН України звернувся до Урядової комісії з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади (далі — Урядова комісія), утвореної постановою Кабінету Міністрів України від 07.05.2000 р. № 777, з пропозиціями про внесення до проекту Завдань Національної програми інформатизації на 2001 рік пункту про розробку "Кодексу про інформацію" та розгляду на її засіданні "Концепції реформування законодавства України у сфері суспільних інформаційних відносин" (далі — Концепція) *.

* Відповідно до Закону України "Про авторське право та суміжні права" від 23.12.1993 р. № 3792-XII робота засвідчена Свідоцтвом про реєстрацію авторського права на твір № 25784 від 24.09.2008 р. (заявка від 06.06.2008 р. № 25472). Автори Швець М., Калюжний Р., Брижко В., Гавловський В., Цимбалюк В.

На черговому засіданні, у жовтні 2000 р., Урядова комісія розглянула вказане питання та прийняла Концепцію за основу (Протокол № 7 від 06.10.2000 р.). Її зміст з урахуванням пропозицій та зауважень членів Урядової комісії див у Додатку 2.

Значення втілення у життя Концепції полягає у створенні умов комплексного вирішення проблем державної політики в інформаційній сфері щодо нормативно-правової бази інформаційного суспільства, поступ до якого передбачений Програмою інтеграції України до Європейського Союзу (розділ 13 "Інформаційне суспільство"). Як вважаємо, реалізація положень Концепції може дозволити здійснити більш ефективне та цілеспрямоване упорядкування інформаційних відносин за умов входження України в інформаційне суспільство.

Сьогодні в Україні вже створені не тільки наукові, а й законодавчі засади щодо здійснення систематизації інформаційного законодавства на рівні кодифікованого акта. Так, Законом України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 09.01.2007 р. № 537-V (частина 2, Розділ III. "Національна політика розвитку інформаційного суспільства в Україні") передбачено: "З метою підвищення ефективності розвитку інформаційного суспільства необхідно створити цілісну систему законодавства, гармонізовану з нормами міжнародного права з питань розвитку інформаційного суспільства, зокрема здійснити кодифікацію інформаційного законодавства. …При створенні інформаційного законодавства слід керуватися загальними принципами Конституції України, а також базуватися на принципах свободи створення, отримання, використання та розповсюдження інформації; об'єктивності, достовірності, повноти і точності інформації; гармонізації інтересів людини, суспільства та держави в інформаційній діяльності; обов'язковості публікації інформації, яка має важливе суспільне значення; обмеження доступу до інформації виключно на підставі закону; мінімізації негативного інформаційного впливу та негативних наслідків функціонування ІКТ; недопущення незаконного розповсюдження, використання і порушення цілісності інформації; гармонізації інформаційного законодавства та всієї системи вітчизняного законодавства".

Аналіз упорядкування інформаційних відносин в Україні і в міжнародній практиці дозволяє визначити ряд основних положень на рівні інформаційного законодавства, що виступає публічно-правовою основою інформаційного права:

• предмет правового регулювання – інформаційні відносини;

• об'єкти інформаційних відносин – інформація (знання, відомості) та дані (електронні сигнали й структури в е-просторі, до яких інформація пристосована);

• метод правового регулювання – системне, комплексне застосування методів цивільного, адміністративного і кримінального права (що визначає міжгалузеву сутність публічно-правового регулювання) з урахуванням методів приватноправового регулювання (на рівні угод, добрих звичаїв, традицій, норм суспільної моралі, ділової етики).

Через предмет правового регулювання та міжгалузеві комплексні інститути права інформаційне право має зв'язок з іншими галузями права (зокрема, господарським, трудовим та ін.) і створює з ними складну, велику, агреговану гіперсистему права інформаційного суспільства.

Серед основних напрямів упорядкування та регулювання інформаційних відносин, які складають правове поле інформаційної діяльності, можна виділити наступні:

• визначення і правове закріплення головних напрямів державної інформаційної політики виходячи із загальнолюдських принципів новаці і гуманного ставлення до людини, її честі, гідності, репутації та інших особистих прав;

• забезпечення правового режиму формування і використання національних інформаційних ресурсів щодо збирання, обробки, зберігання та поширення інформації;

• створення системи юридичних процедур реалізації конституційних прав громадян України стосовно гарантій, охорони, захисту їх персональних даних за умов розвитку процесів інформатизації державних органів управління;

• забезпечення умов для розвитку гарантій, охорони і захисту всіх форм власності на інформацію, інформаційні продукти, інформаційні ресурси, інформаційні технології та інформаційні послуги;

• державно-правове сприяння формуванню ринку інформаційних продуктів, інформаційних ресурсів, інформаційно-комп'ютерних технологій, телекомунікаційних мереж та інформаційних послуг з пріоритетами для вітчизняних виробників;

• організація створення державних та регіональних інформаційно-комп'ютерних систем і мереж, забезпечення їх сумісності і взаємодії в єдиному інформаційному просторі України;

• створення реальних умов для якісного і ефективного забезпечення необхідною інформацією громадян, органів державної влади та органів місцевого самоврядування, державних і приватних організацій;

• забезпечення балансу прав і обов'язків людини, суспільства і держави з урахуванням інтересів національної безпеки, невід'ємною складовою якої є інформаційна безпека;

• державне стимулювання та удосконалення механізму залучення інвестицій, розробки і узгодження проектів Національної програми інформатизації і відомчих програм інформатизації (міністерств, комітетів, установ, підприємств, організацій всіх форм власності).

Виходячи із зазначеного нормативно-правовим документом, що структурує, визначає і упорядковує інформаційні відносини, має бути кодифікований акт щодо усієї сфери інформації, інформатики, інформатизації та інформаційної безпеки. Сфера застосування цього кодифікованого акта як складової загального права України стосовно інформаційної діяльності має назву — інформаційне право, а сам кодифікований акт пропонується назвати Кодексом України про інформацію.

Кодекс України про інформацію, як базовий правовий акт, має отримати офіційний статус пріоритетності в системі інформаційного законодавства України, порівняно з усіма іншими нормативно-правовими актами щодо інформаційної сфери, про що необхідно обов'язково зазначити у прикінцевих його положеннях.

5.1.2. Проекти систематизації інформаційного законодавства

На сьогодні відомо про два офіційно запропонованих для розгляду проекти щодо систематизації інформаційного законодавства:

• проект Інформаційного кодексу України, розробник — Державний комітет інформаційної політики, телебачення та радіомовлення України за участю представників міністерств та комітетів, 2001 р., 201 стор.;

• проект модельного Інформаційного кодексу, розробники — О. Баранов, кандидат технічних наук, член Консультативної ради з питань інформатизації при Верховній Раді України, І. Жиляєв, доктор економічних наук, заступник завідувача секретаріату Комітету Верховної Ради України з питань науки і освіти, М. Родіонов, народний депутат України, голова підкомітету з питань інтелектуальної власності та інформатизації Комітету Верховної Ради України з питань науки і освіти, 2005 р., 22 стор.

Проект Інформаційного кодексу України. Складається з двох частин: Загальної, яка має 5 розділів, 2 глави, та Особливої – 13 розділів, 34 глави, і має наступну структуру:

Загальна частина

Розділ I. Предмет (об'єкт) регулювання і суб'єкти інформаційної діяльності
Розділ II. Державне регулювання інформаційної сфери
Розділ III. Використання мови
Розділ IV. Міжнародні відносини в інформаційній сфері
  Глава 1 Міжнародна інформаційна діяльність
  Глава 2 Міжнародне співробітництво у видавничій сфері
Розділ V. Відповідальність за порушення норм цього Кодексу

Особлива частина

Розділ VI. Інформація як предмет правового регулювання
Розділ VII. Правовий режим інформаційної діяльності
Розділ VIII. Діяльність інформаційних агентств
  Глава 1. Діяльність і статус інформаційних агентств
  Глава 2. Порядок заснування, державна реєстрація та припинення діяльності інформаційних агентств
  Глава 3. Статус суб'єктів інформаційних агентств
  Глава 4. Розповсюдження продукції інформаційних агентств
  Глава 5. Особливості відповідальності за порушення цього Кодексу суб'єктами інформаційної діяльності
Розділ IX. Правове регулювання діяльності друкованих засобів масової інформації
  Глава 1. Організація діяльності друкованих засобів масової інформації
  Глава 2. Діяльність редакцій друкованих засобів масової інформації
  Глава 3. Відносини редакції із споживачами
Розділ X. Правові засади функціонування телебачення і радіомовлення
  Глава 1. Основа і заснування телерадіомовних організацій України та ліцензування каналів мовлення
  Глава 2. Організація телерадіомовлення
  Глава 3. Права і обов'язки телерадіоорганізацій та їх працівників
  Глава 4. Права телеглядачів і радіослухачів
  Глава 5. Матеріально-технічна база телерадіоорганізацій
  Глава 6. Правовий режим організації й роботи кабельного і супутникового телебачення
  Глава 7. Супутникове мовлення
  Глава 8. Про систему Суспільного телебачення і радіомовлення України
Розділ XI. Діяльність мережі Інтернет в Україні
  Глава 1. Державна політика України щодо Інтернету
  Глава 2. Застосування державної мови в українському сегменті Інтернету
  Глава 3. Реєстрація мережних засобів масової інформації
  Глава 4. Збір, використання і захист інформації персонального змісту
Розділ XII. Видавнича діяльність
  Глава 1. Особливості видавничої справи
  Глава 2 Організація і здійснення видавничої справи
  Глава 3. Припинення діяльності у видавничій справі та особливості відповідальності суб'єктів видавничої діяльності

Віддаючи належне значній та складній роботі із створення кодексу, маємо зазначити наступне. Основний його недолік у тому, що проект передбачав інкорпорацію чинного законодавства та упорядкування інформаційних відносин в аспекті забезпечення ЗМІ. По суті, було запропоновано здійснити інкорпорацію в обсязі консолідації, тобто здійснити зовнішню обробку нормативного матеріалу і структурувати його згідно з пріоритетами ЗМІ. Кодекс створювався через призму традиційних уявлень про інформацію та інформаційні процеси.

В умовах становлення і розвитку глобальної інфраструктури інформаційного суспільства навряд чи це виправдано і доцільно. Саме на базі поняття "інформатизація та інформатика" має розвиватися інформаційне право. Його фундамент – забезпечення пріоритету прав і основоположних свобод людини. Функціональна спрямованість – виклад стратегії вирішення суспільних проблем щодо інформації, інформатики та інформатизації. Предмет – регулювання взаємовідносин різних суб'єктів в електронно-цифровому інформаційному просторі. Мета – співвідношення прав людини, балансу її прав у суспільстві та державі, а також підтримка інформаційної безпеки України. Крім цього, слід звернути увагу на те, що обсяги продажу продуктів традиційних ЗМІ (газети, журнали, радіо, телебачення) в країнах "великої сімки" не перевищує 5 % всього обсягу інформаційних продуктів та послуг. Основний продаж в інформаційному суспільстві припадає на сферу комп'ютерних програмних продуктів, інтелектуальної власності і науково-технічної інформації (попад 50 % товарообороту).

Одночасно з вказаним, вважаємо що робота здійснена не даремно. Підходи до

створення кодексу, окремі думки та правові формули, що були запропоновані, є досить цікавими та корисними для створення кодифікованого акту, який відповідає потребам упорядкування інформаційних відносин у всьому інформаційно-електронному просторі України. Тому вказаний проект має обов'язково бути взятий до уваги у подальшому.

Проект модельного Інформаційного кодексу. Як вже зазначалось, на початку 2005 р. у Комітеті Верховної Ради України з питань науки і освіти був презентований проект модельного Інформаційного кодексу. У Пояснювальній записці до проекту (*надається на мові оригіналу - від авт.*) зазначалось наступне.

1. Объективные условия необходимости законодательного регулирования общественных отношений в информационной сфере

Отличительной чертой современного мирового социально-экономического развития является возрастание значимости информации. В связи с этим создаются национальные системы законов и подзаконных нормативных актов по правовому регулированию общественных информационных отношений и процесса информатизации, учитывая темпы их развития и проникновения в разные сферы общественной деятельности.

Для упорядочивания и регулирования информационных отношений на государственном уровне возникла необходимость юридически определиться в наиболее актуальных правовых нормах поведения их участников, в том числе предотвращении и борьбе с правонарушениями в информационной сфере. В свою очередь, это обусловило необходимость выделения и фиксации в праве отдельного направления, которое можно определить как информационное право, целью которого является построение эффективной государственной политики в условиях ускоренного внедрения информационно-коммуникационных технологий: создания информационных ресурсов, их распространения, потребления, хранения и защиты, информационной безопасности.

2. Состояние правового регулирования информационных отношений.

Законодательство, регулирующее общественные отношения в информационной сфере, должно содержать:

- правовые нормы, регулирующие общественные отношения в информационной сфере, содержащиеся в Конституции (основные права и гарантии);

- законы, регулирующие общественные отношения по поводу информации как объекта правоотношений и процесса информатизации (об информации, ее отдельных видах (научно-технической, экологической, статистической и др.), о государственной тайне и защите данны в автоматизированных системах, об информатизации и т. п.);

- законы, регулирующие отдельные общественные отношения, возникающие в информационной сфере или по поводу информации (о средствах массовой информации (пресса, телевидение, радиовещание информационные агентства и др.); о статистике; о связи; библиотечном, издательском, музейном и архивном деле; о рекламе и т. п.);

- законы, целью которых является урегулирование различных общественных отношений (по поводу собственности, по поводу предпринимательской деятельности и другое), объектом которых в отдельных случаях выступает информация (об авторском праве и смежных правах, интеллектуальной собственности, защите от недобросовестной конкуренции; о страховании и банках; о культуре, науке, образовании, здравоохранении и другие);

- правовые нормы, направленные на урегулирование общественных отношений в информационной сфере, которые находятся в кодифицированных нормативных актах, а также международных правовых актах.

Информационное право в своем развитии должно отвечать тенденциям, принципам и нормам международного права и иметь примерно следующую структуру:

- нормы Конституции, имеющие отношение к регулированию информационных общественных отношений;

- закон об информации; законы, об открытой информации и информации с ограниченным доступом как объектах правоотношений;

- законы, посвященный вопросам защиты информации и обеспечения информационной безопасности;

- законы, целью которых является урегулирование общественных отношений, возникающих в информационной сфере при осуществлении отдельных информационных процессов;

- нормы кодифицированного законодательства, имеющие информационное содержание.

3. Проблемы правового регулирования информационных отношений

Современное законотворчество в сфере информационных отношений постепенно встает на путь системы общего права. При этом часто не учитывается его специфика, все аспекты правовой доктрины, национальный менталитет населения и другие особенности социального и государственного строя.

В современных условиях законодательная деятельность разных общественных институтов, с точки зрения когнитивного (познавательного) подхода, имеет значительные недостатки:

во-первых, в связи с тем, что разные законы и подзаконные акты, содержащие информационно-правовые нормы, принимались в разные сроки без согласования понятийного аппарата, значительное количество недостаточно корректных терминов, например, «информация», «тайная информация», «тайна», «информация о личности», «персональные данные», «документированная информация», «документ», «собственность», «владение», «автоматизированная система» и т. д.

Терминологические неточности и разное толкование одинаковых по названию и форме понятий и категорий приводят к неоднозначности их понимания и использования на практике, что, в свою очередь, порождает социальные конфликты между участниками информационных отношений,

во-вторых, значительное количество законов и подзаконных нормативных актов в информационной сфере затрудняет их поиск, анализ и согласование;

в-третьих, существуют различия в понимании структуры и состава системы законодательства в сфере информационных отношений и подходов к их формированию. Это создает на практике правоприменения коллизию норм, что является причиной игнорирования норм закона в пользу подзаконных актов;

в-четвертых, новые правовые акты в сфере общественных информационных отношений нередко не согласованы концептуально с ранее принятыми, что приводит к правовому хаосу.

Наиболее эффективным путем разрешения проблемы правового урегулирования общественных отношений в информационной сфере является систематизация норм права, наивысшей формой которого является кодификация. Кодификация в континентальной системе права разрешает избежать вышеназванных недостатков, свойственных системе общего права.

Кодификация признается формой систематизации права, осуществляемая путем его всесторонней переработки, в том числе исключения его устаревших, на практике не применяемых норм, устранения внутренних противоречий, очевидных пробелов, и имеющая своим результатом создание системно взаимосвязанного сводного правового акта, более качественного и прогрессивного. Российский юрист Л.А. Комаровский от-

мечал в XIX ст., что «кодификация призвана не только сводить в одно целое действующее право, но и улучшать его». Н. Коркунов, работавший в то же время, писал, что кодификация может «сообщить праву большую определенность и сделать более удобным его практическое применение». В более поздние времена достаточно подробное определение кодификации дано в ст. 15 Положения о Комиссии международного права как «более точное формулирование и систематизация права в тех областях, где имеются нормы, установленные обширной практикой государств, прецедентами и доктриной» . Наиболее яркими примерами кодификации национального права являются Кодекс Юстиниана; Русская правда; Кодекс династии Тан; Кодекс Наполеона.

4. Научное обеспечение кодификации правовых норм, направленных на урегулирование общественных отношений в информационной сфере и информатизации. Идея кодификации правовых норм, направленных на урегулирование общественных отношений в информационной сфере и информатизации, определена и научно обоснована в современных юридических исследованиях, имеет теоретические наработки.

Однако, в условиях развития информатизации система существующих правовых норм, направленных на урегулирование общественных информационных отношений, требует мониторинга и согласования с новыми социальными отношениями, выявления проблем в этих отношениях с научным обоснованием их решения.

В основу модельного Информационного кодекса необходимо вносить отработанные юридической наукой и проверенные практикой инкорнорированные нормы действующего информационного законодательства. При разработке Кодекса внимание должно быть уделено определению структуры, места юридических норм в системе правового регулирования. Необходимо четко определиться по вопросам:

- объектной, субъектной и территориальной сферы отношений;

- правил поведения и обязательств участников информационных отношений; информации как объекта права собственности и др.

Доктринально определено – как межотраслевой институт, информационное законодательство регулирует общественные отношения в информационной сфере в условиях информатизации.

Среди основных сфер правового регулирования необходимо назвать следующие:

- определение и правовое закрепление ведущих направлений государственной политики информатизации;

- обеспечение соотношения права на информацию и информационную безопасность (в том числе безопасность информации) как составляющую национальной безопасности;

- правовая защита информации (а также правовая регламентация организационной и технической защиты информации), прав и интересов субъектов информационных отношений и процессов информатизации;

- определение угроз информационной безопасности всех сфер деятельности общества;

- обеспечение условий для развития и защиты всех форм собственности на информацию и информационные ресурсы;

- организация и управление созданием и развитием государственных региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве;

- правовое регулирование создания реальных условий для качественного и эффективного обеспечения информационных нужд граждан, органов государственной влас-

ти, местного самоуправления, предприятий, учреждении и организации на основе национальных информационных ресурсов, современных информационных технологий:

- обеспечение реализации конституционных прав граждан и организаций при условии информатизации государственных органов;

- государственно-правовое содействие формирования рынка информационных ресурсов, услуг, информационных систем и технологий;

- государственное стимулирование усовершенствования механизма привлечения инвестиций, разработки и реализации проектов национальной программы информатизации и локальных программ информатизации;

- правовое обеспечение формирования и использования информационных ресурсов на основе создания, сбора, обработки, накопления, сохранения, поиска и предоставления потребителям документированной информации;

- правовое регулирование создания и использования информационных технологий.

Кодекс потенциально имеет широкий спектр сфер правового регулирования, однако особую важность его разработки составляет обеспечение информационной безопасности всех сфер жизнедеятельности общества как комплексного феномена.

Установление круга субъектов информационных правоотношений, их прав и обязанностей, гарантий реализации прав, определение ограничений в осуществлении информационной деятельности и других аспектов, подлежащих законодательному регулированию, регламентация применения организационных и технических средств защиты информации – предупредительные меры защиты информации и обеспечения информационной безопасности. В результате обеспечивается защита прав и законных интересов соответствующих субъектов, а также защита объектов информационных правоотношений.

Таким образом, содержание даже регулятивных, а не только правоохранительных норм сводится к защите и обеспечению безопасности элементов правоотношений, поскольку информационная одновременно обеспечивает возможность осуществления информационных отношений и реализации прав их субъектов. То есть, регулируя весь круг вышеназванных проблем, Кодекс будет являть собой действенный и пригодный к практическому использованию механизм именно обеспечения информационной безопасности. Это обуславливается особенностью правового регулирования общественных информационных отношений – с одной стороны, урегулирование этих отношений на уровне закона позволяет регламентировать способы защиты информации и обеспечивать информационную безопасность, а с другой стороны, Кодекс представляет собой средство нормативно-правовой защиты.

Развитие теоретико-правовой базы практического регулирования информационных отношений необходимо совершенствовать, учитывая передовой зарубежный опыт.

Особенное внимание требуется уделить исследованию недостатков с целью их дальнейшего недопущения в правотворческой и правоприменительной деятельности, предотвращения негативных последствий информатизации.

5. Методологические подходы по формированию Кодекса. Новый подход по правовому регулированию общественных отношений предложен правовой информатикой. Это применение принципов, подходов и методов информатики к разрешению проблем права, а именно правотворчества.

Правотворчество должно основываться на методологии системного подхода – формировании комплексных гиперсистем права. Их образующей системой должен стать Кодекс, который инкорпорирует и развивает нормы и принципы.

Методологической базой разработки Кодекса является юридическая доктрина, касающаяся условного разделения права на отрасли, модель которой выглядит следующим образом:

- основа – конституционное право;

- его положения находят параллельное развитие (в соответствии с методами правового регулирования и защиты прав) в криминальном, административном, гражданском праве.

Разработка проекта Кодекса должна выполняться методом агрегации: совершенствование отдельных правовых норм или создание новых межотраслевых правовых институтов не должно нарушать целостность и назначение Кодекса, а наоборот, улучшать его действенность в целом, создавать новое системное качество, которое не свойственно отдельным его составляющим.

Цель Кодекса. Проект Кодекса регулирует общественные информационные отношения. При подготовке проекта Кодекса были учтены нормы международных правовых актов, регулирующих отношения в информационной сфере, опыт законотворческой и правоприменительной практики в этой области. Проект Кодекса ориентирован на совершенствование существующего законодательства в сфере информации и уточнение его положений.

Ведущими функциями и задачами Кодекса являются:

- регулятивная – определение прав и обязанностей субъектов в контексте доминирующей методологии и доктрины современного конституционного права и наиболее эффективных разработок международного права в информационной сфере;

- нормативная – определение норм, правил поведения субъектов информационных отношений;

- охранительная – определение гарантий и границ правомерного поведения, когда действия создают правонарушения (деликты), и ответственности за их деяния в соответствии с нормами криминального, административного, трудового и гражданского права;

- интегративная – системное совмещение комплекса определенных юридических норм, регулирующих информационные отношения;

- объединяющая – построение взаимозависимостей между ведущими традиционными отраслями права по применению их методов правового регулирования в информационной сфере;

- коммуникативная – упоминание в отдельных статьях ссылок (если необходимо не создавать большого количества бланкетных норм) на действующие законодательные акты или будущие, необходимость в которых может возникнуть.

Исходные положения примерной структуры проекта Кодекса. В соответствии с традициями кодификации Кодекс должен состоять из двух частей:

Общая часть (Книга 1. Общие положения);

Особенная часть (Книга 2. Информационные отношения).

Книга 3. Информационно-инфраструктурные отношения.

Книга 4. Информационная безопасность).

Каждая из книг разделяется на разделы. Разделы состоят из отдельных статей.

Структура статьи состоит, как правило, из гипотезы и диспозиции. В статьях, где говорится о правонарушениях, необходима обязательная ссылка на вид ответственности в соответствии с Гражданским кодексом, Кодексом законов о труде, Кодексом об административных правонарушениях, Криминальным кодексом, а также на конкретные статьи (при необходимости). Это обуславливает необходимость параллельной доработ-

ки норм соответствующих кодексов, в первую очередь это касается Кодекса об административных правонарушениях и Криминального кодекса (в последнем вообще необходимо создать отдельную главу по информационным преступлениям).

Основные положения содержания частей Кодекса.

В основу первой части входят положения Конституции, ратифицированных международных соглашений, законов об информации. Она включает основы информационного законодательства:

- задачи Кодекса; сфера действия Кодекса;
- определение иерархической системы правового регулирования информационных отношений; определение понятий информации и информатизации, информационных отношений, других терминов;
- основные принципы информационных отношений, язык информационных отношений; государственная политика в сфере информационных отношений и информатизации; субъекты и объекты информационных отношений; информационная деятельность и ее виды; основные положения, касающиеся обязанностей в информационных отношениях.

В состав общих положений Кодекса включаются разделы, составляющие комплекс правовых норм: по действию и применению норм международного права, относительно системы способов защиты прав в информационных отношениях (главы по инкорпорации обозначенных в Конституции способов самозащиты, способов защиты в административно-правовом и криминально-правовом порядке, судебной защиты в гражданско-правовом порядке; защиты через органы государственной исполнительной власти, прокуратуры, уполномоченного по правам человека при парламенте; способов и порядка обращения за защитой к международным организациям и судам). Также необходимо положения последнего раздела включить в содержание раздела по вопросам информационной безопасности (или защиты информации и прав субъектов информационных отношений).

Структурно первая книга «Общие положения» состоит из 2 разделов, 5 глав, 19 статей.

Положения по отдельным видам или категориям информации, а также отдельных средств информатизации, которые имеют специфику, конкретизируются в нормах особенной части Кодекса. В этой части содержатся правовые нормы, регулирующие специфические подсистемы информационных отношений, с указанием из системообразующих законов, а именно (наиболее общий вид, который конкретизируется в соответствующих разделах Кодекса):

- открытая информация (в том числе и правовая);
- информация с ограниченным доступом;
- информация о личности;
- средства информатизации;
- международный информационный обмен;
- обеспечение информационной безопасности (правовое, а также правовая регламентация организационного и технического обеспечения).

В этой части речь идет о системе угроз информационной безопасности, а также о защите информации и прав субъектов информационных отношений (более узкое понимание обеспечения информационной безопасности), поскольку фактически весь Кодекс – правовое обеспечение информационной безопасности при осуществлении не только правоохранительной, но и регулятивной и других функций, что, соответственно, может повлиять и на название Кодекса – Кодекс об информационной безопасности).

Структурно вторая книга «Информационные отношения» состоит из 2 разделов, 9 глав, 36 статей. Предполагается дальнейшая разработка книги 3 «Информационно-инфраструктурные отношения», состоящей из трех разделов и 25 глав, и книги 4 «Информационная безопасность», состоящей из 5 глав.

В случае определения новых сфер регулирования информационных отношений в Кодексе (методом агрегации) вводятся новые разделы, главы. При принятии Кодекса это обязательно должно учитываться в дальнейшей разработке законопроектов в информационной сфере (желательно не как проектов отдельных законов, а соответствующих разделов или глав Кодекса).

Віддаючи належне складній, великій, системній та цікавій роботі із створення проекту модельного Інформаційного кодексу, підкреслимо його, на наш погляд, особливість, яка полягає у тому, що інформаційне право має базуватися на таких видах відносин (див. [183]):

• інформаційні відносини – це суспільні відносини, що мають місце в процесі створення, поширення, використання, збереження і знищення (утилізації) інформації;

• інформаційно-інфраструктурні відносини – це суспільні відносини, що мають місце в процесі забезпечення реалізації інформаційних відносин, тобто пов'язані з функціонуванням суб'єктів інформаційної інфраструктури, які надають інформаційні послуги і виконують роботи в інформаційній сфері, використовують інформаційні технології і ресурси, забезпечують інформаційну безпеку тощо.

5.2. Методологія кодифікації інформаційного законодавства

5.2.1. Основи кодифікації

Методологічною основою кодифікації та створення проекту Кодексу України про інформацію (далі – Кодекс) є юридична доктрина умовного визначення інформаційного права України як галузі права, яка екстраполюється на всю загальну систему законодавства України на основі наступної принципової моделі:

* основа – конституційне право (Конституція України), з урахуванням положень міжнародних стандартів щодо інформаційної сфери;

* конституційні положення знаходять розвиток (відповідно до методів правового регулювання, охорони і захисту прав) в адміністративному, цивільному, кримінальному праві та інших підсистемах національного права України, в яких інформація виступає як додатковий (факультативний) предмет регулювання;

* Кодекс – нормативний акт, що відображає нормативно-правову сутність інформаційних відносин, більша частина їх норм має загальносистемні ознаки стосовно інформації та інформаційної діяльності в умовах розвитку інформаційного суспільства.

Мета Кодексу визначається відповідно до теорії системи цілей. Вона передбачає правове упорядкування відносин між суб'єктами стосовно інформації в різних формах її об'єктивного виразу (різноманітних творах, результатах інтелектуальної діяльності тощо) незалежно від сфери (або галузі) відносин, матеріальних носіїв інформації (паперових, електронних і т. п.) і технології фіксації (букви, цифри, сигнали, структури).

Напрями, підцілі, завдання Кодексу повинні формуватися відповідно до теорії системи підцілей ("дерева цілей").

Основними функціями Кодексу є:

* регулятивна – формулювання прав і обов'язків суб'єктів стосовно інформації;

* нормативна – формування правил поведінки суб'єктів інформаційних відносин;

* охоронна – формулювання гарантій і меж правомірної поведінки, за якими дії можуть створювати правопорушення (делікти), які визначають відповідальність згідно з нормами цивільного, адміністративного або кримінального права;

* захисна – визначати процедури захисту права на інформацію;

* інтегративна – системне поєднання комплексу певних юридичних норм, які регулюють інформаційні відносини в Україні, тобто Кодекс має стати об'єднувальною ланкою провідних традиційних галузей права щодо застосування їх методів у сфері інформаційних відносин;

* комунікативна (інформативна) – посилання в окремих статтях на існуючі галузі законодавства, які є системоутворювальними в різних міжгалузевих інститутах права у певному галузевому правовому полі суспільних відносин.

Серед головних завдань Кодексу можна вказати наступні:

• визначення консенсусу в суспільних відносинах, у сфері інформаційної діяльності, узгодженості, порозуміння у застосуванні юридичних норм, правомірної поведінки учасників інформаційних відносин в інформаційній сфері;

• захист інформації, даних від несанкціонованого доступу, правопорушень (знищення, модифікації, перекручення і т. д.);

• підтримка інформаційної безпеки України у її провідних складових: захисту людини, громадян, їх об'єднань, суспільства і держави (як складових національної безпеки України та безпеки відповідно до міжнародних угод держави).

До основних категорій в інформаційній сфері можна віднести:

• *об'єкти правового упорядкування та регулювання* – це суспільні відносини, які виникають, змінюються та припиняються при реалізації і забезпеченні процесів інформаційної діяльності особи, суспільства і держави.

Для інформаційної сфери поняття "суспільні відносини" визначає дві групи відносин: "інформаційні відносини" та "інформаційно-інфраструктурні відносини". До першої групи відносяться ті відносини, які пов'язані із збиранням, зберіганням, обробкою, використанням, поширенням та знищенням інформації (щодо традиційних видів інформаційної діяльності), а до другої – які пов'язані із процесами функціонування інформаційної інфраструктури та відповідною діяльністю суб'єктів у зв'язку із застосуванням новітніх, зокрема, інформаційно-комп'ютерних технологій;

• *об'єкти (предмети) суспільних відносин в інформаційній сфері* – це інформація (вторинна, похідна), дані, нова інформація, інформаційний продукт, інформаційний ресурс, інформаційна технологія, інформаційна послуга, документ, електронний документ, електронний документообіг та інші результати інформаційної діяльності.

Термін "інформація" стосується явищ, подій та їх властивостей, за якими виникають суспільні відносини, що визначаються поняттям "інформаційні відносини".

Термін "дані" стосується явищ, подій та їх властивостей, за якими виникають відносини, що визначаються поняттям "інформаційно-інфраструктурні відносини".

Пропонується також такі ключові дефініції для інформаційної сфери:

інформація – повідомлення про будь-які відомості чи сукупність відомостей щодо фактів або особистих уявлень. *Факти* – це дійсні, реальні події та явища;

інформація нова (знання) – документовані або публічно оголошені відомості про події та явища щодо особи, суспільства, держави та навколишнього природного середовища, зміст яких має інтелектуальне самовираження і не може бути наперед відомий чи передбачений їх одержувачем;

– *інформація масова* (щодо засобів масової інформації) – документовані або публічно оголошені відомості про події та явища, що відобуваються у суспільстві, державі та навколишньому природному середовищі;

– *дані* – це електронні сигнали, коди або структури щодо повідомлень на матеріальному носії, до яких інформація пристосована (прикріплена);

– *інформаційний продукт* – це закріплена на носії інформація, підготовлена для економічного обігу у відповідній технологічній формі обробки, поширення за допомогою певної технічної мережі передачі даних (телекомунікації);

– *інформаційний ресурс* – це організовані в базах даних інформаційні продукти, які мають ретроспективний зміст стосовно господарського та негосподарського їх обігу, необхідні для задоволення інформаційних потреб особи, суспільства і держави;

інформаційна технологія – комплекс методів, способів і засобів обробки інформації (даних) щодо її пошуку, збирання (придбання), реєстрації, накопичення, зберігання (знищення), використання та поширення (реалізації), охорони, захисту і відображення, у тому числі за допомогою автоматизованих систем і мереж передачі даних;

інформаційна послуга – вид інформаційної діяльності з метою задоволення інформаційних потреб певних суб'єктів інформаційних відносин.

• *суб'єкти відносин в інформаційній сфері* – це фізичні і юридичні особи, об'єднання громадян, органи державної влади, інші держави і міжнародні організації з визначеним їх правовим статусом стосовно інформаційних відносин.

Щодо інформатизації, то виділяють три групи суб'єктів інформаційних відносин:

- *перша група:* особи, що створюють електронно-цифрову, програмно-технічну частину інформаційної інфраструктури (включаючи засоби зв'язку, телекомунікацій), забезпечують її експлуатацію, розвиток. Це: розробники і створювачі електронних мереж, у тому числі їх технічних засобів, засобів зв'язку, телекомунікацій, комп'ютерних програмних засобів різного рівня і призначення, іншого устаткування, що складає інформаційну інфраструктуру;
- *друга група:* особи, що надають інформаційні послуги. У число суб'єктів групи входять фахівці, що створюють вихідну інформацію, формують інформаційні ресурси, наповнюють бази даних і надають споживачам можливість підключитися до електронних мереж телекомунікації;
- *третя група:* споживачі інформаційних ресурсів, тобто невизначене велике коло суб'єктів (користувачів, споживачів), що підключаються до мереж телекомунікації для одержання необхідної їм інформації і застосування її у власній діяльності.

Суб'єктний зміст інформаційних відносин щодо майнових прав пропонується наступний:

суб'єкти права власності на інформацію (дані), інформаційний продукт, інформаційний ресурс, інформаційну технологію, інформаційну послугу – це власники, володільці, розпорядники та користувачі інформації (даними), як різновиду майна, незалежно від носіїв інформації, інформаційних технологій, доменних імен тощо, та інші учасники інформаційних відносин.

Об'єктну складову інформаційних відносин пропонується розглядати наступним чином:

види інформаційної діяльності – створення, пошук, збирання, обробка, накопичення, зберігання, поширення, реалізація, охорона і захист прав на інформацію, дані,

інформаційний продукт, інформаційний ресурс, інформаційна технологія, інформаційну послугу тощо;

сфери, що пов'язані з інформаційними правовідносинами – духовна (культурна); фінансова; господарська (економічна); політична; наукова; науково-технічна; науково-технологічна; екологічна; статистична; міжнародна; охорони та захисту інформаційних інтересів особи, суспільства, держави та ін.

При аналізі структурованості і цілісності правового упорядкування інформаційних відносин варто враховувати інформаційну сутність традиційних правовідносин, те, що норми інформаційного законодавства немов пронизують усю правову систему України як по вертикалі (по видах нормативно-правових актів), так і по горизонталі (по галузях суспільних відносин). При цьому не повинно здійснюватися "вторгнення" в зазначені традиційні сфери правовідносин. Інформаційне законодавство щодо цих сфер повинно мати нормативно визначений гіперзв'язок з ними у формі бланкетних, інформаційних (декларативних) норм.

"Вертикальна" структура законодавства створюється виходячи з принципу ієрархії законів: норми вищого за ієрархією акта мають більшу юридичну чинність і є визначальними для відповідних норм нижчих, підзаконних нормативно-правових актів. Необхідність ієрархії актів зумовлюється тим, що на практиці реалізація правових норм законодавства нерідко вимагає прийняття оперативних правових актів Президентом чи урядом України або відомчих, нижчих за ієрархією нормативних актів. Ця система доповнюється актами органів місцевої виконавчої влади в конкретних умовах їх діяльності з метою виконання норм вищих за ієрархією правового регулювання нормативно-правових актів.

"Горизонтальна" структура законодавства створюється виходячи з того, що вона містить у собі не тільки норми, які входять до блоку предметних, спеціальних нормативно-правових актів, а й норми провідних галузей законодавства України, зокрема конституційного, адміністративного, цивільного, кримінального галузей.

Повноту правового регулювання можна очікувати тільки в тому випадку, коли інформаційно-правові норми "перекриють" наведені у матриці відносини, що підлягають правовому регулюванню в інформаційній сфері (див. Додаток 6).

Сьогодні інформація вже не тільки засіб забезпечення потреб у інформуванні. Вона все більше стає самостійним ресурсом економіки та всього громадського життя, що вимагає більш уважного ставлення з точки зору наявності у ній якості об'єкта права власності, який має відповідного власника, що безпосередньо притаманне інституту права власності. Це додає їй суспільну вагомість, а відтак можливості більш ефективного (справедливого) регулювання суспільних майнових відносин. Сказане грунтується на тому, що в інформаційному суспільстві інформаційний ресурс є різновидом майна, а отже, одним із головних засобів задоволення життєвих потреб людини, діяльності суспільства і держави.

Технологічно розробка проекту Кодексу має здійснюватися методом агрегації: удосконалення окремих правових норм або створення нових міжгалузевих правових інститутів, які не порушують цілісності і призначення інших інститутів. Напрями, підцілі, завдання Кодексу повинні формуватися відповідно до теорії системи підцілей ("дерева цілей").

Структурно проект Кодексу може складатися з чотирьох частин: преамбули, загальної, особливої і спеціальної (прикінцевих положень).

Преамбула. Акцентує увагу на сутності і змісті інформаційного суспільства, його розвитку в Україні, розвитку національного інформаційного простору на основі сучасних технологій, його суспільних переваг і нових загроз Національній інформаційній безпеці України.

Частина І (загальна). Включає загальні положення та положення, які притаманні основним сферам упорядкування інформаційної діяльності, де визначаються:

* мета інформаційного законодавства (законодавства про інформацію, інформаційну діяльність) – упорядкування, регулювання, охорона та захист інформаційних відносин, їх виникнення, здійснення, зміни та припинення в інформаційній діяльності, а також законних прав учасників цієї діяльності та обов'язків суб'єктів суспільних відносин;

* завдання інформаційного законодавства: забезпечення правовими засобами державних гарантій, охорони і захисту прав людини на інформацію, у тому числі охорону і захист суспільно корисної інформації та захист від аморальної, суспільно небезпечної інформації, а також дотримання балансу прав людини, суспільства і держави в умовах розвитку в Україні інформаційного суспільства;

* сфера дії кодексу (його правове поле);

* основні поняття (при цьому пропонується уникати визначення понять, які становлять об'єкти, суб'єкти та зміст інформаційних правовідносин, зокрема таких, як інформація, інформатика, інформатизація, мова інформаційних відносин і т. п.);

* система правового регулювання інформаційних відносин;

* основні принципи інформаційних відносин;

* суб'єкти відносин (їх основні права і обов'язки);

* об'єкти відносин (інформація (вторинна, похідна), дані, нова інформація, інформаційний продукт, інформаційний ресурс, інформаційна технологія, інформаційна послуга тощо);

* галузі, види, джерела інформації, інформаційних продуктів, інформаційних ресурсів;

* інформаційна діяльність, її види та основи правового режиму інформації, інформаційних продуктів та інформаційних ресурсів, доступу до них;

* права власності на інформацію (інформаційні продукти, інформаційні ресурси, надані інформаційні послуги) як різновид майна;

* забезпечення інтелектуальної свободи;

* інформаційні технології і електронні засоби телекомунікаційного забезпечення;

* правове регулювання стосовно інформаційної безпеки;

* охорона прав в інформаційних відносинах;

* гарантії держави для забезпечення прав суб'єктів інформаційних відносин і принципи стратегії державної політики в інформаційній сфері;

* захист прав в інформаційних відносинах (адміністративним, цивільним, трудовим, кримінальним законодавством через відповідні органи влади, судовий захист; можливості звернення в спеціалізовані міжнародні органи із захисту прав людини);

* міжнародне співробітництво (транскордонне переміщення інформації і даних, підтримка інформаційних потреб громадян, які знаходяться за кордоном тощо).

У цій частині повинні бути відображені основні засади комплексних інформаційних відносин, які врегульовані на рівні спеціального законодавства (з вказівкою їх системоутворювальних законодавчих актів), зокрема: державна, комерційна і професійна таємниці; роль державних технічних стандартів як нормативно-правових актів та доступ до їх змісту тощо.

Частина ІІ (особлива). Має включати підсистеми (інститути) інформаційних відносин, які мають специфічні ознаки і вже визнані як спеціальні сфери інформаційної діяльності на рівні спеціального законодавства. У названій частині визначаються поло-

ження, які є складовими державної інформаційної політики і мають істотні між собою відмінності з погляду цільового призначення і застосування інформаційних ресурсів. Структуризація цієї частини пропонується методом гіперсистем. Ієрархія ключових чинників систематизації повинна здійснюватися в наступній послідовності, а саме: суб'єктні, потім об'єктні ознаки.

Суб'єктні ознаки становлять: права, свободи та інтереси людини, громадянина у сфері інформації, інформаційної діяльності, за ними права суспільства, громадських організацій, громадського порядку, за ними права та обов'язки держави в інформаційній сфері.

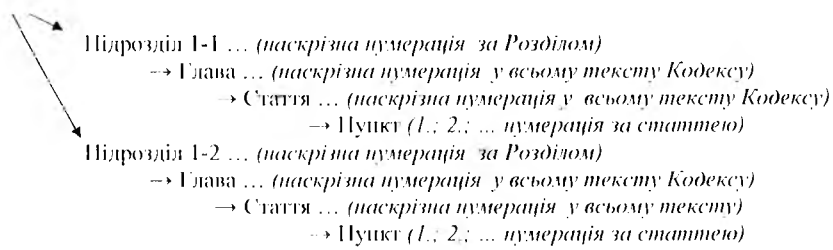
За об'єктними ознаками пропонується така систематизація діяльності:

* відносини у сфері засобів масової інформації (видавнича справа, друковані засоби масової інформації, телебачення, радіомовлення, кінематограф, Інтернет тощо);
* відносини у сфері науки, науково-технічної діяльності та освіти;
* відносини у сфері інформатизації та національної програми інформатизації;
* інші сфери інформаційної діяльності.

У разі виникнення потреб у визначенні нових сфер правових відносин вони також можуть бути відзеркалені у частині кодексу щодо іншої сфери інформаційної діяльності. Серед таких можуть бути у перспективі виділені відносини, що стосуються захисту персональних даних, електронної комерції, електронного урядування та ін.

Ієрархія частин кодексу може бути такою:

Частина …
Розділ 1



Структурно кодекс може бути створений на базі методу побудови предметно-систематичного каталогу (гіперсистеми) відповідно до ієрархії: галузь, підгалузь, інститут права, предметний напрям, предметні компоненти виходячи з родових властивостей інститутів правовідносин, і поділятися на частини, розділи, підрозділи, глави, статті (нумерація – наскрізна). При відповідному обсязі статей і необхідності може бути здійснена структуризація у такій формі, як книга кодексу, яка буде акумулювати відповідні інформаційні відносини та мати, за необхідності, свою структурну ієрархію.

Структура статті повинна складатися з чіткого визначення диспозиції (прав та обов'язків учасників правовідносин). Окремі статті можуть містити прив'язки (посилання) до норм іншого законодавства України, відносно до якого створюється нова підсистема, інститут права.

В окремій статті повинен визначатися гіперзв'язок стосовно правопорушень у інформаційній сфері – посилання на делікті складові провідних галузей публічного права: до Цивільного кодексу, Кодексу законів про працю, Кодексу про адміністративні правопорушення, Кримінального кодексу. Ці кодекси доповнюються нормами щодо

відповідальності за правопорушення інформаційних відносин, із посиланням на норми Кодексу, особливо стосовно визначення змісту понять, термінів, їх дефініцій.

Прикінцеві положення. Мають включати положення, які визначають термін введення Кодексу в дію, законодавчі акти, які втрачають чинність у зв'язку з прийняттям і набуттям чинності цим кодексом, та інше.

Як зазначалося у п. 5.1.1., дуже важливим є те, що у прикінцевих положеннях має бути визначений статус Кодексу, як базового правового акту в системі законодавства України, по відношенню до всіх інших нормативних актів в інформаційній сфери.

Незважаючи на надану деталізацію підходів до систематизації інформаційного законодавства, вважаємо, що проблема практичної розробки кодексу є завданням надзвичайно складним і трудовитратним. Особливо обережно слід ставитися до того, щоб не втрутитися у сферу інших галузей права.

5.2.2. Структуризація норм щодо інформаційних відносин

Найбільш складним питанням щодо створення Кодексу є визначення методики структуризації норм інформаційних відносин. Можна почати діяти по-різному, зокрема за методикою створення проектів, визначених у підрозділі 5.1.1.

Так, проект Інформаційного кодексу Держкомтелерадіо України створювався завдяки залученню пропозицій відомств щодо упорядкування відносин у їх сферах відповідальності (видавничій справі, телерадіомовленні та кінематографії, бібліотечній, архівній та музейній справах тощо) які, по-суті не вносили ніяких змін до чинного законодавства і розміщувались в одному збірнику, який отримав назву кодексу.

В основу проекту модельного Інформаційного кодексу покладена ідея нового підходу до класифікації інформаційних відносин у правовому регулюванні, тобто розмежування відносин на "інформаційні відносини" та "інформаційно-структурні відносини". Далі, на основі юридичних та технічних знань та досвіду авторів, використовуючи відомі структурні схеми побудови нормативних актів щодо інформації, був створений законопроект, який, на наш погляд, вийшов достатньо змістовним і гармонійним і про який можна з повною підставою сказати, що проект заслуговує на особливу увагу.

Проте є деякі зауваження й до цього проекту. Вони стосуються його дещо декларативності, відсутності механізмів (або посилання на механізми) реалізації положень та уявлень про необхідність більшої деталізації окремих складових, як це зроблено, наприклад, у Цивільному кодексі України. До речі, цей кодекс розроблявся вченими вищої кваліфікації (на що з бюджету було виділено 8 млн. грн.) протягом багатьох років та на базі положень Цивільного кодексу УРСР, тобто було на що "спиратися". З кодексом щодо інформаційної сфери справи інші – аналогів його створення нема, за винятком того, що зазначено у цій роботі.

З початку 2000-х рр. НДЦЦП АПрН України неодноразово звертався до різних органів влади з пропозицією розпочати під державним патронатом роботу щодо систематизації інформаційного законодавства України та створення відповідного кодексу. Проте складність систематизації всієї інформаційної бази держави, про що свідчить обсяг інформаційного законодавства України (за попередніми розрахунками, це понад 4000 документів), масштабність роботи (яка потребує інтелектуальних та трудових ресурсів) та відсутність коштів, не дозволяють вирішити завдання, яке затверджено до виконання, зокрема, Законом України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 09.01.2007 р. № 537-V.

У 2007 р. у ПДЦІП АПрН України була створена ініціативна група (з докторів та кандидатів наук) для виконання зазначеної роботи, члени якої погодилися із попередньою структурою проекту Кодексу, яка визначена наступним чином:

Преамбула

Частина І. Загальна частина

Розділ 1. Загальні положення
Розділ 2. Державна інформаційна політика
Розділ 3. Суб'єкти інформаційних відносин
Розділ 4. Об'єкти інформаційних відносин
Розділ 5. Галузі, джерела інформації, інформаційних продуктів, інформаційних ресурсів
Розділ 6. Інформаційна діяльність та її види
Розділ 7. Інформаційні послуги
Розділ 8. Інформаційні ресурси
Розділ 9. Інформаційні системи, інформаційні технології і засоби забезпечення
Розділ 10. Інформаційне забезпечення інтелектуальної свободи
Розділ 11. Підтримка інформаційної безпеки
Розділ 12. Охорона прав в інформаційних відносинах
Розділ 13. Захист прав в інформаційних відносинах
Розділ 14. Дія та застосування норм міжнародного права

Частина ІІ. Особлива частина

Розділ 15. Основні інститути інформаційного права
Глава 15-1. Засоби масової інформації
Глава 15-2. Наука та освіта
Глава 15-3. Інформатизація та Національна програма інформатизації
Розділ 16. Інші інститути інформаційного права
Глава 16-1. Захист персональних даних
Глава 16-2. Зв'язок та телекомунікації
Глава 16-3. Електронні документи, електронний цифровий підпис та електронний документообіг
Глава 16-4. Дистанційне навчання
Глава 16-5. Телемедицина
Глава 16-6. Електронна торгівля (комерція)
Глава 16-7. Електронне урядування
Глава 16-8. Бібліотечна та архівна справа
Глава 16-9. Державні інформаційні стандарти
Глава 16-10. Комерційна та державна таємниця

Частина ІІІ. Заключна частина

Прикінцеві та перехідні положення

Структура та методика створення проекту Кодексу України про інформацію може бути й дещо іншою. Це потребує більш кропіткої технічної та аналітико-синтетичної роботи. Проте при цьому, як вважаємо, можуть бути отримані деякі переваги з погляду наочності, системності в порівнянні правових формул і зменшення помилок у результатах роботи, а також можливості у визначенні прогалин у правовому регулюванні.

В основу структуризації норм інформаційних відносин має бути покладена так звана матриця положень (статей) основних законів України в інформаційній сфері та положень у наявних сьогодні проектах кодексів, про які йшлося вище. Приклад створення структури матриці див. у Додатку 4.

Вказана вище загальна структура була вписана у ліву колонку (боковик). Вона поповнювалась (деталізувалась) завдяки положенням законів та проектів концепцій. У зв'язку з обмеженістю місця у Додатку 4 наведені лише деякі закони, перелік положень щодо інших законів може бути продовжений завдяки збільшенню колонок справа (граф). Загальне завдання щодо структуризації інформаційних відносин полягає у створенні, так би мовити, "скелету" Кодексу, який поступово має наповнюватися, змінюватися, при необхідності, та удосконалюватися. Робота має враховувати те, що у подальшому обов'язково з'явиться необхідність у розширенні статей до глав або введення нових розділів, підрозділів глав, статей тощо.

Складним завданням, яке можливо виконати лише завдяки розумовій діяльності дослідника, є зіставлення норм, аналітико-синтетична та лінгвістична оцінка термінів, правових формул з метою узгодженості та відповідності їх змісту єдиним принципам правового регулювання відносин в інформаційній сфері. Ця робота має обов'язково враховувати напрацювання та узагальнення за суттєвими ознаками певного матеріалу щодо інформаційного права, який одержав системно-структурне оформлення у вигляді схем та таблиць, які розроблено нами у продовж 1997 – 2008 рр., таких як:

- загальна структура інформаційного права – див. Додаток 1;
- Концепція реформування законодавства України у сфері суспільних інформаційних відносин – див. Додаток 2;
- структурна схема – Інформаційні війни: види, зміст, зброя, засоби нападу та захисту – див. Додаток 3;
- матриця положень (статей) основних законів України в інформаційній сфері та положень у проектах кодексів – див. Додаток 4;
- класифікація предметних областей в інформаційній сфері – див. Додаток 5;
- матриця упорядкування відносин в інформаційній сфері – див. Додаток 6;
- структурна схема щодо інформаційних ресурсів – див. Додаток 7;
- структурна схема щодо інформаційної інфраструктури – див. Додаток 8;
- структурна схема щодо індустрії інформації – див. Додаток 9;
- структурна схема щодо захисту інформації та даних – див. Додаток 10;
- структурна схема щодо інформаційної безпеки – див. Додаток 11.

Крім вищезазначеного є ще завдання, яке полягає у необхідності порівняння положень кодексу із положеннями європейських стандартів, що має здійснюватися за допомогою інформаційно-пошукових систем та комп'ютерних технологій.

5.2.3. Порівняння законодавства України з європейським законодавством

Загальнодержавна програма адаптації законодавства України до європейського законодавства є пріоритетною складовою процесу інтеграції України в ЄС та передбачена рядом нормативно-правових актів України [81, с. 7-10; 240, с. 58-63].

Інформаційне законодавство України складає великий масив нормативно-правових актів. Порівняльний аналіз їх з актами країн РС та ЄС може зайняти багато часу, якщо це здійснюватиметься традиційними методами та засобами. Щоб скоротити час відпрацювання документів і збільшити ефективність роботи в нормотворчій діяльності необхідне створення відповідної інформаційно-пошукової системи (далі – ІПС) із залу-

ченням сучасних комп'ютерних та телекомунікаційних технологій. Проект такої системи, що отримав назву ІПС порівняння нормативно-правових документів – "Матриця інформаційного законодавства", був розроблений у НДЦПІ АПрН України та пройшов відповідну апробацію [241] *.

Процес проведення порівняльного аналізу виконується за допомогою певної кількості програмних блоків (модулів), які пов'язані між собою. Загальний вигляд функціональної схеми, де наведені програмні блоки та їх зв'язки, подається на Рис. 5.1.

Рис. 5.1.

* Відповідно до Закону України "Про авторське право та суміжні права" від 23.12.1993 р. № 3792-XII робота засвідчена Свідоцтвом про реєстрацію авторського права на твір № 12208 від 08.02.2005 р. (заявка від 16.12.2004 р. № 12119). Авт.: Базанов О., Базанов Ю., Брижко В., Швець М.

Центральним блоком зазначеної системи є "Матриця інформаційного законодавства". Вона складається з двох модулів: перший модуль під назвою "Модуль зберігання документів українською мовою", який є базою даних всіх документів, що потрапили в поле зору фахівців, які досліджують якусь певну порівняльну тематику, та другий модуль – "Модуль пошуку документів для порівняльного аналізу". Всі інші блоки, що наведені в схемі, виконують роль допоміжних і забезпечують роботу центрального блоку. Вони є в комп'ютеризованій інформаційно-аналітичній системі Верховної Ради України [242, с. 6]. Розглянемо більш детально окремі блоки.

Інформаційно-пошуковий тезаурус EUROVOC. Спеціально розроблений для роботи з документальною інформацією, якою володіють бібліотеки та відділ офіційних публікацій Європейського Парламенту, служби документації та бази даних інституцій Європейського Союзу [244]. Мета створення – індексування документів та виконання автоматизованого пошуку різними мовами, за умов еквівалентності понять (дескрипторів) щодо кожної з національних (природних) мов. Тезаурус допомагає у визначенні предметної суті документів, виборі термінів, сукупність яких стисло передає зміст, зазначення відношень між поняттями, що визначаються цими термінами. Традиційно при написанні документів автори вільно використовують засоби природної мови. Водночас людина, яка бажає знайти певний документ, може зіткнутися з труднощами, пов'язаними з тим, що одне й те саме поняття може бути виражене низкою синонімів або понять, які частково збігаються, один і той же термін може мати різні значення. Використання тезауруса виключає багатозначність та надає можливість отримати загальну інформацію про термінологічний апарат та структуру предметної області.

Програми автоматизованого перекладу текстів документів на українську мову. Існують різні програми, які здійснюють переклад текстів з європейських мов на російську (Promt XT, Socrat тощо). Після використання цих програм можна перекладати тексти з російської мови на українську за допомогою програм Play або Pragma, за допомогою якої є можливість перекладати тексти з англійської мови на українську. Проте на сьогодні програми автоматизованого перекладу працюють незадовільно. В більшості випадків переклад здійснюється дослівно, не враховуються лінгвістичні відмінності кожної мови. Словники цих програм не використовують знання перекладачів, які закладені в ПТТ EUROVOC.

Бази даних країн Європи та СНД. Це різні сховища інформації, з яких можна отримати тексти документів мовами їх видання. Сховищами інформації можуть бути бази даних на електронних паконичувачах, книгах, журналах та інше. Роботи, що пов'язані із застосуванням автоматизованих засобів, потребують первинних документів в електронному вигляді.

Для виконання порівняльного аналізу запропоновано наступний алгоритм пошуку документів країн Європи та країн СНД за допомогою автоматизованих систем. Послідовність операцій, які потребують виконання, наведена на Рис. 5.2.

На першому етапі користувач формулює термін, ключове слово (дескриптор), що визначає поняття. Це необхідно виконати для того, щоб окреслити область, предметне коло пошуку документів щодо яких буде виконуватись аналіз. В електронному вигляді цей запит надсилається до ІПС "Термінологія законодавства України". На даному етапі користувач уточнює свій запит відповідно до мовних вимог законодавства України. Далі він звертається до україномовного ПТТ EVROVOC. Після обробки запиту на виході з'явиться оброблений сучасними лінгвістичними засобами переклад терміна (дескриптора), який цікавить фахівця. Якщо є сумніви, користувач звертається за уточненням до ІПС "Термінологія (глосарій) СС".

Рис. 5.2

Після цього пошук документів здійснюється в інформаційно-пошукових базах даних Європейського Союзу EVR-Lex, CELEX, EPOQVE, CATEL [241] та ін. В результаті пошуку в цих базах користувач отримує перелік документів, які містять в своїй текстовій частині надане поняття. Проаналізувавши перелік документів, користувач відбирає потрібні йому документи і надсилає їх до програм автоматизованого перекладу документів на українську мову. Всі перекладені українською мовою документи ЄС в електронному вигляді надсилаються до ІПС "Матриця інформаційного законодавства" (Рис. 5.3).

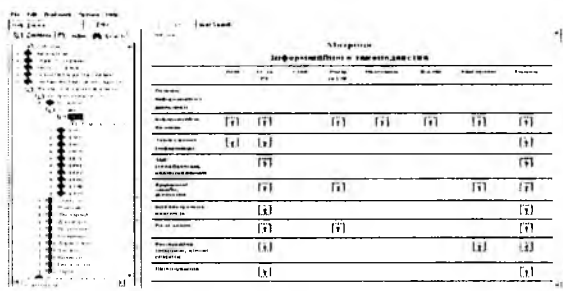


Рис. 5.3

Програма обробляє базу даних, у якій зосереджені законодавчі акти. Перевагою цього варіанта бази даних є те, що є можливість обробляти текстову інформацію. У лівій частині вікна розміщено ієрархічне дерево з основними розділами назв законодавчих актів. За допомогою "мишки" і курсору є можливість відшукати назву необхідного документа. У разі якщо документ знайдений, для його прочитання потрібно навести курсор на назву документа та натиснути на ліву клавішу "мишки". В правому вікні з'явиться текст. За допомогою лінійки прокрутки в правій частині вікна можна відшукати будь-який розділ або частину цього документа. За бажанням документ чи його частину можна перенести до іншого текстового редактора, який розуміє кодування літер текстів Microsoft Office.В лівій колонці матриці розміщено відомості, за якими можна провести аналіз законодавчої бази. У верхньому горизонтальному рядку наведені країни, законодавчі акти яких наявні в базі даних. На перетинанні цих рядків і колонки лівої частини в таблиці є кнопки. При наведенні курсору на кнопку і натисканні лівої клавіші "мишки" можна побачити у віконці, що з'явилося, перелік документів, у яких є посилання на теми, зазначені в лівій колонці таблиці (Рис. 5.4).

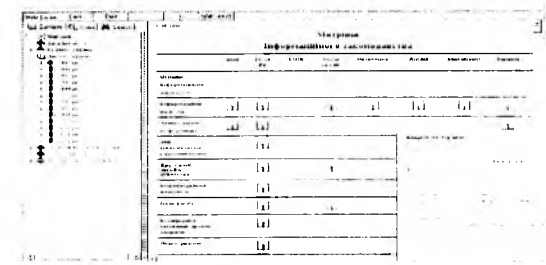


Рис. 5.4

Для ознайомлення з документами достатньо навести курсор на назву документа. При правильному наведенні з'явиться рука з указівним пальцем. Після натискання на ліву клавішу "мишки" у вікні з'явиться потрібний документ. У лівій частині екрана в місці відображення ієрархічного дерева можна побачити, в якій частині цього дерева знаходиться знайдений документ (Рис. 5.5).

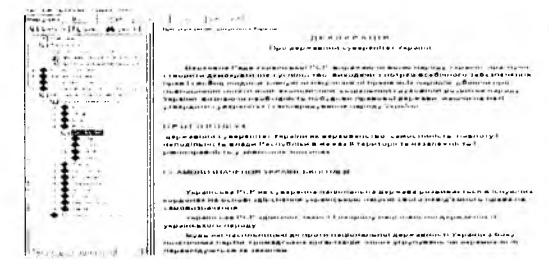


Рис. 5.5

Документ буде знайдений, якщо відомо: його назву, до якої країни чи союзу він належить, в якому році прийнятий законодавцем.

Програма дозволяє виконувати пошук документів за ключовими словами. Для цього потрібно перейти до режиму пошуку (Search) (Рис. 5.6).

У верхньому вікні набирається за допомогою клавіатури ключове слово. В нижньому віконці з'являється перелік документів, де можна зустріти ключове слово. При наведенні курсору на назву потрібного документа і натисканні лівої клавіші "мишки" в правому вікні

з'явиться текст документа. При здійсненні "прокрутки" документа можна відшукати ключове слово, яке було задано, і прочитати текст, де це ключове слово присутнє.

Рис. 5.6

Таким чином фахівець може оперативно провести аналіз будь-якої групи документів, виявити схожість чи розбіжності в тлумаченні різних понять, термінів.

ІПС порівняння нормативно-правових документів "Матриця інформаційного законодавства" зручна в роботі і нескладна для освоєння. Робота за програмою дозволяє спростити користувачу виконання окремих пошуків. Так, деякі документи мають між собою зв'язок швидкого переходу від одного документа до іншого. Якщо в тексті документа є слово чи речення, що підкреслені прямою лінією, то при наведенні курсору на підкреслене місце і натисненні лівої клавіші "мишки" у віконці миттєво з'явиться текст.

На сьогодні система автоматизованого пошуку та аналізу нормативно-правових документів розроблена та апробована на рівні експериментального зразка. Продовження роботи є необхідною з точки зору виконання програм адаптації законодавства України до законодавства Європейського Союзу. Зараз існують і працюють основні блоки, проте є потреба узгодити їх між собою. Необхідним є створити такі програми, які нададуть можливість лінгвістичного узгодження мов у зв'язку з автоматизованим перекладом та забезпечать "розуміння" між блоками. Продовження роботи потребує відповідних ресурсів, зокрема щодо можливості залучення фахівців-програмістів з подальшого удосконалення програм, що зазначені на Рис. 5.1.

Питання для самоконтролю

1. Передумови систематизації інформаційного законодавства.
2. Концепція реформування законодавства України у сфері суспільних інформаційних відносин (затверджено рішенням Урядової комісії з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади (Протокол № 7 від 06.10.2000 р.).
3. Характеристика проектів правових актів щодо систематизації інформаційного законодавства в Україні.
4. Методологічні основи кодифікації інформаційного законодавства.
5. Основні функції та завдання кодифікованого акту у інформаційній сфері.
6. Структура кодифікованого акту у інформаційній сфері.
7. Методика створення кодифікованого акту у інформаційній сфері.
8. Застосування інформаційно-пошукових систем для порівняння інформаційного законодавства України з європейським законодавством.

ЗАГАЛЬНІ ВИСНОВКИ

У загальних висновках вважаємо за необхідне акцентувати увагу на найголовніших моментах, пов'язаних з предметом теми.

1. Побудова в Україні демократичної, соціальної, правової держави, найвищою цінністю в якій визнаються людина, її життя і здоров'я, честь і гідність, недоторканність і безпека та підтримання ефективного функціонування державних інститутів, пов'язана із необхідністю вдосконалення нормативно-правових засад упорядкування суспільних відносин в інформаційній сфері. Виходячи з положень статей 3 та 21 Конституції України, які визначають природне право початком і основою української правової системи, інформаційне право як сфера врегулювання інформаційних відносин щодо інформаційної діяльності спрямовано на збереження функціональної визначеності будь-якої системи та підтримки її у стані динамічної рівноваги з середовищем, тобто воно є антиподом дезорганізації.

2. Сьогодні економічні, фінансові, банківські, культурні, правоохоронні та інші форми діяльності все активніше здійснюються за допомогою інформаційно-комунікаційних технологій та мереж. Вони не тільки надають більше можливостей вільного та оперативного обігу інформаційних ресурсів щодо товарів, капіталів і послуг але й потребують більшої узгодженості та упорядкованості у інформаційній діяльності. У цих умовах управління, як система упорядкування та регулювання юридичними та організаційними засобами інформаційних відносин щодо реалізації потреб людини, суспільства і держави в політичних, економічних, технологічних, медичних, освітянських, культурних, правоохоронних та інших процесах, набуває значення цільового напряму суспільного розвитку, заснованого на пізнанні її законів та аналізі наслідків. Таке трактування приводить до розуміння ролі інформації як керівного фактора управлінської діяльності, за яким будь-яка динамічна система органічно пов'язана з обігом інформації та отриманням нових знань.

Поєднання (конвергенція) у сучасних умовах традиційних видів та форм інформаційної діяльності та інформаційній діяльності у зв'язку із застосуванням інформаційно-комунікаційних технологій та мереж, які мають один предмет правового регулювання інформаційні відносини, визначають об'єктивну необхідність у створенні спільної системи упорядкування інформаційних відносин. Ця система визначає собою нову юридичну галузь в загальній системі права "Інформаційне право", яка спрямована на реалізацію державної інформаційної політики.

При цьому, ефективність державної інформаційної політики залежить не тільки від наявності декларацій доктринальних положень, а й потребує спільних науково-методологічних підходів до нормативно-правового упорядкування та систематизації суспільних відносин у всьому інформаційному законодавстві.

3. Сучасне інформаційне законодавство має ряд недоліків. Вони зумовлені тією обставиною, що різні закони і підзаконні акти, що регулюють відносини, об'єктом яких є інформація, приймалися в різний час без узгодження понятійного апарату. У юридичній практиці застосовують ряд термінів, які не досить коректні, не викликають відповідної інформаційної рефлексії або взагалі не мають чіткого гносеологічного наповнення. Результатом є термінологічна неузгодженість, різне трактування однакових за назвою і формою категорій, помилки омонімії, коли застосовують слова, які позначають різні по суті предмети (речі), що призводить до їх неоднозначного розуміння і застосування на практиці. Для втілення у життя проголошених Конституцією України та відповідними

міжнародними стандартами ідеалів та ідей постає необхідність у створенні термінологічної єдності та узгодженості понять щодо сфери інформаційного права.

У зв'язку з великою кількістю чинних нормативних документів щодо інформаційної сфери (які не завжди узгоджуються між собою), безперервним їх зростанням (внаслідок чого напромаджуються помилки), постійно виникаючими складнощами в плані гармонійної єдності інформаційного законодавства, узгодженості з європейським законодавством, та, одночасно, розвитком електронно-інформаційного середовища система інформаційного права країни все більше потребує науково-системних підходів та узгодженості усього інформаційного законодавства на рівні кодифікованого акта.

До головних негативних тенденцій в становленні інформаційного законодавства можна віднести його фрагментарний розвиток як у цілому, так і по окремих секторах і формах інформаційної взаємодії суб'єктів із застосуванням новітніх інформаційних технологій.

4. На сьогодні в Україні відсутнє цілісне інформаційне законодавство щодо становлення в державі інформаційного суспільства. Українське законодавство не відображає комплексно зміни у суспільному житті, що виникають в результаті розвитку технологій та мереж, які складають основу інформаційного суспільства. Багато техніко-технологічних елементів, які стосуються сфери інформаційного права, продовжують існувати поза правовим полем, що не тільки стримує розвиток але й негативно впливає на загальний соціально-економічний стан країни.

Становлення та розвиток інформаційного суспільства в Україні потребує створення цілісної системи інформаційного законодавства, гармонізованого з нормами міжнародного права. Це передбачає здійснення відповідної кодифікації усієї інформаційної сфери.

Кодифікаційний акт має містити розділи, зокрема, про засади електронної торгівлі та електронного банкінгу, охорону баз даних, створення системи захисту персональних даних (що потребує від України ратифікації Конвенції Ради Європи № 108 "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних" 1981 р.), охорону та захист прав щодо змісту комп'ютерних програм, у зв'язку із поширенням творів у мережі Інтернет, про дистанційне навчання, телемедицину, надання органами державної влади та органами місцевого самоврядування юридичним та фізичним особам інформаційних послуг з застосуванням Інтернету.

Упорядкування відносин усієї інформаційної сфери потребує також єдиної термінологічної бази, системи стандартів для урядових послуг за допомогою інформаційно-комп'ютерних технологій та мереж, активності у боротьбі з поширенням спаму та електронних вірусів, розробки технологій віддаленої роботи для створення нових робочих місць, внесення змін у систему і методи вищої освіти у напрямі не загального застосування новітніх технологій, а запровадження їх у конкретні предмети освіти та багато ін.

У загальному підсумку є необхідним розробка та прийняття на рівні Кабінету Міністрів України Плану Дій щодо становлення інформаційного суспільства в Україні за умов врахування наукових напрацювань, думок та пропозицій громадського сектору та бізнесу.

5. У результаті оцінки стану питання щодо рефлексивного управління суспільною думкою, розгляду сутності, основних понять, чинників, видів маніпулювання та можливостей інформаційно-психологічного впливу на людину маємо висновок про те, що застосування відомостей, які мають неправдивий зміст, сприяє порушенням прав людини та свобод, пригнічують її емоційно-вольову сферу. Складові маніпулювання перешкоджають формуванню адекватної інформаційно орієнтованої основи соціальної

поведінки, сприяють коливанням соціально-політичних орієнтацій, оцінок, установок у населення, що трансформується в нестабільність в суспільстві та зниження рівня управління в державі. Зазначене виступає як одна із загроз національній безпеці в політичній, соціальній і економічній сферах, що перешкоджає розвитку і зміцненню демократичної, соціальної, правової держави.

Розуміючи те, що застосування засобів цього феномену досить складно визначити, а результати їх нерідко непередбачувані, вважаємо за необхідне підкреслити більш уважне ставлення наукової та правової експертизи до цього феномену, який безпосередньо стосується розробки та прийняття нормативно-правових актів щодо інформаційної сфери. Слід виходити з того, що деструктивні інформаційні маніпуляції людиною і масовою свідомістю можуть разом з національними конфліктами, екологічними катастрофами і демографічними лихами перетворитися на ще одну дуже велике лихо з негативними наслідками, що далеко йдуть, та, навіть, глобальну світову проблему щодо інформаційно-психологічної безпеки людини.

6. Особливість інформації як об'єкта суспільних відносин в інформаційній сфері полягає в тому, що, з одного боку, право само по собі має інформаційну змістовність і спрямовано на систематизацію відправних знань щодо людських відносин, вироблених історією цивілізації, а з іншого, – визначає принципи інформаційного процесу і комунікативних зв'язків, без чого людина існувати не може.

7. Щодо гносеології понять "інформація" та "дані" зазначимо, що в нормах законодавства України ці поняття у більшості випадків ототожнюються. Універсального визначення поняття "інформації" не існує. Кожне з визначень вірне для певного застосування, і кожне стає неконструктивним, якщо воно застосовується не за призначенням. Дефініції у законах та проектах використовують семантичний аспект інформації, тобто змістовний опис об'єкта. Проте поняття "інформація" має два аспекти:

• семантичний – інформація розглядається як знання (відомості), як якісне значення змісту повідомлення. Звідси можна говорити про те, що інформація – це відомості про дійсність на основі мислення і висновків людей або вирішення завдань засобами, що наділені "інтелектуальними" можливостями. У загальному плані поняття "інформація" властиве лише мислячому суб'єктові. Тим самим під інформацією мається на увазі не тільки відповідний сигнал, його зміст, а й інтерпретація, що у подальшому забезпечує, за необхідності, комунікаційну взаємодію. У цьому аспекті зміст слова "інформація" визначає традиційні інформаційні відносини;

• онтологічний аспект – інформація розглядається як кількісне значення міри пропускної здатності каналу телекомунікації (визначеності її упорядкованості (інтенсивності) потоку повідомлення в мережах передачі даних, що зветься "трафік") і упорядкування повідомлень (організація процесу кодування/декодування і передачі/прийому інформації). Інформація в даному аспекті розглядається як упорядкована субстанція, яку можна описати математично. При цьому під системою упорядкування розуміється будь-яка алгоритмізована система з об'єктивно заданим алгоритмом, що може бути розпізнаний. Мова йде не про змістовний аспект інформації, а про можливості її неспотвореного перетворення-кодування для обробки в автоматизованих системах і переміщення по комунікаційних лініях. Для технічного об'єкта "інформація" не "відомості" і, тим більше, не "знання". Машина не вміє мислити ("усвідомлювати", "уявляти", "роз'ясновати") як людина. Вона вміє тільки перетворювати виділену тим або іншим засобом множину кодів (сигналів, структур) на основі однозначно заданої послідовності фіксованих операцій. Для традиційного документа захист інформації є захистом відомостей, для електронного документа захистом інформації є захист даних, тобто захист ко-

дів (сигналів, структур). Самі відомості не мають значення, нехай це навіть безглуздий з позицій людини їх набір. Для машини важливе чергування кодів, до яких "прикріплені", "пристосовані" відомості, і захист даних є збереженням порядку їх черги. У неживій природі об'єкти взаємодіють з інформаційним кодом, але не зі "знанням" чи "відомостями". У цьому аспекті слово "інформація" відповідає гносеології поняття "дані", яке визначає інформаційно-телекомунікаційні відносини.

Виходячи з зазначеного виникає потреба у розмежуванні в інформаційному законодавстві таких понять як "інформація" та "дані".

8. Інформаційне право – це система суспільних уявлень про духовні цінності та справедливий життєвий устрій, історично сформовані світовою цивілізацією, та сформульовані на їх основі соціальні принципи взаємостосунків у вигляді правових формул (норм права) щодо відносин суб'єктів в інформаційній сфері, які виникають у процесі створення, збирання, збереження, користування, використання і поширення інформації, даних та інформаційних ресурсів (продуктів), що охороняються та захищаються державою у правових нормах інформаційного законодавства.

За теорією позитивного права, правове регулювання інформаційної сфери – це юридично визначені суспільні відносини, що виникають у процесі інформаційної діяльності людей для задоволення їх потреб та інтересів щодо інформації та стосовно інших сфер через інформацію. Щодо останнього, то інформація у таких відносинах відіграє допоміжну, забезпечуючу роль.

Не випадково, що інформаційне право України як напрям наукових досліджень розміщене поки що поряд з адміністративним правом та фінансовим правом. Це не тільки данина першопрохідцям і ученим-юристам, які стояли біля витоків правового регулювання сучасної інформаційної діяльності (згадаємо про дуже прогресивний у свій час Закон України "Про інформацію" 1992 р.), а й свідчення того, що інформаційне законодавство для того, щоб забезпечити розвиток інформаційного суспільства в Україні, змушене було починати не тільки із застосування напрацьованих методів адміністративного стимулювання інновацій (в економічній площині), а й стримувати негативні тенденції у контексті безпеки людини, суспільства і держави. У цьому сенсі на рівні визначення юридичних деліктів (міжнародних правопорушень) інформаційно небезпечних діянь та необхідності стримування їх негативного зростання, правове регулювання здійснюється методами не тільки адміністративної, а й кримінальної юрисдикції.

Фінансово-правовий аспект інформаційного законодавства визначає можливість державної економічної підтримки інновацій щодо інформаційної діяльності (через бюджетні видатки, банківські кредити, податкові пільги тощо) з перспективою повернення грошей (через податки, розширення бази оподаткування тощо). У контексті фінансового законодавства можна говорити, що інформаційна діяльність потрібне для надходжень до державного бюджету.

Цивільне законодавство зі своєю юрисдикцією щодо змагальності сторін не в змозі оперативно реагувати на негативні соціальні тенденції в суспільстві (така його природа), хоча не виключається застосування його можливостей стосовно вирішення колізій у правовідносинах. Як вважаємо, "Право інтелектуальної власності", що визначено книгою четвертою Цивільного кодексу України, стосовно інформаційної діяльності має бути складовою частиною кодексу щодо сфери інформаційного права. Згадаємо, що об'єкти інтелектуальної власності є не що інше, як інформація, яка може отримувати оболонку охороноздатності у вигляді охоронного документа під назвою патент, свідоцтво тощо.

У свою чергу інформаційне право та інформаційне законодавство також сприяють розвитку традиційних провідних та інших галузей права. З інформатики у право перейшло економічне розуміння сутності інформації як різновиду майна: що вона не річ і не енергія, але має економічний зміст. Інформація через таке поняття, як "дані" може на рівні з речами та енергією бути об'єктом її обігу, зобов'язань, а отже – і об'єктом права власності (і не тільки в контексті права інтелектуальної власності). Зазначене, зокрема, свідчить, що інформаційне право вже сформувалося як нова галузь юридичних наук, яка апробована та увійшла в їх систему у статусі наукової спеціальності та навчальної дисципліни.

9. Класифікаційні ознаки частини права, що претендує на самостійність як галузь права, обов'язково визначаються предметом та методами правового регулювання, які базуються на відповідних принципах. У кожній із сфер суспільного життя відносини неоднорідні, тому їх також можна поділити на більш вузькі, відособлені групи відносин, які мають свої особливості, а отже, і певну функціональну самостійність. Такі групи норм у межах конкретної галузі права, що регулюють однорідні групи суспільних відносин у рамках певного їх виду та функціональної спрямованості, складають правовий інститут. Таким чином, правовий інститут – це група правових норм конкретної галузі права, що врегульовує певний масив функціонально однорідних відносин у межах певного їх виду.

Предметом інформаційного права є упорядкування та правове регулювання суспільних інформаційних відносин, які відображають специфічні умови і правила поведінки різних суб'єктів права і управління в інформаційній сфері. Методи інформаційного права – це засоби, прийоми і способи вивчення діяльності, процесів та відносин у інформаційній сфері.

10. Принципи інформаційного права – це зафіксовані в правових формулах світових стандартів ідеї і положення, які визначають суть інформаційних відносин та надають системний зміст правовим нормам і інститутам в інформаційній сфері. Потім принципи інформаційного права залежно від національних, політичних уявлень трансформуються у принципи правового регулювання інформаційних відносин відповідного національного законодавства, яке встановлює межі стосовно світових принципів права в діяльності щодо пошуку, створення, обробки, використання та користування, поширення інформації та даних, визначає спеціальні режими доступу до відповідних видів інформації, гарантії доступу, форми охорони та захисту, заходи відповідальності тощо.

11. Організаційною основою структуризації суспільних відносин є інститути.

До основних інститутів інформаційного права відносяться інформаційні відносини щодо галузей засобів масової інформації, науки та освіти, інформатизації та Національної програми інформатизації.

До інших інститутів інформаційного права відносяться інформаційні відносини щодо інтелектуальної власності, захисту персональних даних, електронної комерції, електронного банкінгу, електронного урядування, інформаційної безпеки. Структуризація, за необхідністю, має можливість бути розширеною, зокрема, у зв'язку з потребами у визначенні нових інформаційних відносин щодо інших галузей господарства.

12. Інформаційне законодавство України складає великий масив нормативно-правових актів. Порівняльний аналіз їх з положеннями європейських стандартів може зайняти багато часу, якщо це здійснюється традиційними методами та засобами. Щоб скоротити час відпрацювання документів і збільшити ефективність роботи в нормотворчій діяльності, необхідне залучення сучасних інформаційних систем та технологій.

Додатки

Додаток 1

Загальна структура інформаційного права

ІНФОРМАЦІЙНЕ ПРАВО – комплексна система суспільних уявлень про духовні цінності та справедливий життєвий устрій, які історично сформовані світовою цивілізацією, та сформульовані на їх основі соціальні принципи взаємостосунків і правових відносин суб'єктів в інформаційній сфері, що виникають у процесі створення, збирання, збереження, використання і поширення інформації та інформаційних ресурсів (продуктів), які охороняються та захищаються державою.

Підсистема з регулювання відносин в області інформації

ІНФОРМАЦІЯ – повідомлення про будь-які відомості чи сукупність відомостей щодо фактів або особистих уявлень.

Інформація нова (знання) – документовані або публічно оголошені відомості про події та явища, щодо особи, суспільства, держави та навколишнього природного середовища, зміст яких має інтелектуальне самовираження і не може бути наперед відомий чи передбачений їх одержувачем.

Інформація масова (щодо засобів масової інформації) – документовані або публічно оголошені відомості про події та явища, що відобуваються у суспільстві, державі та навколишньому природному середовищі

Підсистема з регулювання відносин в області інформатики

ІНФОРМАТИКА – наукова дисципліна, яка вивчає процеси створення, обробки та захисту даних, інформаційних ресурсів, інформаційних продуктів, (зокрема, об'єктів інтелектуальної власності), інформаційно-комп'ютерних технологій, надання інформаційних послуг у різних сферах життєдіяльності людини, суспільства і держави, їх носій, технологій, системи зв'язку і мережі телекомунікацій.

Дані – електронні сигнали, коди або структури щодо повідомлень на матеріальному носії, до яких інформація пристосована (прикріплена)

Підсистема з регулювання відносин в області інформатизації

ІНФОРМАТИЗАЦІЯ – сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, які спрямовані на створення умов для задоволення потреб громадян та суспільства на основі розвитку і використання інформаційних систем, мереж, ресурсів та інформаційно-комунікаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки

ІНФОРМАЦІЙНЕ ЗАКОНОДАВСТВО

"Про мови в Українській РСР", 28.10.1989;
"Про інформацію", 02.10.1992;
"Про друковані засоби масової інформації (пресу) в Україні", 16.11.1992;
"Про телебачення і радіомовлення", 02.06.1995;
"Про інформаційні агентства", 28.02.1995;
"Про видавничу справу", 05.06.1997;
"Про рекламу", 03.07.1996;
"Про бібліотеки і бібліотечну справу", 27.01.1996;
"Про національний архівний фонд і архівні установи", 24.12.1993;
"Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації", 23.09.1997 тощо

"Про інформацію", 02.10.1992;
"Про науково-технічну інформацію", 25.06.1993;
"Про наукову та науково-технічну діяльність", 13.12.1991;
"Про наукову і науково-технічну експертизу", 10.02.1995;
"Про освіту", 23.03.1991;
"Про авторське право і суміжні права", 23.12.1993;
"Про охорону прав на винаходи і корисні моделі", 23.12.1993;
"Про охорону прав на знаки для товарів і послуг", 23.12.1993 тощо

"Про інформацію", 02.10.1992;
"Про Національну програму інформатизації", 04.02.1998;
"Про Концепцію Національної програми інформатизації", 04.02.1998;
"Про електронні документи та електронний документообіг", 22.05.2003;
"Про електронний цифровий підпис", 22.05.2003;
"Про телекомунікації", 8.11.2003;
"Про захист інформації в інформаційно-телекомунікаційних системах", 31.05.2005 тощо

Закон України від 09.01.2007 р. № 537-V "Про Основні засади розвитку Інформаційного суспільства в Україні на 2007-2015 роки"

Додаток 2

Затверджено та взяте за основу
рішенням Урядової комісії з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади (Протокол № 7 від 06.10.2000 р.)
(Свідоцтво про реєстрацію авторського права на твір № 25784 від 24.09.2008 г.)

КОНЦЕПЦІЯ
реформування законодавства України у сфері суспільних інформаційних відносин

Ця Концепція визначає стан правового забезпечення регулювання суспільних інформаційних відносин в Україні та стратегію (основні засади) реформи інформаційного законодавства при входженні її до інформаційного суспільства.

1. Об'єктивні умови необхідності законодавства у сфері суспільних інформаційних відносин та його реформи в Україні

Однією з відмінних, визначних ознак сучасного світового соціального прогресу є зростання значимості інформації в суспільних відносинах. Суспільні інформаційні відносини постійно розвиваються, особливо з удосконаленням техніки та технології збору, обробки, зберігання та передачі інформації, по мірі опанування людством законами природи, зростання суспільного інтелекту за принципом "досконалість не має обмежень". Зазначені процеси визначають інформаційне суспільство, сутність якого розкрита у 1993 році Комісією Європейського Союзу: "інформаційне суспільство – це суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій та технологій зв'язку".

Не знаходиться поза цим процесом і Україна. Після проголошення 24 серпня 1991 року державної незалежності України створюється національна система законів та підзаконних нормативних актів щодо правового регулювання соціальних відносин, визначною складовою яких є інформація. В суспільних інформаційних відносинах для упорядкування та врегулювання на державному рівні виникла потреба юридично визначитися в найбільш важливих правових нормах поведінки їх учасників, в тому числі й можливості запобігання та боротьби з правопорушеннями, які учиняються з використанням сучасних інформаційних технологій. В свою чергу, це зумовило необхідність відокремлення та фіксування в державному управлінні напряму (інституції), що визначається як державне управління у галузі суспільних інформаційних відносин. Метою його є втілення в життя державної політики в умовах розвитку суспільних інформаційних відносин в Україні: методів і засобів створення інформаційних ресурсів, їх обігу, збирання, накопичення, систематизації, використання, зберігання та захисту. Важливим аспектом інформаційних відносин є забезпечення національної інформаційної безпеки як важливої складової національної безпеки.

2. Стан правового регулювання суспільних інформаційних відносин в Україні

Національне право України має значний масив нормативно-правових актів, які безпосередньо чи опосередковано регулюють суспільні інформаційні відносини.

Чинне законодавство з регулювання соціальних інформаційних відносин базується на таких системоутворювальних його нормативних актах: Конституція України, закони України "Про інформацію", "Про мови", "Про державну таємницю", "Про науково-технічну інформацію", "Про телебачення і радіомовлення", "Про друковані засоби масової інформації (пресу) в Україні", "Про захист інформації в автоматизованих системах", "Про бібліотеки і бібліотечну справу", "Про інформаційні агентства", "Про зв'язок", "Про національний архівний фонд і архівні установи", "Про національну програму інформатизації", "Про концепцію національної програми інформатизації", "Про авторське право і суміжні права" та інші, які створюють певні умови для розвитку їх положень в системі підзаконних актів.

Разом з тим, у правовому регулюванні суспільних інформаційних відносин в Україні існує ряд проблем, які потребують вирішення.

3. Проблеми правового регулювання суспільних інформаційних відносин в Україні

У сфері суспільних інформаційних відносин нормотворення в Україні здійснюється шляхом вирішення окремих проблем в окремих законах та підзаконних нормативних актах фрагментарно. В той же час значний масив норм щодо інформації розміщено в кодифікованому законодавстві, зокрема в цивільному, адміністративному, трудовому, кримінальному. Таким чином, в Україні сформувалася національна специфічна змішана доктрина права, яка поєднує в собі елементи англо-американської та європейської континентальної доктрини права. Серед недоліків законотворчої діяльності за існуючою доктриною в Україні визначаються такі:

Правотворчий процес нерідко здійснюється без узгодження з чинним законодавством, не враховується специфіка національної ментальності, правової культури систематизації права, які є основою правосвідомості, інших особливостей соціального та державного життя.

Різні закони та підзаконні акти, що регулюють суспільні відносини, об'єктом яких є інформація, приймались у різні часи без узгодження понятійного апарату, тому вони мають ряд термінів, які не є достатньо коректними, а отже, розуміються неоднозначно учасниками суспільних інформаційних відносин. Деякі категорії взагалі не мають чіткого визначення свого змісту, що призводить до їх неоднозначного застосування на практиці. Наприклад, "інформація" і "дані", "таємна інформація" і "таємниця", "документ" і "документована інформація", "майно" і "власність", "інтелектуальна власність", "володіння", "автоматизована система" тощо. Це, в свою чергу, породжує соціальні конфлікти (правопорушення) в інформаційних відносинах між їх учасниками та створює умови для уникнення від відповідальності правопорушників, що негативно впливає на формування високої культури правовідносин на рівні найкращих здобутків світової цивілізації.

Значна кількість юридичних норм, які регулюють суспільні інформаційні відносини, розпорошена по різних законах та підзаконних нормативних актах, що ускладнює їх пошук, аналіз та узгодження для практичного застосування.

Має місце розбіжність щодо розуміння структури системи законодавства в сфері інформаційних відносин та підходів до її формування. Нерідко в окремих законах в систему законодавства включають норми, виражені в підзаконних нормативних актах, що суперечить положенням Конституції України. Це викликає в практиці правозастосування колізію норм – імперативних норм закону на користь норм підзаконного акта.

Нові юридичні норми в сфері суспільних інформаційних відносин нерідко не узгоджені з раніше прийнятими, що призводить до правового хаосу, падіння авторитету публічного права, нігілістичного ставлення суб'єктів суспільних відносин до законодавства.

Через неузгодженість правового регулювання у законодавстві щодо збору інформації на різних рівнях державного управління, зокрема персональних даних, різні органи державної влади примушують громадян надавати довідки з різних установ для отримання іншої довідки. Існує порочний принцип недовіри до документа, який був виданий іншою інстанцією, в результаті чого громадяни змушені витрачати багато часу на ходіння по різних державних установах, щоб підтверджувати правомірність виданих їм раніше документів. Це повинно викорінюватися, у тому числі правовими засобами, зокрема, на рівні законодавства.

Сукупність правових норм у сфері суспільних інформаційних відносин, визначених у законах і підзаконних актах, досягла за кількістю критичного стану (критичної маси), що зумовлює необхідність виділення їх в окрему галузь законодавства.

Зростає загроза особі, суспільству, державі від такого негативного явища, як комп'ютерна злочинність – вчинення злочинів з використанням інформаційних технологій та технологій зв'язку.

Одним із шляхів подолання проблем правового регулювання суспільних інформаційних відносин є законодавча систематизація правих норм.

4. Етапи систематизації інформаційного законодавства

Систематизація інформаційного законодавства передбачається в три етапи.

1. Інкорпорація законодавства – визначення ієрархічної системи та структури інформаційного законодавства на рівні правової доктрини.

2. Виділення в системі законодавства галузі та закріплення її легально у Зводі законів України як розділу "Інформаційне законодавство".

3. Кодифікація – розробка і прийняття Верховною Радою України такого нормативного акту як Кодекс України про інформацію.

У цьому Кодексі повинні бути зведені і систематизовано узгоджені між собою та іншим законодавством України її зобов'язання щодо інтеграції у світове співтовариство, в тому числі відповідно до Програми інтеграції України до Європейського Союзу (до її Розділу 13 "Інформаційне суспільство").

5. Наукове забезпечення систематизації інформаційного законодавства України

В Україні щодо систематизації законодавства склалися певні добрі національні традиції, дієвість яких перевірена часом. Ідея інкорпорації та кодифікації правових норм у сфері інформаційних відносин визначена та науково обґрунтована в дослідженнях вітчизняних науковців, має відповідні теоретичні напрацювання.

За умов розвитку інформатизації, система чинних правових норм регулювання інформаційних відносин потребує моніторингу щодо їх дієвості і узгодження з новими соціальними відносинами, зокрема щодо виявлення проблем у цих відносинах з науковим обґрунтуванням їх вирішення. Це в першу чергу потрібно для упередження негативних соціальних наслідків.

В основу законодавчої інкорпорації покладаються відпрацьовані юридичною наукою і перевірені практикою норми чинного законодавства України.

При систематизації увага повинна звертатися на визначення структури, місця юридичних норм у системі правового регулювання. Необхідно чітко визначити суб'єкти і об'єкти інформаційних відносин, правила поведінки учасників, їх права та обов'язки.

5.1. Державна доктрина у сфері регулювання суспільних інформаційних відносин

На рівні державної доктрини визначається:

Інформаційне законодавство є галуззю законодавства, яке тісно пов'язане з іншими галузями законодавства України.

Інформаційне законодавство регулює суспільні правовідносини щодо інформації як форми виразу інших правовідносин: у засобах масової інформації, освіті, культурі, бібліотечній та архівній справі, науковій та науково-технічній діяльності, права інтелектуальної власності, інформатизації, інформаційно-аналітичному забезпеченні діяльності органів влади всіх рівнів соціального управління (представницької, виконавчої та судової), захисту інформації, інформаційної безпеки тощо.

Основними напрямами правового регулювання інформаційних відносин є:

Визначення та правове закріплення провідних напрямів державної політики в галузі соціальних інформаційних відносин в умовах інформатизації.

Забезпечення умов для розвитку і захисту всіх форм власності на інформацію та інформаційні ресурси, права інтелектуальної власності.

Організація та управління створенням і розвитком загальнодержавних та регіональних систем і мереж інформаційно-аналітичного забезпечення діяльності органів влади, забезпечення їх технічної та технологічної сумісності і взаємодії на основі державних стандартів в єдиному інформаційному просторі України, інтеграції його з європейським та світовим інформаційним простором.

Правове регулювання щодо створення реальних умов для якісного та ефективного забезпечення необхідною інформацією громадян, органів державної влади, органів місцевого

самоврядування, державних і приватних організацій, об'єднань на основі державних інформаційних ресурсів, сучасних інформаційних технологій

Забезпечення співвідношення інтересів суб'єктів суспільних інформаційних відносин у сфері національної безпеки, її складової - інформаційної безпеки.

Забезпечення реалізації прав осіб (фізичних та їх об'єднань) на режим доступу до інформації, зокрема персональних даних – інформації про громадян та організації за умов інформатизації державних органів управління та суспільства в цілому.

Державно-правове сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем, технологій з визначенням пріоритетів для вітчизняних виробників інформаційної продукції, засобів, технологій

Державне стимулювання вдосконалення механізму залучення інвестицій, розробки і реалізації проектів Національної та локальних програм інформатизації

Забезпечення правового режиму формування і використання національних інформаційних ресурсів, збору, обробки, систематизації, накопичення, зберігання, пошуку, поширення та надання споживачам інформації.

Правове регулювання щодо стимулювання створення і використання в Україні новітніх інформаційних технологій, засобів комунікації, зв'язку, розробка економічних механізмів для протидії відтоку висококваліфікованих спеціалістів у сфері інформатики за кордон, легалізації програмних продуктів (комп'ютерних програм, пакетів та систем комп'ютерних програм, автоматизованих (комп'ютерних) баз даних та знань)

Постійний моніторинг та визначення найбільш небезпечних загроз безпеці суспільним інформаційним відносинам, відповідне реагування на загрози, регулювання захисту інформації, в тому числі в автоматизованих (комп'ютерних) системах.

Створення реальних правових бар'єрів, механізмів їх реалізації для недопущення свавілля державними та недержавними структурам, посадовими особами щодо примушення подання їм громадянами інформації, яка існує в інших структурах. Утвердження принципу кримінальної, адміністративної та цивільно-правової презумпції невинності (невиновності) громадянина щодо надання ним різним організаціям персональних даних: перевірка достовірності документа, встановлення юридичного факту та його документування має бути функцією органу (державного чи громадського), уповноваженого видати відповідний документ.

Регулювання суспільних інформаційних відносин між фізичними та юридичними особами, суспільством і державою через засоби масової інформації.

Визнання засобом масової інформації окремих регіональних, національних та глобальних комп'ютерних мереж, в тому числі таких, як Інтернет (електронних газет та журналів, рекламних та інформаційних сторінок установ, організацій, підприємств тощо), подібно до радіо і телебачення. Упорядкування на рівні законодавства інформаційних правовідносин, що виникають при використанні комп'ютерних мереж загального користування.

Розробка правової доктрини гармонізації національного інформаційного права України з міжнародним інформаційним правом. Розвиток теоретико-правової бази та практики правового регулювання суспільних інформаційних відносин в нашій країні потрібно здійснювати з урахуванням зарубіжного досвіду та міжнародного права. Особлива увага повинна звертатися на виявлення та дослідження недоліків, для уникання їх у правотворчій та правозастосовній діяльності, запобігання негативним для суспільства наслідкам інформатизації. Імплементація норм міжнародного права здійснюється з урахуванням вітчизняної доктрини права щодо поділу його на провідні галузі права: публічне і приватне, а також конституційне, адміністративне, цивільне, трудове і кримінальне право та міжгалузеві комплексні інститути права.

5.2. Принципи наукового забезпечення правотворчої діяльності

Провідними принципами наукового забезпечення правотворчої діяльності щодо систематизації в сфері соціальних інформаційних відносин є:

системний та комплексний підходи у вирішенні проблем правотворчості,

ґрунтовне фундаментальне та прикладне теоретичне обґрунтування новацій (понять, категорій тощо);

демократизм – залучення широкого кола вітчизняних фахівців до обговорення проблем інформаційного законодавства;

недопустимість необґрунтованого копіювання зарубіжного досвіду;

повага та гуманне ставлення до людини, її честі, гідності, репутації;

презумпція невинності людини, громадянина, приватної особи

Фахівці, які залучаються до систематизації інформаційного законодавства, повинні володіти знаннями в галузі права та інформатики, теорії та практики.

5.3. Методологічні підходи до систематизації інформаційного законодавства України

Правотворення повинно базуватися на основі методології системного і комплексного підходів - теорії формування комплексних ієрархічних гіперсистем інформаційного законодавства: розвиток конституційних норм знаходить вираз у системоутворювальних законодавчих актах, які регулюють суспільні інформаційні відносини в Україні. Системоутворювальним законодавчим актом повинен стати прийнятий Верховною Радою України Кодекс про інформацію, в якому будуть розвиватися визначені в Конституції України положення про суспільні інформаційні правовідносини.

Систематизація інформаційного законодавства повинна вирішити наступні завдання-цілі:

розвивати норми і принципи правового регулювання суспільних відносин, що визначені в Конституції України;

враховувати ратифіковані Україною нормативні акти міжнародного права (міждержавні угоди, конвенції);

легалізувати позитивні звичаї в сфері інформаційних відносин та норми суспільної моралі, загальнолюдські цінності, визначені Організацією Об'єднаних Націй в Декларації прав людини та інших загальноприйнятих міждержавних нормативних актах

2. Методологічною базою правотворення інформаційного законодавства України є юридична доктрина щодо умовного поділу права на галузі за такою принциповою моделлю: основа – конституційне право; його положення знаходять паралельний розвиток (відповідно до методів правового регулювання і захисту прав) в адміністративному, цивільному, трудовому та кримінальному праві, інших підсистемах національного права України, в нормах яких інформація виступає як опосередкований, додатковий (факультативний) предмет регулювання суспільних відносин

3. Домінуючою в методології систематизації суспільних інформаційних відносин в Україні є доктрина сучасного вітчизняного конституційного права (основа – Конституція України) та прогресивних здобутків міжнародного права щодо верховенства прав людини

4. Доктринально визнається багатооб'єктність юридичних норм, законодавства в юридичній кваліфікації суспільних інформаційних відносин

5. Систематизація інформаційного законодавства повинна проводитися методом агрегації: удосконалення окремих правових норм чи створення нових міжгалузевих правових інститутів повинно не порушувати цілісність та призначення інформаційного законодавства, а удосконалювати його цілість в цілому, створювати нову системну якість, яка не притаманна окремим його складовим.

6. Напрями, підцілі, завдання систематизації інформаційного законодавства повинні чітко формуватися відповідно до теорії системи підцілей ("дерева цілей").

5.4. Мета систематизації інформаційного законодавства України

Метою систематизації інформаційного законодавства України є створення чіткої структури правового регулювання суспільних відносин між їх суб'єктами щодо інформації, забезпечення співвідношення потреб та інтересів людини, соціальних спільнот та держави.

Інше визнається підцілями, функціями, напрямами, окремими завданнями регулювання в сфері інформаційних суспільних відносин.

6. Провідні функції та завдання систематизації інформаційного законодавства України

6.1. Провідні функції

Провідними функціями систематизації інформаційного законодавства України є:

регулятивна – визначення зобов'язань, прав та обов'язків суб'єктів, регулювання суспільних інформаційних відносин;

нормативна – визначення норм, правил поведінки суб'єктів інформаційних відносин,

охоронна – визначення гарантій та меж правомірної поведінки, форм та умов, за якими діяння утворюють правопорушення (делікти), та відповідальності за них згідно з нормами цивільного, адміністративного, трудового, кримінального законодавства;

інтегративна – системне поєднання комплексу визначених юридичних норм, які регулюють інформаційні відносини в Україні; поєднуюча ланка між провідними традиційними галузями права (конституційним, цивільним, адміністративним, трудовим та кримінальним) щодо застосування їх методів та принципів із захисту прав в сфері інформаційних відносин;

комунікативна – зазначення в окремих статтях посилань на наявні законодавчі акти, створення підсистем різних міжгалузевих інститутів права, в яких інформація виступає як форма виразу правовідносин.

6.2. Провідні завдання

Провідні завдання систематизації інформаційного законодавства:

визначення консенсусу (згоди) в суспільних стосунках, узгодженості розуміння та застосування юридичних норм, правомірної поведінки учасників інформаційних відносин;

забезпечення інформаційного суверенітету, незалежності України у міжнародних стосунках,

забезпечення інформаційної безпеки громадян, їх об'єднань, суспільства та держави як складових національної безпеки України;

визначення правомірної поведінки учасників інформаційних відносин в Україні,

захист інформації від витоку, несанкціонованого доступу, знищення, підробки, модифікацій, перекручення незалежно від технології обробки.

7. Вихідні положення структури інформаційного законодавства України

Відповідно до традицій систематизації законодавства України система інформаційного законодавства України на рівні Кодексу має складатися з двох частин

Частина І. Загальна частина (Загальні положення);

Частина ІІ. Особлива частина (Особливості регулювання інформаційних відносин щодо галузей (сфер) суспільної діяльності).

Кожна з частин поділяється на розділи, розділи, при необхідності, - на глави, які складаються з окремих статей.

Структура статті складається з чіткого формулювання диспозиції суспільних правовідносин між їх суб'єктами. В статтях, в яких визначаються правопорушення, повинно бути обов'язкове посилання на вид відповідальності: відповідно до Цивільного кодексу, Кодексу законів про працю, Кодексу про адміністративні правопорушення, Кримінального кодексу.

Модельні зразки:

"...покарання за це правопорушення наступає у відповідності зі статтею... Кодексу про адміністративні правопорушення України",

"...відповідальність наступає у порядку, визначеному статтями... Кримінального кодексу України",

"...матеріальна відповідальність наступає у порядку, визначеному Цивільним кодексом України",

"...відповідальність наступає відповідно до Кодексу законів про працю".

У Цивільному кодексі, Кодексі законів про працю, Кодексі про адміністративні правопорушення, Кримінальному кодексі створюються відповідні розділи чи глави щодо питань регулювання та відповідальності за правопорушення суспільних інформаційних відносин з посиланням на норми інформаційного законодавства України.

8. Основні положення змісту інформаційного законодавства України

Частина І. Загальні положення. Ця частина включає основні засади інформаційного законодавства: завдання; сферу дії; визначення основних понять; визначення системи правового регулювання інформаційних відносин (законодавство та підзаконні акти, їх чітка ієрархія), мову інформаційних відносин, зміст (сутність) інформаційних відносин; основні принципи інформаційних відносин, державну політику в сфері інформаційних відносин та інформатизації, суб'єкти (учасники) інформаційних відносин; об'єкти інформаційних відносин (предмет правового регулювання); інформаційну діяльність та її види, основні положення щодо зобов'язань в інформаційних відносинах.

Окремі розділи складають комплекс правових норм:

дія та застосування норм міжнародного права;

система захисту прав в інформаційних відносинах (складається з наступних глав: глави про інкорпорацію визначених в Конституції України способів самозахисту, в тому числі через громадські об'єднання; глави про способи захисту в адміністративно-правовому порядку, глави щодо кримінально-правового порядку захисту інформаційних відносин, глави щодо захисту через прокуратуру та Уповноваженого з прав людини при Верховній Раді України; глави про судовий захист в цивільно-правовому порядку, глави щодо способів і порядку звернення за захистом прав суб'єктів суспільних відносин у міжнародні організації та суди)

Частина ІІ. В Особливій частині визначаються урегульовані законодавством підсистеми інформаційних відносин із зазначенням їх системоутворювальних законів, зокрема

державна таємниця;

науково-технічна інформація;

телебачення і радіомовлення;

засоби масової інформації (друковані, преса, електронні);

суспільні відносини щодо автоматизованих інформаційних систем;

бібліотеки і бібліотечна діяльність,

архіви та архівна діяльність,

інформаційні агентства;

зв'язок, комунікаційні системи;

інформатизація та національна програма інформатизації;

державна статистика тощо.

В разі визначення нових сфер регулювання інформаційних відносин (методом агрегації) вводяться нові розділи чи глави. Зокрема, такими можуть бути наступні

захист персональних даних (інформації про особу, особистої інформації),

забезпечення інформаційної безпеки суспільства і держави, регламентація основоположних заходів захисту інформації (організаційно-правових, організаційно-управлінських, організаційно-технічних, програмно-математичних);

захист професійної таємниці;

міжнародні інформаційні відносини із застосуванням електронно-цифрових засобів.

Основні організаційні засади щодо систематизації

Відповідно до законодавства України здійснення заходів щодо систематизації інформаційного законодавства покладається на визначені Верховною Радою України її комітети.

За участю Президента України, Кабінету Міністрів України, Національної академії наук України, Академії правових наук України, провідних наукових закладів України формується робоча група вітчизняних фахівців у галузі інформатики, інших суспільних інформаційних відносин та права (науковців і практиків) для наукового обґрунтування та розробки законодавчих актів у сфері суспільних інформаційних відносин та кодифікації їх норм.

Кабінет Міністрів України формує провідний міжгалузевий орган центральної виконавчої влади (міжвідомчу урядову комісію), який буде відповідальним за організацію та забезпечення створення проектів законодавчих актів та кодифікації інформаційного законодавства.

Визначений Кабінетом Міністрів України орган центральної виконавчої влади без посередньо створює умови та забезпечує діяльність робочої групи щодо систематизації інформаційного законодавства України.

Інші зацікавлені міністерства та відомства вносять свої пропозиції до організації робочої групи, у межах своїх можливостей та компетенції сприяють її діяльності.

Проекти нормативних актів попередньо розглядаються на спільних засіданнях Консультативної ради з питань інформатизації при Верховній Раді України, Урядової комісії з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади, інших урядових органів і представників відповідних структур міністерств, відомств та ін.

Проекти нормативних актів виносяться на обговорення громадськості через засоби масової інформації (пресу, радіо, телебачення тощо).

Пропозиції щодо удосконалення окремих положень проектів нормативних актів адресуються до створеної робочої групи.

Для врахування думок авторів пропозицій, їх обґрунтування організовуються та проводяться наукові конференції, семінари тощо.

Після розгляду пропозицій та доопрацювання проекти нормативних актів надсилаються на розгляд Верховній Раді України у порядку, визначеному для проходження законопроектів.

Розробки нових законів та підзаконних нормативних актів у сфері суспільних інформаційних відносин можуть поєднуватися з розробкою проекту Кодексу про інформацію.

Фінансове забезпечення роботи щодо систематизації

Фінансове забезпечення роботи щодо систематизації інформаційного законодавства України здійснюється відповідно до Національної програми завдань і проектів з інформатизації та інших програм, в яких визначені проблеми суспільних інформаційних правовідносин, права інтелектуальної власності та інформаційної безпеки України.

Зацікавлені органи державної влади, міністерства та відомства здійснюють додаткове фінансування та матеріальне забезпечення функціонування робочої групи щодо систематизації інформаційного законодавства.

Фінансову підтримку робочій групі також можуть надавати недержавні організації, громадські фонди, благодійні організації.

Інформаційні війни: види, зброя, засоби нападу та захисту

Види	Зміст	Зброя	Засоби нападу	Засоби захисту
Радіоелектронна війна (складовою частиною є радіо-, кінотрансляція та радіорозвідувальні дії)	радіоелектронна розвідка, постановка перешкод радіозв'язку, руйнування засобів зв'язку та придушення інформаційного обміну	електромагнітне випромінювання акустичних і інфрачервоних сигналів	радіоелектронне устаткування, зокрема, передавачі перешкод	забезпечення перешкодостійкості, захист устаткування та мереж зв'язку
Електронно-інформаційна війна (складовою частиною є телетрансляція та е-розвідувальні дії)	несанкціонований доступ до інформації та файлів	відомості щодо противника	інформаційно-комунікаційні технології та мережі	організаційно-технічний, програмний
	крадіжка, перекручення або знищення інформації та файлів	отримання або знищення інформації та файлів	" "	" "
	розміщення відомостей у базах даних	файли з недостовірними даними	" "	" "
	розміщення відомостей у корпоративних мережах	файли з недостовірними даними	" "	" "
	розміщення відомостей в Інтернеті	" "	" "	"
	використання е-пошти	" "	" "	" "
	постановка перешкод засобам зв'язку	електромагнітне випромінювання	радіоелектронне устаткування	забезпечення перешкодостійкості
	розміщення або недопущення розміщення відомостей у ЗМІ (зокрема, у е-ЗМІ)	відомості з недостовірною інформацією	радіо- та радіоелектронне устаткування	захист від маніпулювання свідомістю людини
Комп'ютерна агресія (хакерський напад), що здійснюється завдяки файлу-вірусу (програми), зокрема:	фізичне руйнування комп'ютерних систем	електромагнітне випромінювання	мікроелектронна схема (чіпи)	організаційно-технічний, програмний
	перепрограмування або руйнування програмного забезпечення комп'ютерних систем та мереж	файли-віруси	комп'ютерні технології	програмний організаційно-технічний
• "Троянські коні" ("бомби")	фрагменти коду, що приховуються у програми, імітуючи будь-яку іншу програму, шукають слабкі місця системи та повідомляють про них зломщиков			
• "Черв'яки"	віруси -"хробаки", які зменшують ресурси системи, зокрема, щодо заповнення магнітних носіїв, скорочують швидкість та порушують її роботу,			
• "Логічні бомбі"	посилюють активність "Троянського коня" та можливості "Черв'яків", запускає в програму вірус-"хробака" у певний час або за сигналом, заданим звонк			
• Трендор	механізм, вбудований в комп'ютер або програму його виробником для проникнення в систему після того, як програма була продана або поширена.			

Додаток 4

Матриця положень (статей) основних законів України в інформаційній сфері та положень у проектах кодексів

	Закон України **"Про інформацію"** (1992 р.)	Закон України **"Про науково-технічну інформацію"** (1993 р.)	Закон України **"Про Нац. програму інформатизації"** (1998 р.)	Закон України **"Про телекомунікації"** (2003 р.)	Закон України **"Про захист інформації в інформаційно-телекомунікаційних системах"** (2005 р.)	Проект **Інформаційного кодексу,** розробленний у Держкомтелерадіо України (2001 р.)	Проект **модельного Інформаційного кодексу,** авт. О.Баранов та ін. (2005 р.)	Закон РФ **"Об информации, информатизации и защите информации"** (1995 г.)
Наявність у законах відповідних розділів, статей та формулювання положень								
Преамбула	+	+	+	+	-		-	
Частина І. Загальна частина								
Розділ 1. Загальні положення							Книга 1 розділ 1	
Стаття 1. Визначення основних понять								
база даних -			ст. 1					
база знань -			ст. 1					
блокування інформації -					ст. 1			
витік інформації -					ст. 1			
власник інформації -					ст. 1			
власник персональних даних -								
власник системи -					ст. 1			
власник інформаційних ресурсів, інформаційних систем і засобів їх забезпечення -								ст. 2
володілець персональних даних -								
володілець інформаційних ресурсів, інформаційних систем і засобів їх забезпечення -								ст. 2

дані -				ст. 1				
документ -	ст. 27						ст. 15	ст. 2
документ офіційний -								
доступ до інформації в системі -					ст. 1			
електронний цифровий підпис -								
засоби інформатизації -			ст. 1					
захист інформації в системі -					ст. 1			
захист інформації -			ст. 1					
знищення інформації в системі -					ст. 1			
ідентифікація персональних даних -								
Інтернет -				ст. 1				
інформація -	ст. 1			ст. 1			ст. 13	
нова інформація (знання) -								
інформація в АС -								
інформатика -								
інформатизація -			ст. 1					ст. 2
інформаційна продукція -	ст. 40						ст. 14	
інформаційна послуга -	ст. 41		ст. 1					
інформаційна технологія -			ст. 1					ст. 2
інформаційна (автоматизована) система -					ст. 1			
інформаційно-телекомунікаційна система -					ст. 1			
інформаційний продукт (продукція) -			ст. 1				ст. 14	
інформаційні ресурси -		ст.1	ст. 1				ст. 13	ст. 2
Національні інформаційні ресурси -							ст. 13	
іноземні інформаційні ресурси -							ст. 13	
міжнародні інформаційні ресурси -							ст. 13	
відомчі інформаційні ресурси -							ст. 13	
інформаційний ринок -		ст.1. Розділ IV						
інформаційний суверенітет держави -			ст. 1		ст. 1			
інформаційні процеси -								ст. 2
інформаційні ресурси спільного користування -		ст. 1						
інформація про громадян -								ст. 2
конфіденційна інформація -								ст. 2
користувач інформації в системі -					ст. 1			ст. 2
науково-технічна інформація -		ст. 1						

науково-інформаційна діяльність -		ст. 1						
несанкціоновані дії щодо інформації в системі -					ст. 1			
окреме завдання -			ст. 1					
обробка інформації в системі -					ст. 1			
обробка персональних даних -								
персональні дані -								
порушення цілісності інформації в системі -					ст. 1			
порядок доступу до інформації в системі -					ст. 1			
право власності на персональні дані -								
проект інформатизації -			ст. 1					
порядок доступу до інформації в системі -					ст. 1			
міжнародний інформаційний обмін -								
мережа телекомунікацій -				ст. 1				
обробка інформації в системі -				ст. 1				
телекомунікації -				ст. 1				
телекомунікаційна система -					ст. 1			
технічний захист інформації -					ст. 1			
Стаття... Засади інформаційного законодавства							Книга 1 глава 1	
Стаття... Мета і завдання інформаційного законодавства	ст. 2			ст. 2			ст. 1	
Стаття... Сфера дії інформаційного законодавства	ст. 3			ст. 5				
Стаття... Законодавство та підзаконні акти	ст. 4	ст. 4		ст. 4			ст. 3	
Стаття... Мова інформаційних відносин	ст. 11			ст. 7				
Розділ 2. Державна інформаційна політика				Глава 2				
Стаття... Основні принципи	ст. 5			ст. 6			ст. 2	
Стаття... Головні напрями і функції	ст. 6						ст. 12	ст. 3
Стаття... Національна інформаційна інфраструктура							ст. 16	
Розділ 3. Суб'єкти інформаційних відносин	ст. 7	ст. 3					ст. 10	
Глава... Права та основні обов'язки								
Стаття... Визначення суб'єктів (учасників)	ст. 42							
Стаття .. Права суб'єктів (учасників)	ст. 9, 43	ст. 5,7					ст. 4	
Стаття... Обмеження прав							ст. 5	
Стаття... Основні обов'язки суб'єктів (учасників)	ст. 44							
Стаття...Суб'єкти інформаційної інфраструктури							ст. 19	

Глава... Право власності на інформацію		ст. 6					ст. 55	
Стаття... Визначення права власності	ст. 38							
Стаття... Підстави виникнення права власності	ст. 38	ст. 6,7						
Стаття... Особиста власність		ст. 6						
Стаття... Спільна власність	ст. 38	ст. 6						
Стаття... Державна власність	ст. 38	ст. 6						
Стаття... Обмеження права власності							ст. 7	
Стаття... Інформація як товар	ст. 39	ст. 13						
Глава... Інформаційно-інфраструктурні відносини							Книга 3, розділ 1	
Розділ 4. Об'єкти інформаційних відносин	ст. 8	ст. 2					ст. 9	
Глава... Інформація, інформаційний продукт, інформаційний ресурс								
Стаття... Інформація та нова інформація								
Стаття... Інформаційна продукція	ст. 40						ст. 14	
Стаття... Інформаційна технологія			ст. 1					
Стаття... Інформаційний ресурс		ст. 1	ст. 1					ст. 2
Глава... Правовий режим інформації							Книга 2 розділ 2 ст. 46	
Стаття...Відкрита інформація							ст. 47	
Стаття... Обов'язковість публікації							ст. 48	
Стаття... Право на отримання інформації							ст. 49	
Стаття... Обмеженість на обов'язковість публікації							ст. 50	
Стаття... Інформація з обмеженим доступом							глава 3	
Стаття... Конфіденційна інформація							ст. 50	
Стаття... Таємна інформація							ст. 52	
Стаття... Інформація обмеженого користування							глава 4	
Глава... Види інформації	ст. 18							
Стаття... Інформація щодо прав і свобод людини								
Стаття... Соціологічна інформація	ст. 25							
Стаття... Статистична інформація	ст. 19						ст. 29-31	
Стаття... Правова інформація	ст. 22							
Стаття... Персональні дані	ст. 23							

Стаття... Масова інформація та її засоби	ст. 20						
Стаття... Інформація довідково-енциклопедичного змісту	ст. 24						
Стаття... Інформація органів державної влади та місцевого самоврядування	ст. 21					ст. 32-34	
Розділ 5. Галузі, джерела інформації, інформаційних продуктів, інформаційних ресурсів							
Глава... Галузі інформації							
Стаття... Визначення галузей	ст. 17						
Стаття... Основні галузі	ст. 17						
Глава... Джерела і бази даних (інформації)							
Стаття... Джерела даних (інформації)	ст. 26						
Стаття... Джерела інформаційних продуктів і інформаційних ресурсів							
Стаття... Бази даних (банки даних, бази знань)							
Розділ 6. Інформаційна діяльність та її види							
Глава... Інформаційна діяльність							
Стаття... Визначення інформаційної діяльності	ст. 12	ст. 1					
Стаття... Основні напрями інформаційної діяльності	ст. 13						
Глава... Основні види інформаційної діяльності	ст. 14						
Стаття... Створення інформації						Книга 2 Глава 2	
Стаття... Одержання інформації	ст. 14	ст. 12					
Стаття... Накопичення інформації							
Стаття... Обробка інформації				ст. 8			
Стаття... Використання інформації	ст. 14					Книга 2 Глава 4	
Стаття... Поширення інформації	ст. 14					Книга 2 Глава 3, ст. 39, 40	
Стаття... Зберігання інформації	ст. 14					Книга 2 Глава 5	
Стаття... Захист інформації				ст. 9			
Стаття... Знищення інформації						Книга 2 Глава 6	

Стаття... Обіг інформації						ст. 20	
Стаття... Освіта щодо інформаційної діяльності	ст. 15						
Стаття... Організація досліджень щодо інформаційної діяльності	ст. 16						
Розділ 7. Інформаційні послуги						ст. 18, Книга 3, Розділ 2	
Глава... Загальні вимоги							
Стаття... Умови надання інформаційних послуг		ст. 15					
Стаття... Відносини між власником даних і споживачем		ст. 7					
Стаття... Відносини між власником даних і посередником		ст. 7					
Стаття... Відносини між виробником даних і споживачем		ст. 16					
Стаття... Відносини між власником даних і власником системи				ст. 5			
Стаття... Відносини між власником системи і користувачем				ст. 6			
Стаття... Відносини між власниками систем				ст. 7			
Глава... Телекомунікаційні послуги			Глава 10				
Стаття... Загальнодоступні телекомунікаційні послуги			ст. 62				
Стаття... Порядок надання та отримання			ст. 63				
Глава... Споживачі							
Стаття... Права споживачів			ст. 32				
Стаття... Обов'язки споживачів			ст. 33				
Стаття... Захист інтересів споживачів			ст. 35				
Стаття... Відповідальність споживачів			ст. 36				
Глава... Оператори та провайдери			Глава 7				
Стаття... Правові основи діяльності			ст. 37				
Стаття... Права			ст. 38				
Стаття... Обов'язки			ст. 39				
Стаття... Відповідальність			ст. 40				
Розділ 8. Інформаційні ресурси							Глава 2
Глава... Основи правового режиму							ст. 4
Стаття... Документування							ст. 5
Стаття... Інформаційні ресурси як об'єкт права власності							ст. 6
Стаття... Державні інформаційні ресурси							ст. 7

Стаття... Надання документованої інформації для формування державних інформаційних ресурсів							ст. 8
Стаття... Віднесення інформаційних ресурсів до національного надбання							ст. 9
Глава... Доступ до документів							
Стаття... Режим доступу до даних	ст. 28						ст. 10
Стаття... Доступ до відкритих даних	ст. 29						ст. 10
Стаття... Доступ до даних з обмеженим доступом	ст. 30						ст. 10
Стаття... Доступ громадян до персональних даних	ст. 31						ст. 11, 14
Стаття... Гарантії надання інформації							ст. 13
Стаття... Реалізація права доступу							ст. 12
Стаття... Обов'язки та відповідальність володільця інформаційних ресурсів							ст. 15
Стаття... Інформаційний запит щодо доступу до офіційних документів і запит щодо надання письмових або усних відомостей	ст. 32						
Стаття... Термін розгляду запиту щодо доступу до офіційних документів	ст. 33						
Стаття... Відмова та відстрочка задоволення запиту щодо доступу до офіційних документів	ст. 34						ст. 13
Стаття... Оскарження відмови і відстрочки задоволення запиту щодо доступу до офіційних документів	ст. 35						ст.13
Стаття... Порядок відшкодування витрат, пов'язаних із задоволенням запитів щодо доступу до офіційних документів і надання письмових відомостей	ст. 36						
Стаття... Документи та дані, що не підлягають наданню для ознайомлення за запитами	ст. 37						
Розділ 9. Інформаційні системи, інформаційні технології і засоби їх забезпечення						Книга 3 розділ 3	Глава 4
Глава... Загальні вимоги							
Стаття... Розробка і впровадження							ст. 16
Стаття... Право власності							ст. 17
Стаття... Право авторства							ст. 18
Глава... Технічні засоби							

Стаття... Види телекомунікаційних мереж				Глава 5				
Стаття... Стандартизація				Глава 4				
Стаття... Сертифікація								ст. 19
Стаття... Взаємоз'єднання телекомунікаційних мереж				Глава 9				
Стаття... Номерний ресурс				Глава 11				
Глава... Регулювання у сфері телекомунікацій				Глава 3				
Стаття... Мета				ст. 16				
Стаття... Органи регулювання				ст. 17				
Стаття... Нагляд за ринком				ст. 18				
Стаття... Регулювання доступу до ринку (ліцензії)				Глава 8				
Розділ 10. Інформаційне забезпечення інтелектуальної свободи								
Глава... Інтелектуальна свобода								
Стаття... Визначення інтелектуальної свободи								
Стаття... Принципи забезпечення інтелектуальної активності і свободи								
Глава... Інформаційна свобода як гарантія інтелектуальної свободи								
Стаття... Функции государства и его органов в информационной сфере							Книга 1 глава 4	
Стаття... Інформація, одержання, використання і зберігання якої належить до виключних функцій держави								
Стаття... Оприлюднювання інформації критичного змісту								
Стаття... Доведення до відома громадськості інформації про виборчих осіб								
Стаття... Гарантії свободи інтелектуального самовираження журналістів								
Стаття... Свобода наукових стратегій і переконань								
Стаття... Інтелектуальна свобода в системі державної освіти								
Розділ 11. Підтримка інформаційної безпеки							Книга 4	Глава 5
Глава... Загальні вимоги								
Стаття... Мета інформаційної безпеки								ст. 20
Стаття... Права та обов'язки суб'єктів								ст. 22

Стаття... Встановлення вимог і правил захисту даних								ст. 21
Стаття... Забезпечення захисту від недостовірної, неправдивої інформації								
Стаття... Затримання інформаційного обміну								
Глава... Захист даних								
Стаття... Політика щодо захисту даних								
Стаття... Державне управління захистом даних								
Стаття... Служби захисту даних								
Стаття... Фінансування робіт із захисту даних								
Глава... Захист від маніпулювання свідомістю								
Стаття... Організаційно-технічний захист								
Стаття... Програмно-технологічний захист								
Розділ 12. Охорона прав в інформаційних відносинах								
Глава... Охорона інформації								
Стаття... Охорона прав на інформацію	ст. 45							
Стаття... Неприпустимість зловживання правом на інформацію	ст. 46							
Глава... Охорона авторських і суміжних прав								
Стаття... Охорона авторських прав								
Стаття... Охорона суміжних прав								
Глава... Охорона патентних прав								
Стаття... Охорона прав на винаходи і корисні моделі								
Стаття... Охорона прав на знаки для товарів і послуг								
Стаття... Охорона прав на промислові зразки								
Розділ 13. Захист прав в інформаційних відносинах							ст. 8	ст. 23, 24
Глава... Захист прав в адміністративно-правовому порядку								
Глава... Захист прав у кримінально-правовому порядку								
Глава... Захист прав через прокуратуру								
Глава... Захист прав через Уповноваженого Верховної Ради України								
Глава... Судовий захист прав у цивільно-правовому								

порядку								
Глава... Захист прав у міжнародних судах								
Розділ 14. Відповідальність								
Стаття... Відповідальність за порушення прав	ст. 47	ст. 19						
Стаття... Відповідальність за порушення порядку і правил захисту інформації					ст. 11			
Стаття... Порядок оскарження протиправних діянь	ст. 48							
Стаття... Відшкодування матеріальної та моральної шкоди за порушення прав	ст. 49							
Розділ 15. Дія та застосування норм міжнародного права								
Стаття... Міжнародна інформаційна діяльність	ст. 50	ст. 20, 22						
Стаття... Міжнародне співробітництво при виконанні Національної програми інформатизації					ст. 27			
Стаття... Міжнародні договори (співробітництво)	ст. 51				ст. 28			
Стаття... Інформаційний суверенітет	ст. 53							
Стаття... Гарантії інформаційного суверенітету	ст. 54	ст. 23						
Стаття... Передача даних через кордони	ст. 52	ст. 21						
Стаття... Підтримка громадян, які проживають за кордоном								
Частина II. Особлива частина								
Розділ 16. Основні інститути інформаційного права								
Глава 16-1. Засоби масової інформації						див. проект Інформаційного кодексу	ст. 26, 27, 36, 37, 38, 39	
Глава 16-2. Наука та освіта								
Стаття... Державна політика у сфері науки та освіти (науково-технічної інформації)		Розділ III						
Стаття... Склад і структура національної системи науково-технічної інформації		ст. 8						
Стаття... Основні завдання національної системи науково-технічної інформації		ст. 9						
Стаття... Інформаційні ресурси національної системи		ст. 10						

науково-технічної інформації							
Стаття... Державна реєстрація, облік і використання результатів науково-технічної діяльності	ст. 11						
Стаття... Державна підтримка науково-технічної діяльності	ст. 17, 18						
Глава 16-3. Інформатизація та Національна програма інформатизації						Книга 3 глава 2	
Стаття... Визначення		ст. 2					
Стаття... Зміст		ст. 2					
Стаття... Формування		ст. 2					
Стаття... Завдання законодавства		ст. 3					
Стаття... Сфера дії та суб'єкти		ст. 4					
Стаття... Головна мета та основні завдання		ст. 5					
Стаття... Функції органів державної влади з реалізації		ст. 6					
Стаття... Взаємозв'язок Національної програми інформатизації та системи планування економічного і соціального розвитку України		ст. 7					
Стаття... Порядок представлення та затвердження Національної програми інформатизації		ст. 9					
Стаття... Замовники		ст. 10					
Стаття... Конкурс проектів		ст. 13					
Стаття... Експертиза окремих завдань (проектів)		ст. 14					
Стаття... Виконавці		ст. 15					
Стаття... Умови вибору нерезидентів		ст. 16					
Стаття... Галузеві програми		ст. 17					
Стаття... Регіональні програми		ст. 18					
Стаття... Програми та проекти інформатизації органів місцевого самоврядування		ст. 19					
Стаття... Порядок закупівлі програмних та технічних засобів		ст. 20					
Стаття... Порядок використання програмних засобів		ст. 21					
Стаття... Права та обов'язки Генерального державного замовника		ст. 22					
Стаття... Права та обов'язки суб'єктів		ст. 23					
Стаття... Фінансове забезпечення та економічне стимулювання		ст. 24, 25					

Стаття... Державний контроль за формуванням та використанням Національної програми інформатизації			ст. 26				
Розділ 17. Інші інститути інформаційного права							
Глава 17-1. Захист персональних даних							
Глава 17-2. Зв'язок та телекомунікації							
Глава 17-3. Електронні документи, електронний цифровий підпис та електронний документообіг							
Глава 17-4. Дистанційне навчання							
Глава 17-5. Телемедицина							
Глава 17-6. Електронна торгівля (комерція)							
Глава 17-7. Електронне урядування							
Глава 17-8. Бібліотечна та архівна справа							
Глава 17-9. Державні інформаційні стандарти							
Глава 17-10. Комерційна та державна таємниця							
Частина III. Заключна частина							
Розділ 18. Прикінцеві та перехідні положення							
Стаття... Гарантії забезпечення прав	ст. 10					ст. 6	

Додаток 5

Класифікація предметних областей в інформаційній сфері

Предмет правового регулювання	Суб'єкти правового регулювання	Об'єкти правового регулювання	Об'єкті інформаційної діяльності	Суб'єкти права власності
Суспільні відносини, що виникають при реалізації та забезпеченні процесів інформаційної діяльності	Громадяни; об'єднання громадян; юридичні особи; державні органи	Інформаційна діяльність – сукупність дій, спрямованих на задоволення інформаційних потреб особи, суспільства і держави	Інформація, дані, інформаційний продукт, інформаційний ресурс, інформаційна послуга	Власники; володільці; розпорядники; споживачі

Види інформаційної діяльності	Області правового регулювання
Створення; пошук, отримання, збір, накопичення, зберігання; охорона, розповсюдження, реалізація; захист, споживання тощо. У автоматизованих системах узагальнюючий термін – обробка об'єктів інформаційної діяльності (обробка даних)	Духовна; фінансово-економічна; політична; наукова і науково-технічна; екологічна; персональних даних; статистична, міжнародна

1. Області об'єктів інформаційної діяльності

1.1 Інформація за змістом відомостей (і види)
- наукова та науково-технічна,
- масова (соціальна),
- персональні дані,
- правова інформація,
- фінансово-економічна,
- політична,
- державних органів та органів місцевого самоврядування,
- статистична,
- про стандарти та метрологічна,
- про охорону здоров'я,
- про надзвичайні події,
- довідково-енциклопедична та ін. види інформації

1.2 Інформація за режимом доступу :
- відкрита (без обмеження доступу);
- з обмеженим доступом:
  - персональні дані;
  - конфіденційна;
  - комерційна таємниця,
  - професійна таємниця;
  - службова таємниця,
  - медична таємниця;
  - державна таємниця

1.3 Інформація щодо її функцій:
- призначення: довідкова документальна;
- функціонально-організаційної спрямованості: наукова, освітянська, управлінська, комерційна, масова;
- відомостей: бібліографічна, реферативна, оглядова;
- достовірності: наукова, офіційна, неофіційна,
- розподілу: періодична, по запиту, депонована;
- використання: вхідна, робоча, вихідна;
- носіїв надання: письмова, електронна, звукова, графічна

1.4 Інформація за методом обробки:
- ручна;
- механізована;
- автоматизована

1.5 Інформація за засобами формування та поширення:
- стаціонарні,
- мобільні

1.6 Інформація за видами носіїв:
- на папері,
- на е-носіях,
- на екрані, у пам'яті ПК,
- у мережах зв'язку

1.7 Інформація за методом організації ресурсів:
- традиційні форми:
  - документи;
  - масиви документів;
  - фонди документів;
  - архіви;
- автоматизовані форми:
  - банки та бази даних;
  - бази знань;
  - сайти та ін. системи

1.8 Види інформаційних ресурсів:
- ідеї і знання, що перетворені у інформацію та інформаційні продукти;
- методи і форми накопичення, збереження та поширення інформаційних продуктів та надання технології

1.9 Області формування інформаційних ресурсів:
- технологічна;
- управлінська;
- комерційна (фінансова, банківська тощо)

1.10 Інформаційні продукти:
- форми продуктів
  - документи на паперових носіях (книги, брошури, статті, монографії, рукописи, звіти, періодичні видання);
  - документи на е-носіях
- види продуктів:
  - наукові: ідеї, теорії, концепції, відкриття (закономірності, властивості, явища), факти,
  - відомості ЗМІ,
  - інші відомості

1.11 Інформаційні технології та засоби їх забезпечення.
- автоматизовані інформаційні системи, мережі:
  - бази даних та знань;
  - системи управління базами;
  - експертні системи;
  - інформаційно-обчислювальні системи, ПК;
  - інформаційні мережі.
- технічні засоби:
  - засоби обчислювальної техніки та ПК,
  - копіювально-розмножувальна техніка,
  - оргтехніка,
  - засоби зв'язку,
  - засоби телекомунікації,
- програмні засоби
  - операційні системи,
  - прикладні програми,
- лінгвістичні засоби
  - словники,
  - тезауруси,
  - класифікатори тощо;
- види розподілу інформації (види пошуку)
  - за логічними ознаками ягідно сфери, галузі, області, інституційності, предметів та проблем,
  - за формальними ознаками, ягідно алфавіту, нумерації, хронології, територіальності, авторського (предметного) порядку;
- технолог. забезпечення:
  - інформаційні технології,
  - інструкції, правила;
- організаційно-правові засоби
  - положення, статути,
  - посадові інструкції,
  - нормативно-технічні документи

1.12 Інформація, дані, інформаційні продукти, технології, інформаційні ресурси за формою власності:
- приватна,
- комунальна,
- державна.

1.13 Інформаційні послуги:
- види послуг
  - з обслуговування: пошук, збір (набуття, придбан-

1.14 Інформаційна безпека:
- об'єкти безпеки
  - інформація, дані, інформаційні продукти, техно-

	ня), обробка, накопичення, збереження, поширення (розповсюдження, реалізація) даних чи документів; - зі створення інформаційних технологій, продуктів, аудіо-, відео-, комп'ютерних програм; - консультаційні (консалтинг). • форми організації та надання послуг: - правові форми: обов'язкове надання інформації на підставі закону або договору, ін. правові форми інформаційного обслуговування; - організаційні форми: самообслуговування, через посередника; • умови оплати послуг: - за плату; - безоплатне; - пільгове	логії, ресурси, послуги; - носії; - інфраструктура (засоби створення, обробки, поширення продуктів; засоби зв'язку та мереж). • система компонентів: - виробництво продуктів; - надання продуктів; - виробництво засобів виробництва продуктів; - виробництво технологій; - накопичення і збереження продуктів; - сервісне обслуговування інфраструктури; - підготовка кадрів; • види захисту: - прав людини і основоположних свобод; - інтересів суспільства і держави; - підприємницької, фінансової і комерційної діяльності; - документованої інформації, інформаційних продуктів та ресурсів; - інформаційних технологій, систем, мереж, засобів забезпечення від неправомірних дій; • механізми захисту: - нормативно-правові; - адміністративні (економічні, організаційні); - апаратно-технічні; - програмні

2. Області суб'єктів інформаційної діяльності		
2.1. Громадяни, в тому числі іноземці, та особи без громадянства. **Об'єднання громадян**, у тому числі юридичні особи.	**2.2. Організації** власники та володільці інформаційних ресурсів, продуктів і послуг: • бібліотеки; • архіви та музеї; • інформаційні центри; • інформаційні фонди; • інформаційні агентства; • ін. органи масової інформації; • ін. організації-розпорядники інформаційних ресурсів	**2.3. Органи державної влади:** • Верховна Рада; • Президент; • Уряд; • Конституційний Суд; • Верховний Суд; • Вищий арбітражний Суд; • органи виконавчої влади; • органи місцевого самоврядування • органи представницької влади; • ін. органи судової влади

3. Області суспільних відносин, що підлягають правовому регулюванню			
3.1. Права: • права людини і свободи; • власності на інформаційні продукти і інформаційні ресурси; • власності на персональні дані; • інтелектуальної власності; • доступу, одержання і використання інформації; • одержання і використання інформаційних послуг; • інформаційної безпеки; • на міжнародну діяльність	**3.2. Обмеження прав:** • на діяльність; • майнових прав; • права на доступ і поширення інформації та даних, • особистих прав у зв'язку з захистом державної таємниці; • права на особисту таємницю за умов правоохоронної діяльності	**3.3. Зобов'язання:** • захисту прав осіб, інтересів суспільства і держави; • захисту персональних даних; • щодо розвитку інформатизації; • щодо формування інформаційних ресурсів, продуктів; • щодо доступу до інформації та даних; • із використання інформації у відповідності з законодавством; • із надання інформації, інформаційних продуктів і послуг	**3.4. Відповідальність:** • за порушення прав та свобод, інтересів суспільства і держави; • за порушення роботи систем та засобів інформаційної інфраструктури; • за створення та поширення недоброякісних інформаційних продуктів, ресурсів; • за нав'язування інформації та послуг; • за невиконання зобов'язань щодо інформаційної діяльності

Додаток 6

Матриця
щодо упорядкування відносин в інформаційній сфері

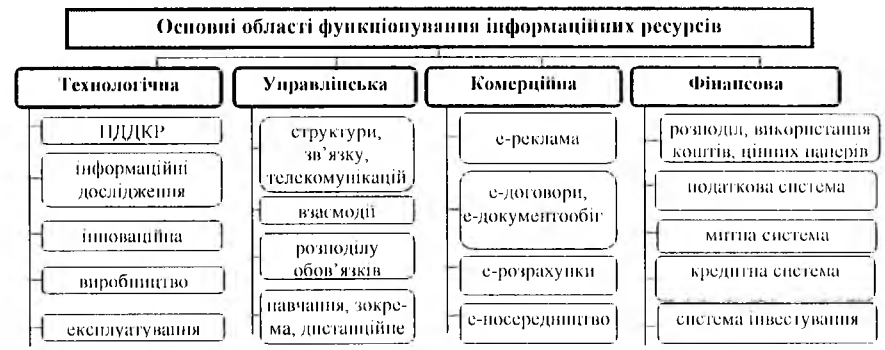
Категорії відносин / Предметні області діяльності	ПРАВО	ОБМЕЖЕННЯ ПРАВА	ЗОБОВ'ЯЗАННЯ	ВІДПОВІДАЛЬНІСТЬ
СТВОРЕННЯ ТА ДОКУМЕНТУВАННЯ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНИХ ПРОДУКТІВ (ІП), ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ (ІТ):	на створення інформації, ІП, ІКТ; на власність на інформацію, ІП, ІТ, зокрема, на інтелектуальну власність	на створення інформації, ІП, ІКТ; обмеження права на власність, зокрема, на інтелектуальну власність	щодо створення інформації, ІП, ІКТ; зобов'язання щодо права на власність, зокрема, на інтелектуальну власність	за недостовірну, протиправну інформацію ІП, ІКТ; за комп'ютерні злочини; за порушення права власності; за порушення права інформаційної та інтелектуальної свободи
ЗБИРАННЯ, ЗБЕРІГАННЯ ІНФОРМАЦІЙНИХ ПРОДУКТІВ (ІП), ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ (ІКТ) ЩОДО ФОРМУВАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ (ІР), ЗОКРЕМА, БАЗ ТА БАНКІВ ДАНИХ	на формування ІР; на об'єкти інтелектуальної власності; на доступ до ІР та їх використання	на формування ІР; на доступ до ІР та їх використання; на право власності	щодо формування ІР; доступу до ІР та їх використання; щодо права власності	за порушення правил формування ІР та доступу до них; за комп'ютерні злочини; неподання інформаційних послуг; за порушення права власності
ВИКОРИСТАННЯ ТА ПОШИРЕННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ (ІР), ІНФОРМАЦІЙНИХ ПРОДУКТІВ (ІП) ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ (ІКТ):	на використання та поширення ІР, ІП, ІКТ; на надання інформаційних послуг	на використання та поширення ІР, ІП, ІКТ; на надання інформаційних послуг; на право власності	щодо використання та поширення ІР ІП, ІКТ; надання інформаційних послуг; забезпечення права власності	за порушення правил використання, надання або неподання ІР, ІП, ІКТ; за порушення правил щодо інформаційних послуг; за порушення права власності; за комп'ютерні злочини
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ:	на захист прав і свобод людини; на захист ІР, ІП і ІКТ; на захист власності на ІР, ІП, ІКТ; на захист прав щодо надання інформаційних послуг	на розкриття особистої, державної, комерційної таємниці	щодо захисту прав і свобод людини; захисту ІР, ІП і ІКТ; захисту власності на ІР, ІП, ІКТ; захисту прав щодо надання інформаційних послуг; захисту таємниці (особистої, державної)	за порушення прав і свобод людини; за порушення таємниці; за комп'ютерні злочини; за порушення захисту ІР, ІП, ІКТ і інформаційних послуг; захисту персональних даних, таємниці (особистої, державної)

Додаток 7

Структурна схема щодо інформаційних ресурсів

Інформаційні ресурси – організована сукупність інформаційних продуктів, інформаційно-комп'ютерних технологій певного призначення, які необхідні для забезпечення інформаційних потреб громадян, суспільства і держави у визначеній сфері життя чи діяльності

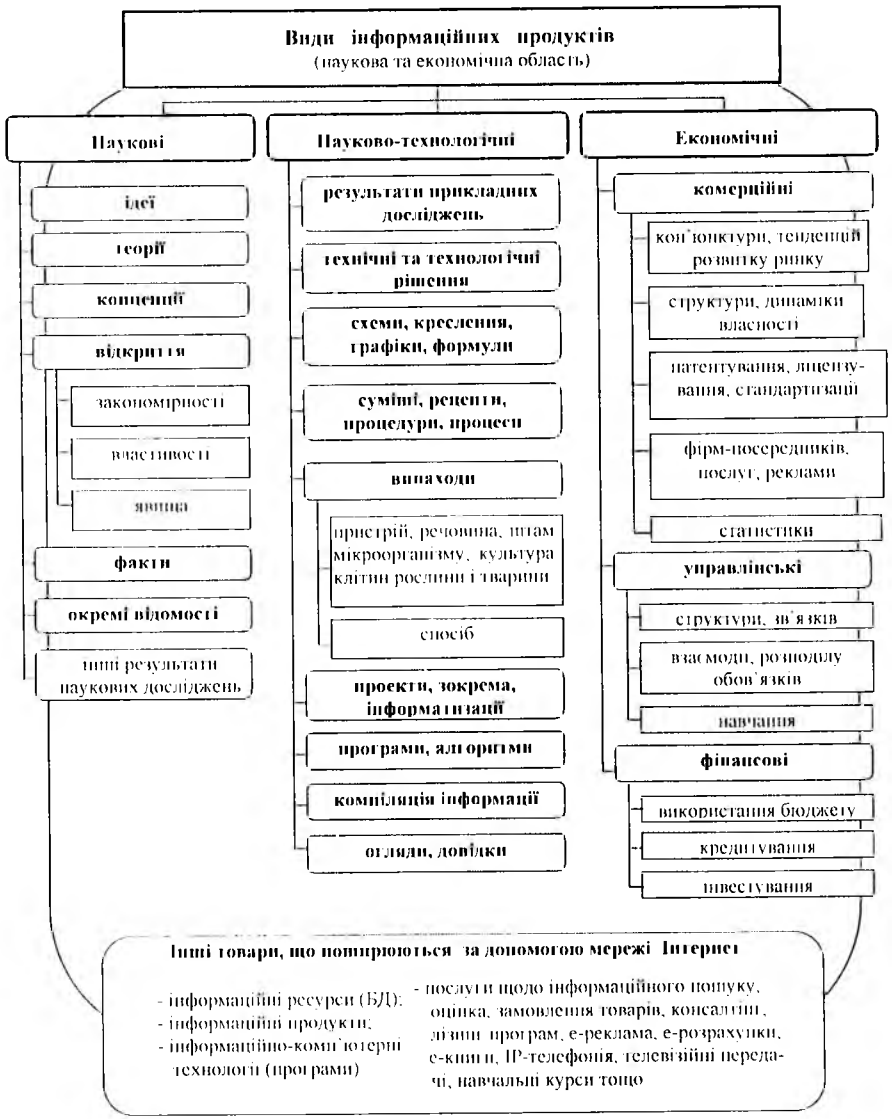
- Ідеї та знання, що перетворені в дані та інформаційні продукти, які зафіксовано на матеріальних носіях
- Методи й форми збирання, зберігання та поширення інформаційних продуктів і надання інформаційних послуг
- Інформаційно-комп'ютерні технології, новітні інформаційні технології та технології щодо енергетичних полів



Класифікація засобів забезпечення інформаційно-комп'ютерних технологій

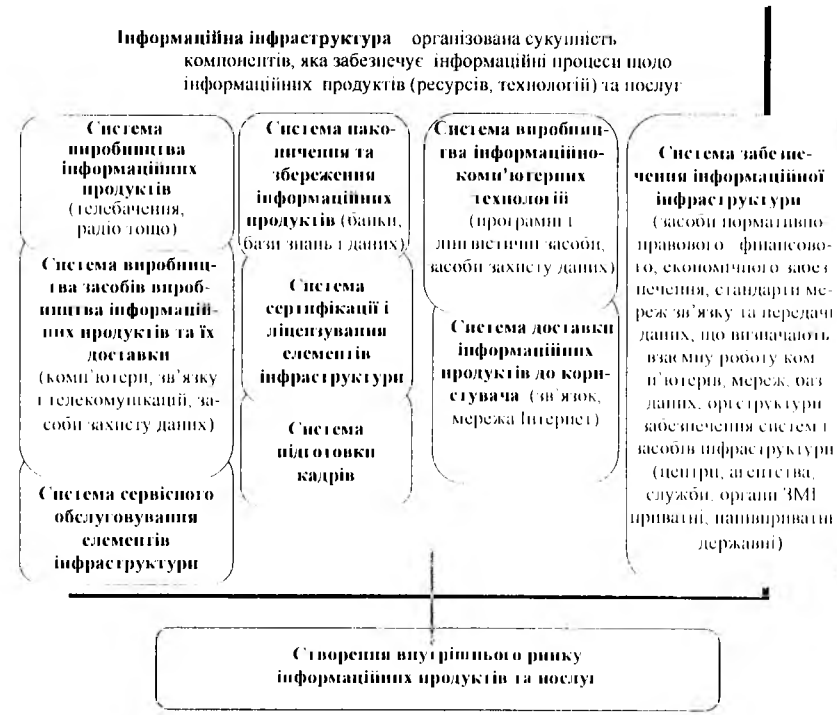
Автоматизовані інформаційні системи та мережі	Технічні	Програмні	Лінгвістичні	Організаційно-правові
- бази знань чи даних; - банки даних; - експертні системи; - системи управління; - системи проектування; - системи обробки даних; - системи ІПТ; - системи забезпечення ІПК; - телекомунікації	- ПК; - копіювально-розмножувальна; - оргтехніка, - засоби зв'язку; - засоби телекомунікації; - інші засоби	- операційні системи; - прикладні програми; - інше	- словники, - тезауруси; - класифікатори - інше	- положення, статут; - порядок реалізації завдань, функцій; - посадові інструкції; - порядок користування; - нормативно-технічні документи

Продовження
додатка 7



Додаток 8

Структурна схема щодо інформаційної інфраструктури



поступове входження держави у

Глобальне інформаційно-комерційне середовище – світове суспільство, в якому створюються організаційно-правові прецеденти е-комерції на базі регіонально-географічного використання інформаційно-комп'ютерних технологій за допомогою мережі Інтернет тощо:

* пошук, вибір, замовлення продуктів, товарів та послуг;
* е-реклама; е-документообіг; е-розрахунки, е-банкінг; консалтинг, лізинг програмного забезпечення;
* інші сервіси за допомогою інформаційно-комп'ютерних технологій та телекомунікаційних мереж

Додаток 9

Структурна схема щодо індустрії інформації

Індустрія інформації виробництво інформації, інформаційних ресурсів, продуктів і технологій

Мета індустрії інформації:
забезпечення використання знань та ефективного управління потоками даних, до яких пристосована інформація;
оснащення технічними (електронними) засобами забезпечення інформаційних та інтелектуальних процесів

- Виробництво засобів мікроелектроніки і комп'ютерної техніки
- Виробництво телекомунікаційної техніки, мереж і засобів зв'язку
- Формування інформаційних мереж і структур
- Створення інформаційних ресурсів (баз, банків даних)
- Виробництво інформаційних продуктів
- Виробництво програмних продуктів (технологій)
- Формування ринку інформаційних ресурсів, продуктів, технологій і послуг
- Виробництво засобів сервісного обслуговування
- Виробництво систем зі штучним інтелектом
- Нормативно-правове та організаційне забезпечення

Області індустрії інформації:

наукові і науково-технічні дослідження; освіта; проектування; промислове виробництво; ЗМІ; е-уряд; е-комерція; е-банкінг; е-медицина; е-будинок; е-розваги; забезпечення різноманітних видів діяльності

Індустрія інформації щодо ЗМІ

Комерційний сектор – орієнтування на ринковий попит інформації ЗМІ: журнали, газети, книги, теле-, радіорепортажі, відеовидання (аудіокасети, диски тощо)	**Некомерційний сектор** – орієнтування на політику, соціологію тощо, стосовно діяльності партій, суспільних організацій, різних груп тощо

Додаток 10

Структурна схема щодо захисту інформації та даних

Засоби захисту інформації та даних

Засоби захисту повинні забезпечити:
- захист від несанкціонованого користування даними, до яких пристосована інформація;
- захист від знищення, модифікації, зміни, зчитування, копіювання даних тощо;
- захист від даних, що нав'язуються

Юридичні (формування статусу та норм правового регулювання різних суб'єктів)

- законодавство,
- нормативні акти,
- акти організацій,

Адміністративні (створення та забезпечення функціонування механізму захисту даних та захисту від даних)

Адміністративно-організаційні

Апаратні (управління доступом до автоматизованих засобів і систем)

- захисні ключі, дескриптори;
- кодуючі та декодуючі пристрої;
- екранування автоматизованих засобів і систем від перехоплення і подальшого розшифровування електромагнітного випромінювання

Програмні (управління доступом до даних захист від даних)

- включення до операційної системи спеціальних програм,
- присвоєння файлам міток, вказуючи на них ім'ям користувача, що має право доступу до цих файлів,
- перевірка права користувача через запит пароля,
- шифрування даних, що надсилаються по телекомунікаційних мереж

Адміністративно-економічне (мотивація, економічне стимулювання захисту даних та захисту від даних, до яких пристосована інформація)

- формування економічних умов мотивації захисту прав на дані,
- захист даних шляхом рекламування та пропаганди;
- розробка системи економічних та статистичних показників, що характеризують ефективність системи захисту даних;
- регулярне повідомлення про зміни та виявлені помилки,
- проведення семінарів і курсів навчання,
- видання методичних матеріалів;
- надання консультацій;
- стимулювання інвестицій у засоби захисту даних

створення режиму доступу користувачів до автоматизованих засобів і систем (ПК, периферійне обладнання, засоби телекомунікації), облік користувачів;
облік і контроль використання носіїв;
реєстрація доступу, вводу даних, джерел, облік і нагляд за спеціалістами, що здійснюють ремонт, наладку, завантаження автоматизованих засобів і систем,
виявлення та реєстрація фактів протиправних намірів або дій, витоку інформації, збоїв автоматизованих засобів і систем,
систем захисту даних та захисту від даних,
аналіз даних фактів протиправних намірів або дій, витоку інформації, збоїв автоматизованих засобів і систем, систем захисту даних та захисту від даних,
вжиття заходів з недопущення порушень юридичних засобів захисту даних та інформації,
реєстрація баз даних та ліцензування діяльності щодо захисту персональних даних

Структурна схема щодо інформаційної безпеки

Інформаційна безпека - стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Інформаційна безпека передбачає забезпечення єдності функціонування елементів інформаційної інфраструктури щодо захисту інформації:

- виробництва інформаційних продуктів (друкованих видань);
- постачання інформаційних продуктів до користувача (мережі радіо-, теле-, телефонні комунікації);
- виробництва засобів виробництва інформаційних продуктів і засобів їх постачання;
- виробництві інформаційно безпечних технологій;
- накопичення і зберігання інформаційних продуктів;
- сервісного обслуговування елементів інфраструктури.

Об'єкти безпеки (об'єкти відносин у галузі безпеки)	**Суб'єкти безпеки** (суб'єкти відносин у галузі безпеки)	**Форми захисту інформації та даних**
• інформація, дані, інформаційні технології, продукти, програми, ресурси на всіх видах носіїв, інформаційні послуги. • ності інформації; • інформаційна інфраструктура. - засоби створення, зберігання (баз, банків даних та знань), обробки і поширення інформації, інформаційних ресурсів, продуктів; - створення і поширення інформаційних технологій (програмні засоби); - засоби зв'язку і телекомунікаційні мережі; - засоби сервісного обслуговування; - засоби підготовки кадрів	• особа – права і свободи; • суспільство – матеріальні і духовні цінності; • держава – конституційний лад, суверенітет і територіальність	• правові (інститут інтелектуальної власності і інститут речової власності). • адміністративно-організаційні; • апаратно-технічні; • програмні
Структура інформаційної безпеки	**Заходи захисту інформації в організаціях**	
• захищеність інформації, інформаційних ресурсів; • захищеність інформаційних прав і свобод; • захищеність особи, суспільства і держави від маніпулювання інформацією, інформаційними ресурсами з метою впливу на суспільну свідомість	• робота з кадрами (контракт, навчання, нагляд і контроль); • облік і грифування інформації; • облік автоматизованих засобів; • створення системи обмеження і забезпечення порядку доступу до інформації і автоматизованих систем; • облік засобів і матеріалів розмноження; • забезпечення захисту інформації при переговорах, виставках тощо	

ТИПОВА НАВЧАЛЬНА ПРОГРАМА З ДИСЦИПЛІНИ "ІНФОРМАЦІЙНЕ ПРАВО"

(для викладання у вищих навчальних закладах за спеціальністю - "правознавство")*

Вступ

Формування в Україні інформаційного суспільства викликало виникнення нової комплексної галузі права, яка набула умовної назви – "інформаційне право".

Інформаційне право як комплексна галузь права визначає правові засади суспільних відносин щодо інформації, інформаційної діяльності, технологій їх об'єктивізації.

Головною передумовою виокремлення інформаційного права в системі права є також соціально-технологічне явище, як інформатика, інформатизація.

У пункті 8 Постанови Верховної Ради України "Про підсумки парламентських слухань "Суспільство, засоби масової інформації, влада: свобода слова і цензура в Україні" від 16 січня 2003 року №441-IV Вищій атестаційній комісії України рекомендовано ввести до переліку спеціальностей, за якими проводиться захист дисертацій на здобуття наукового ступеня кандидата наук і доктора наук, присудження наукових ступенів і присвоєння вчених звань, спеціальність "Інформаційне право".

На підставі зазначеної Постанови, рекомендації експертної ради ВАК України Президія Вищої атестаційної комісії України прийняла Постанову "Про зміну паспорта спеціальності" від 21.05.2003 року № 26-11/5, якою затвердила паспорт спеціальності 12.00.07. У цьому паспорті інформаційне право введено поряд з теорією управління, адміністративним правом і процесом, фінансовим правом (юридичні науки). Зазначене зумовило розробку програми кандидатського мінімуму для складання іспитів за спеціальністю, а також введення навчальної дисципліни у систему підготовки за спеціальністю "правознавство".

Викладання навчальної дисципліни "Інформаційне право" також рекомендується при підготовці фахівців з інших спеціальностей, особливо таких, що пов'язані з інформатикою, інформаційною безпекою, інформаційними технологіями та іншими видами інформаційної діяльності.

Типова програма навчальної дисципліни "Інформаційне право" спрямована на забезпечення відповідності та єдності науки, освіти і практики у сфері суспільних відносин щодо інформації, інформатики, інформатизації, інформаційної культури при розвитку інформаційного суспільства України як складової глобальної інформаційної цивілізації.

Ця типова програма є узагальненням багаторічного досвіду навчальних програм викладання дисципліни "Інформаційне право" у ряді вищих навчальних закладів України з кінця 90-х років XX століття.

При викладанні і вивченні навчальної дисципліни пропонується застосовувати електронні ресурси: "Система (бібліотека) баз даних і знань у галузі держави і права", створені на виконання завдань Національної програми інформатизації України та Національної програми правової освіти України, рекомендованих Міністерством освіти і науки України (грифи № 14/18.2-2150 від 28.09.2005 р. та № 1/11 від 31.01.2007 р.).

* * * * * * * * * * * *

---

* Складено **Цимбалюком В.С.,** кандидатом юридичних наук, старшим науковим співробітником.

Пояснювальна записка

Основна мета навчальної дисципліни – формування системи знань, умінь, навичок стосовно правовідносин, пов'язаних з інформацією, інформатикою, інформаційною діяльністю та інформаційною безпекою.

Основні завдання навчальної дисципліни:

- освоєння сформованих наукою теоретичних положень стосовно структури, джерел і методології права щодо інформації та правової інформатики, єдності та відмінності сутностей інформаційного права та правової інформатики;
- орієнтація в правових аспектах формування, розвитку, охорони та захисту інформаційних ресурсів єдиного інформаційного простору України;
- визначення шляхів удосконалення правових основ інформаційного простору й інформаційних ресурсів України;
- освоєння законодавчого забезпечення формування та розвитку єдиного інформаційного простору України;
- засвоєння правових основ організації та координації дій органів державної влади в єдиному інформаційному просторі України;
- орієнтація у проблемах міжнародного співробітництва в правовому регулюванні та розвитку глобального інформаційного простору.

При вивченні навчальної дисципліни **студенти повинні знати**:

- понятійний апарат, зміст, сутність інформаційного права, його зв'язки з правовою інформатикою, провідними та іншими комплексними галузями права;
- законодавство та підзаконні нормативно-правові акти щодо суспільних відносин у сфері інформації;
- основні напрями та проблеми дослідження в інформаційному праві як комплексній галузевої науці правознавства.

В результаті вивчення навчальної дисципліни **студенти повинні вміти**:

- орієнтуватися у понятійному апараті та природі інформаційного права, його зв'язку з традиційними та новими міжгалузевими інститутами галузей права;
- моделювати і застосовувати у практиці знання щодо правовідносин інформаційної діяльності різних суб'єктів, у тому числі при розвитку єдиного інформаційного простору України, правових основ організації та координації дій органів державної влади в цьому просторі;
- визначати проблеми правозастосування норм вітчизняного інформаційного права, у тому числі співвідношення їх з нормами міжнародного інформаційного права в умовах розвитку глобального інформаційного простору;
- удосконалювати знання через подальшу самоосвіту у сфері права про інформаційну діяльність в майбутній практичній, науковій роботі для розвитку правової основи інформаційного простору й інформаційних ресурсів України.

* * * * * * * * * * * *

Зміст програми за темами

ЗАГАЛЬНА ЧАСТИНА ІНФОРМАЦІЙНОГО ПРАВА

Тема 1. Сутність, зміст, структура інформаційного права

Визначення сутності та змісту інформаційного права: як комплексної галузі суспільних відносин щодо інформації, що знаходять вираз у нормативно-правових актах; як науки; як навчальної дисципліни.

Предмет інформаційного права.

Взаємозв'язок інформаційного права з іншими галузями права та його місце серед них.

Взаємозв'язок інформаційного права як науки з правовою інформатикою, правовою кібернетикою, іншими науками гуманітарного і соціально-технічного спрямування, пов'язаними з інформаційною діяльністю.

Структура, мета та завдання навчальної дисципліни "Інформаційне право".

Тема 2. Джерела інформаційного права

Визначення сутності та змісту джерел інформаційного права. Джерела формування інформаційного права, як науки. Суспільні відносини як джерело інформаційного права. Науково-технічний прогрес у галузі інформаційних технологій як джерело інформаційного права.

Інформаційне суспільство як джерело інформаційного права.

Приватноправові відносини – як джерело інформаційного права.

Міжнародні правові акти (стандарти) – як джерело національного інформаційного права.

Національне право – як джерело інформаційного законодавства.

Інформаційне законодавство: концептуальні підходи до систематизації та розвитку.

Тема 3. Методологія інформаційного права та її зв'язок з методологією правової інформатики

Поняття та сутність методології інформаційного права. Взаємозв'язок методології інформаційного права з методологіями правової інформатики, правової кібернетики та методологіями інших гуманітарних та соціально-технічних наук.

Наукові підходи пізнання як провідний чинник методології інформаційного права. Сутність системного підходу в інформаційному праві та його зв'язок з комплексним підходом. Роль методології теорії права, теорії організації управління соціальними системами та синергетики у формуванні методології інформаційного права. Застосування положень методології семантики, соціальної когнітології, семіотики та герменевтики при формуванні понятійного апарату інформаційного права та правової інформатики.

Поняття та сутність методів агрегації, інтеграції, акумуляції та гіперсистем в інформаційному праві та правовій інформатиці.

Галузевий метод інформаційного права: комплексне застосування методів провідних галузей права (адміністративного, цивільного, кримінального) та інформатики.

Концептуальні підходи формування структури та змісту інформаційного права в умовах формування єдиного інформаційного простору України та глобального інформаційного суспільства.

Критерії формування інститутів загальної, особливої та спеціальної частин інфор-

маційного права за суб'єктивними та об'єктивними ознаками.

Методологічні підходи до кодифікації інформаційного законодавства України.

Імплементація та рецепція норм міжнародної інформаційної діяльності у національному праві України.

Тема 4. Об'єкти інформаційного права

Поняття об'єктів інформаційного права. Інформація – основний об'єкт правовідносин, які виникають в процесі інформаційної діяльності.

Співвідношення категорій "інформація", "відомості", "дані", "знання", "таємниця" та ін. в інформаційній діяльності. Особливості їх застосування в нормативних актах суб'єктами правотворчості в Україні.

Види інформації за галузями застосування, їх зміст.

Інформаційні ресурси як об'єкт правовідносин.

Інформаційний простір як об'єкт інформаційного права. Поняття та сутність глобального інформаційного простору як об'єкта інформаційного права.

Зміст категорії "документ" в інформаційній діяльності.

Класифікація інформації за правовим режимом доступу.

Технічні засоби та технології як об'єкти інформаційної діяльності.

Бази даних та знань як об'єкти інформаційної діяльності.

Інформаційна діяльність як об'єкт правовідносин.

Поняття та сутність Інтернет-правовідносин.

Тема 5. Суб'єкти інформаційної діяльності

Учасники (суб'єкти) інформаційної діяльності.

Види суб'єктів інформаційної діяльності щодо суспільної організації: приватні (фізичні) особи; суспільні формування (громадські організації); юридичні особи; держава та її органи.

Види спеціальних суб'єктів інформаційної діяльності щодо правового статусу в інформаційній діяльності.

Тема 6. Принципи інформаційної діяльності

Поняття принципів інформаційного права. Роль принципів інформаційного права у реалізації інформаційної діяльності.

Співвідношення потреб, інтересів суб'єктів інформаційних правовідносин як провідний принцип інформаційного права.

Роль норм Конституції України у формуванні принципів інформаційного права.

Поняття та зміст законності інформаційної діяльності.

Право на інформацію.

Неприпустимість зловживання правом на інформацію.

Державні гарантії інформаційної діяльності.

Застосування принципів провідних галузей права у реалізації інформаційної діяльності.

Тема 7. Система регулювання інформаційної діяльності в Україні

Приватноправове регулювання інформаційної діяльності.

Публічноправове регулювання інформаційної діяльності.

Конституційно-правові засади регулювання інформаційної діяльності.

Цивільно-правове регулювання інформаційної діяльності.

Адміністративно-правове регулювання інформаційної діяльності.

Сфери спеціального законодавчого регулювання інформаційної діяльності.

Місце і роль юридико-технічних норм у регулюванні та управлінні інформаційною діяльністю (технічні стандарти, регламенти, рекомендації, положення тощо).

Тема 8. Державна політика у сфері інформаційної діяльності. Основні засади розвитку інформаційного суспільства в Україні

Поняття та сутність державної інформаційної політики, її форми, види, сутність.

Сфери державної інформаційної політики.

Роль держави у розвитку суспільної інформаційної діяльності.

Головні напрями і способи державної інформаційної політики.

Органи влади, що розробляють і здійснюють державну інформаційну політику.

Національні, державні та галузеві програми як форми реалізації державної інформаційної політики в Україні.

ОСОБЛИВА ЧАСТИНА ІНФОРМАЦІЙНОГО ПРАВА

Тема 9. Права та обов'язки людини, громадянина щодо інформації

Особисті права людини, громадянина на збирання, зберігання, використання та поширення інформації.

Право людини, громадянина на доступ та отримання інформації.

Правові обмеження на доступ людини, громадянина до інформації.

Права та обов'язки людини, громадянина на обмеження поширення інформації.

Регулювання правовідносин щодо охорони та захисту персональних даних від несанкціонованих їх обробки та поширення.

Тема 10. Права суспільства щодо інформації

Роль суспільства у формуванні правових аспектів розвитку інформаційних ресурсів та єдиного інформаційного простору країни.

Проблеми визначення інформаційних прав суспільства.

Співвідношення інформаційних прав суспільства з нормами суспільної моралі.

Правове регулювання суспільних відносин щодо електронних документів, електронного документообігу та електронного підпису.

Правове регулювання інформаційних відносин щодо електронної економіки, електронної торгівлі, електронного банкінгу та ін.

Дотримання у суспільстві права власності на інформацію, інформаційні ресурси.

Інформаційні права суспільства як засіб здійснення контролю за діяльністю органів державної влади та дотриманням суспільної моралі.

Тема 11. Права та обов'язки держави у сфері інформаційної діяльності

Роль держави в удосконаленні правової основи інформаційного простору.

Гарантії держави у сфері права щодо інформації.

Охоронна та захисна функції держави щодо інформаційних ресурсів єдиного інформаційного простору України.

Обов'язок органів держави публікувати інформацію, яка має важливе суспільне значення.

Організація та координація дій органів державної влади в єдиному інформаційному просторі України.

Правове регулювання надання органами державної влади та органами місцевого самоврядування юридичним та фізичним особам інформаційних послуг із застосуванням Інтернету, запровадження електронного документообігу та електронного цифрового підпису, дистанційного навчання, телемедицини, електронних платіжних систем, електронного бізнесу, електронних бірж, аукціонів і депозитаріїв.

Тема 12. Співробітництво України з іншими державами, зарубіжними і міжнародними організаціями в галузі інформації

Основні засади правовідносин у міжнародній інформаційній діяльності. Поняття та сутність міжнародного інформаційного права.

Форми та види співробітництва України з іншими державами, зарубіжними і міжнародними організаціями в галузі інформації.

Міжнародне публічне право у сфері інформаційної діяльності та його роль у розвитку глобального інформаційного простору. Конвенційні засади міжнародного інформаційного права.

Міжнародні договори, їх роль у регулюванні транскордонної інформаційної діяльності.

Порівняльний аналіз правового регулювання суспільних інформаційних відносин у різних країнах.

Експорт та імпорт інформаційної продукції (послуг).

Проблеми міжнародного співробітництва в правовому регулюванні та розвитку глобального інформаційного простору.

Наукові підходи щодо формування міжнародного інформаційного права.

СПЕЦІАЛЬНА ЧАСТИНА ІНФОРМАЦІЙНОГО ПРАВА

Тема 13. Правове регулювання суспільних відносин у сфері засобів масової інформації

Законодавство України щодо регулювання суспільних відносин у сфері застосування засобів інформації.

Медіаправо. Інформаційні агентства та інші засоби масової інформації (преса, радіо, телебачення) як складові правовідносин.

Правовідносини у сфері архівної, бібліотечної та музейної діяльності.

Видавнича діяльність та її зв'язок з авторським правом.

Реклама, піар, недобросовісна конкуренція, інформаційна боротьба як об'єкти інформаційної діяльності.

Правове регулювання у сфері електронної телекомунікації (зв'язку).

Правове регулювання у сфері поштового зв'язку.

Інформатизація як особливий об'єкт правовідносин в інформаційній діяльності.

Правовідносини у сфері наукової інформації, наукової та науково-технічної діяльності.

Правове регулювання у сфері застосування сучасних інформаційних технологій навчання, освіти, просвітництва, культури.

Кінематографія як засіб масової інформації.

Проблеми визначення Інтернету як інтегрованого засобу масової інформації.

Тема 14. Правові аспекти культури інформаційної діяльності

Історія (онтологія) розвитку культури технологій об'єктивного вираження спілкування між людьми.

Інформаційна культура як об'єкт правовідносин та як об'єкт вивчення.

Роль інформації в культурі соціальних відносин на різних історичних етапах розвитку суспільства.

Інформаційна цивілізація: позитивні та негативні боки.

Поняття, сутність та співвідношення категорій "Інформаційне суспільство", "кібер-цивілізація", "комп'ютеризація" та "інформатизація".

Взаємозв'язок інформаційної та правової культури.

Вплив суспільної інформаційної культури на економіку країни та державне управління.

Тема 15. Правове регулювання безпеки інформаційної діяльності

Поняття та сутність категорій "безпека інформаційної діяльності" та "інформаційна безпека" в інформаційному праві. Інформаційна безпека як об'єкт правовідносин щодо інформаційної діяльності.

Національна інформаційна безпека як інститут інформаційного права.

Концептуальні підходи щодо визначення змісту інформаційної безпеки.

Складові національної інформаційної безпеки.

Співвідношення національної інформаційної безпеки з іншими напрямами (сферами) національної та міжнародної безпеки.

Взаємозв'язок національної інформаційної безпеки з інформаційним суверенітетом.

Специфіка інформаційної безпеки в умовах формування глобальної кіберцивілізації.

Тема 16. Правова охорона та захист інформації в комп'ютерних системах

Суспільні відносини щодо інформаційної діяльності із застосуванням комп'ютерних систем.

Охорона правовідносин із застосуванням комп'ютерних інформаційно-телекомунікаційних систем.

Особливості правової охорони комп'ютерної інформації: комп'ютерних програм, автоматизованих баз даних і знань.

Інтернет-правовідносини: проблеми правового регулювання щодо засобів, способів та методів охорони та захисту електронних даних.

Охорона та захист інформації в автоматизованих (комп'ютерних) системах як вид інформаційної діяльності.

Тема 17. Деліктні правовідносини в інформаційному праві. Відповідальність за правопорушення в інформаційній сфері.

Зв'язок методології інформаційного права з юридичною деліктологією.

Проблеми визначення та класифікації правопорушень та відповідальності в інформаційній сфері суспільних відносин.

Інформація як предмет дисциплінарних проступків.

Інформація як предмет адміністративних правопорушень.

Цивільно-правова охорона та захист суспільних відносин в сфері інформаційної діяльності.

Кримінально-правова охорона та захист суспільних відносин щодо інформації.

Основна рекомендована література

1. Михайлов А.И. Основы научной информации / А.И. Михайлов, А.И. Черный, Р.С. Гиляревский. – М.: "Наука", 1965. – 655 с.
2. Копылов В.А. Информационное право: учебник / В.А. Копылов. – М.: Юристъ, 2002. 512 с.
3. Рассолов М.М. Информационное право: учебное пособие / М.М. Рассолов. М.: Юристъ, 1999. 400 с.
4. Основи інформаційного права України: посіб. / [В.С. Цимбалюк, В.Д. Гавловський, В.М. Брижко та ін.]; за ред. М.Я. Швеця, Р.А. Калюжного та Н.В. Мельника. К.: Знання, 2004. 274 с.
5. Правова інформатика: підручник / [М. Швець, В. Брижко, В. Цимбалюк та ін.]; за ред. В. Дурдинця, С. Моісеєва та М. Швеця. [2-е вид., доп. та перероб.]. К.: ТОВ "ПанТот", 2007. 524 с.
6. е-майбутнє та інформаційне право / [В. Брижко, В. Цимбалюк, М. Швець, Ю. Базанов та ін.]; за ред. М. Швеця. – К.: НДЦПІ АПрН України. 2006.
7. е-боротьба в інформаційних війнах та інформаційне право: монографія / В.М. Брижко, М.Я. Швець, В.С. Цимбалюк. – К.: ТОВ "Пан Тот", 2007 р. 234 с.
8. Інформаційна культура: навч. посіб. / [В.С. Цимбалюк, Н.Б. Новицька, Р.А. Калюжний, М.Я. Швець та ін.]; за ред. М.Я. Швеця, Р.А. Калюжного. Ірпінь, НУДПСУ, 2007. 254 с.
9. Стан та перспективи розвитку інформаційної сфери України: збірник матеріалів з питань становлення інформаційного суспільства в Україні / [Рубан І.А., Семенченко А.І., Троян П.І., Макарова В.С., Задорожня Л.М., Брижко В.М.]; упоряд. та редагування Брижко В.М., Гладківської О.В., Швеця М.Я. К.: ТОВ "Пан Тот", 2009 р. 116 с. (Додаток до наукового журналу "Правова інформатика").
10. Журавський В.С. Україна на шляху до інформаційного суспільства / В.С. Журавський, М.К. Родіонов, І.Б. Жиляєв; за заг. ред. М.З. Згуровського. К.: ВНЦ "Видавництво "Політехніка", 2004. – 484 с.
11. Згуровський М.З. Розвиток інформаційного суспільства в Україні: правове регулювання у сфері інформаційних відносин / М.З. Згуровський. – К.: НТТУ "КПІ", 2006. 542 с.
12. Електронне інформаційне суспільство України: погляд у сьогодення і майбутнє: монографія / [В.М. Фурашев, Д.В. Ланде, О.М. Григор'єв, О.В. Фурашев]. – К.: Інжиніринг, 2005. – 164 с.
13. Комп'ютерна злочинність: навчальний посібник / [П.Д. Біленчук, Б.В. Романюк, В.С. Цимбалюк, В.Д. Павловський та ін.]. – К.: "Атіка", 2002. – 240с.
14. Голубєв В.О. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: навч. посібник / В.О. Голубєв, В.Д. Гавловський, В.С. Цимбалюк; за заг. ред. д.ю.н., проф. Р.А. Калюжного. – Запоріжжя: ГУ "ЗІДМУ", 2002. 292 с.
15. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток: науково-практичний посібник / [Бутузов В.М., Гавловський В.Д., Титуніна К.В., Шеломенцев В.П.]; за ред. І.В. Бондаренко. – К.: "Видавничий будинок "Ава-

пюст-Прим", 2009. – 182 с. с іл. – (Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при Раді Національної безпеки і оборони України).
16. Брижко В.М. Методологічні та правові засади упорядкування інформаційних відносин: монографія / В.М. Брижко. – К.: ТОВ "ПанТот", 2009 р. – 418 с.

Рекомендована література щодо євроінтеграції

1. В.М. Фурашев. Національна безпека України: шляхи забезпечення, роль і місце суспільства. Євроатлантичний курс: монографія / В.М. Фурашев, С.Ф. Джердж. К.: "Синопсис", 2009. – 176 с.
2. Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти упорядкування суспільних інформаційних відносин у зв'язку з автоматизованою обробкою даних у правоохоронній діяльності: посібник / [Брижко В., Швець М., Романюк Б., Цимбалюк В.]. – Кн. 2; за ред. М.Швеця та Б.Романюка. К.: ТОВ "ПанТот", 2006. – 509 с.

Додаткова рекомендована література

1. Расторгуев С. Информационная война / С. Расторгуев. М.: Радио и связь, 1999.
2. Кара-Мурза С. Манипуляция сознанием / С. Кара-Мурза. М., 2000.
3. Питер Л. Дж. Принцип Питера, или Почему дела идут вкривь и вкось / Л. Дж. Питер; [пер. с англ. А.В. Степанова]. М.: ООО "Издательство АСТ", 2002. 283 с.
4. Паркинсон С.Н. Законы Паркинсона / С.Н. Паркинсон; [пер. с англ.; сост. и авт. предисл. В.С. Муравьев]. М.: Прогресс, 1989. 448 с.
5. Бронитейн Я.Н. Оттоворковедение: Секретное оружие чиновника: Инструмент для производства убийственной негативной аргументации и манипулирования. Симферополь: ИД "Квадранал", 2005. 480 с. (Серия "Для Духовного пользования "интелектуальных меньшинств").

СКОРОЧЕНИЙ СЛОВНИК ТЕРМІНІВ*

База даних – іменована сукупність даних, що відображає стан об'єктів та їх відношень у визначеній предметній області *(ст. 1 Закону України "Про Національну програму інформатизації")*.

База знань – масив інформації у формі, придатній до логічної і смислової обробки відповідними програмними засобами *(ст. 1 Закону України "Про Національну програму інформатизації")*.

Бібліотека – це інформаційний, культурний, освітній заклад, що має упорядкований фонд документів і надає їх у тимчасове користування фізичним та юридичним особам *(ст.1 Закону України "Про бібліотеки і бібліотечну справу")*

Використання інформації – це задоволення інформаційних потреб громадян, юридичних осіб і держави *(ст. 14 Закону України "Про інформацію")*.

Власник інформації – фізична або юридична особа, якій належить право власності на інформацію *(ст. 1 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах")*

Власник системи – фізична або юридична особа, якій належить право власності на систему *(ст. 1 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах")*.

Дані – електронні сигнали, коди або структури щодо повідомлень на матеріальному носії, до яких інформація пристосована (прикріплена) (*у визначенні авторів Посібника*).

Діловодство – сукупність процесів, що забезпечують документування управлінської інформації і організацію роботи із службовими документами *(ст. 1 Закону України "Про Національний архівний фонд та архівні установи")*.

Документ, документована інформація – матеріальна форма одержання, зберігання, використання і поширення інформації, зафіксованої на папері, магнітній, кіно-, фотоплівці, оптичному диску або іншому носієві *(ст. 27 Закону України "Про інформацію", ст. 1 Закону України "Про обов'язковий примірник документів")*

Документ, обов'язковий примірник – примірник різних видів тиражованих документів, який передає його виробник на безоплатній або платній основі юридичним особам *(ст. 1 Закону України "Про обов'язковий примірник документів")*

Документ унікальний – документ Національного архівного фонду, що становить виняткову культурну цінність, має важливе значення для формування національної самосвідомості Українського народу і визначає його вклад у всесвітню культурну спадщину *(ст. 1 Закону України "Про Національний архівний фонд та архівні установи")*

Документи, які зберігаються в бібліотечних фондах – матеріальна форма одержання, зберігання, використання і поширення інформації, зафіксованої на папері, магнітній, кіно-, фотоплівці, оптичному диску або іншому носієві *(ст. 1 Закону України "Про бібліотеки і бібліотечну справу")*.

Електронний цифровий підпис – вид електронного підпису, отриманого 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 *(ст. 1 Закону України "Про електронно-цифровий підпис")*

Засекречування матеріальних носіїв інформації – 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 *(ст. 1 Закону України "Про державну таємницю")*

Засоби інформатизації – електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, інформаційні системи або їх окремі елементи, інформаційні мережі і мережі зв'язку, що використовуються для реалізації інформаційних технологій *(ст. 1 Закону України "Про Національну програму інформатизації")*.

Засоби масової інформації аудіовізуальні – радіомовлення, телебачення, кіно, звукозапис, відеозапис тощо *(ст. 20 Закону України "Про інформацію")*.

Засоби масової інформації друковані – періодичні друковані видання (преса) – газети, журнали, бюлетені тощо і разові видання з визначеним тиражем *(ст. 20 Закону України "Про інформацію")*.

Засоби масової інформації друковані (преса) в Україні – 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 *(ст. 1 Закону України "Про друковані засоби масової інформації (пресу) в Україні")*.

Зберігання інформації – це забезпечення належного стану інформації та її матеріальних носіїв *(ст. 14 Закону України "Про інформацію")*.

Індустрія інформації – виробництво інформації, інформаційних ресурсів, продуктів і технологій.

Інформатизація – сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, які спрямовані на створення умов для задоволення потреб громадян та суспільства на основі розвитку і використання інформаційних систем, мереж, ресурсів та інформаційно-комунікаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки *(ст. 1 Закону України "Про Національну програму інформатизації")*

Інформаційна безпека – стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави

Інформаційна діяльність – сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави *(ст. 12 Закону України "Про інформацію")*

Інформаційна інфраструктура – організована сукупність компонентів, яка забезпечує інформаційні процеси щодо інформаційних продуктів (ресурсів, технологій) та послуг

Інформаційна послуга – дії суб'єктів щодо забезпечення споживачів інформаційними продуктами *(ст. 1 Закону України "Про Національну програму інформатизації")*

Інформаційний продукт (продукція) – документована інформація, яка підготовлена і призначена для задоволення потреб користувачів *(ст. 1 Закону України "Про Національну програму інформатизації")*.

Інформаційна продукція – матеріалізований результат інформаційної діяльності, призначений для задоволення інформаційних потреб громадян, державних органів, підприємств, установ і організацій *(ст. 40 Закону України "Про інформацію")*.

Інформаційна послуга – здійснення у визначений законом формі інформаційної діяльності по доведенню інформаційної продукції до споживачів з метою задоволення їх інформаційних потреб (ст. 41 Закону України "Про інформацію").

Інформаційна послуга – дії суб'єктів щодо забезпечення споживачів інформаційними продуктами *(ст. 1 Закону України "Про Національну програму інформатизації")*.

Інформаційний ресурс – сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо) *(ст. 1 Закону України "Про Національну програму інформатизації")*.

Інформаційні ресурси – організована сукупність інформаційних продуктів, інформаційно-комп'ютерних технологій певного призначення, які необхідні для забезпечення інформаційних потреб громадян, суспільства і держави у визначеній сфері життя чи діяльності.

* Більш повний словник див.: *"Інформаційне суспільство. Дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція"* / В.М. Брижко, В.С. Цимбалюк та ін.; за ред. д.ю.н., професора Р. А. Калюжного, д.е.н., професора М. Я. Швеця. – К. : "Інтеграл", 2002 р. – 220 с.

Інформаційна система – це система обробки даних у будь-якій предметній сфері із засобами накопичення, зберігання, оновлення, пошуку і видачі даних.

Інформаційна технологія – цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування *(ст 1 Закону України "Про Національну програму інформатизації")*.

Інформаційне суспільство – суспільство, в якому процес комп'ютеризації дає людям доступ до надійних джерел інформації, позбавляє їх рутинної роботи, забезпечує високий рівень автоматизації виробництва.

Інформаційне право - комплексна система суспільних уявлень про духовні цінності та справедливий життєвий устрій, які історично сформовані світовою цивілізацією, та сформульовані на їх основі соціальні принципи взаємостосунків і правових відносин суб'єктів в інформаційній сфері, що виникають у процесі створення, збирання, збереження, використання і поширення інформації та інформаційних ресурсів (продуктів), які охороняються та захищаються державою (*у визначенні авторів Посібника*).

Інформаційні відносини – відносини, які виникають у всіх сферах життя і діяльності суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації *(ст. 3 Закону України "Про інформацію")*.

Інформаційний ресурс – сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо) *(ст. 1 Закону України "Про Національну програму інформатизації")*.

Інформаційний ресурс науково-технічної інформації – систематизоване зібрання науково-технічної літератури і документації, зафіксоване на паперових чи інших носіях *(ст. 1 Закону України "Про науково-технічну інформацію")*

Інформаційний ресурс спільного користування – сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових та науково-технічних бібліотек, центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання *(ст. 1 Закону України "Про науково-технічну інформацію")*

Інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле *(ст. 1 Закон України "Про захист інформації в інформаційно-телекомунікаційних системах")*.

Інформація – це документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі *(ст. 1 Закону України "Про інформацію")*

Інформація – повідомлення про будь-які відомості чи сукупність відомостей щодо фактів або особистих уявлень (*у визначенні авторів Посібника*).

Інформація документована – матеріальна форма одержання, зберігання, використання і поширення інформації, зафіксованої на папері, магнітній, кіно-, фотоплівці, оптичному диску або іншому носієві *(ст. 27 Закону України "Про інформацію", ст. 1 Закону України "Про обов'язковий примірник документів")*.

Інформація нова (знання) – документовані або публічно оголошені відомості про події та явища, щодо особи, суспільства, держави та навколишнього природного середовища, зміст яких має інтелектуальне самовираження і не може бути наперед відомий чи передбачений їх одержувачем (*у визначенні авторів Посібника*).

Інформація конфіденційна – відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов *(ст. 30 Закону України "Про інформацію")*.

Інформація масова (щодо засобів масової інформації) – документовані або публічно оголошені відомості про події та явища, що видобуваються у суспільстві, державі та навколишньому природному середовищі (*у визначенні авторів Посібника*).

Інформація правова – сукупність документованих або публічно проголошених відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо *(ст. 22 Закону "Про інформацію")*.

Користувач інформації в системі – фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі *(ст. 1 Закону України " Про захист інформації в інформаційно-телекомунікаційних системах")*.

Матеріальні носії секретної інформації – матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо *(ст. 1 закону України "Про державну таємницю")*.

Одержання інформації – це набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою *(ст. 14 Закону України "Про інформацію")*

Поширення інформації – це розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошуваної інформації *(ст. 14 Закону України "Про інформацію")*.

Право на інформацію – можливість громадян України, юридичних осіб і державних органів на вільне одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій *(ст 9 Закону України "Про інформацію")*.

Режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації *(ст 28 Закону України "Про інформацію")*.

Технічний захист інформації – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації *(ст. 1 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах")*.

СПИСОК ЛІТЕРАТУРИ

Нормативно-правові акти

1. Конституція України : Закон України від 28.06.1996 р. – К. : Інформаційно-видавниче агентство "ІВА", 1996. – 52 с.

2. Цивільний кодекс України : Кодекс України від 16.01.2003 р. № 435-IV : за станом на 10.10.2005 р. – К. : Велес, 2005. – 352 с.

3. Господарський кодекс України : Кодекс України від 16 січня 2003 р. № 436-IV : за станом на 15.09.2004 р. – К. : Велес, 2004. – 164 с.

4. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. – Режим доступу : www.rada.gov.ua

5. Про підприємства в Україні : Закон України від 27.03.1991 р. № 887-XII. – Режим доступу : www.rada.gov.ua

6. Про захист від недобросовісної конкуренції : Закон України від 07.06.1996 р. № 236/96-ВР. – Режим доступу : www.rada.gov.ua

7. Про оподаткування прибутку підприємств : Закон України від 28.12.1994 р. № 334/94-ВР. – Режим доступу : www.rada.gov.ua

8. Про Національний банк України : Закон України від 20.05.1999 р. № 679-XIV. – Режим доступу : www.rada.gov.ua

9. Про банки та банківську діяльність : Закон України від 07.12.2000 р. № 2121-III. – Режим доступу : www.rada.gov.ua

10. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 р. № 2135-XII. – Режим доступу : www.rada.gov.ua

11. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII. – Режим доступу : www.rada.gov.ua

12. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII. – Режим доступу : www.rada.gov.ua

13. Про Національний архівний фонд і архівні установи : Закон України від 24.12.1993 р. № 3814-XII. – Режим доступу : www.rada.gov.ua

14. Про друковані засоби масової інформації (пресу) в Україні : Закон України від 16.11.1992 р. № 2782-XII. – Режим доступу : www.rada.gov.ua

15. Про бібліотеки і бібліотечну справу : Закон України від 27.01.1995, N 32/95-ВР. – Режим доступу : www.rada.gov.ua

16. Про інформаційні агентства : Закон України від 28.02.1995 р. № 74/95-ВР. – Режим доступу : www.rada.gov.ua

17. Про приєднання України до Статуту Ради Європи : Закон України від 31.10.1995 р. № 398/95-ВР. – Режим доступу : www.rada.gov.ua

18. Про рекламу : Закон України від 03.07.1996 р. № 270/96-ВР. – Режим доступу : www.rada.gov.ua

19. Про видавничу справу : Закон України від 05.06.1997 р. № 318/97-ВР. – Режим доступу : www.rada.gov.ua

20. Про кінематографію : Закон України від 13.01.1998 р. № 9/98-ВР. – Режим доступу : www.rada.gov.ua

21. Про власність : Закон України від 07.02.1991 р. № 697-12. – Режим доступу : www.rada.gov.ua

22. Про освіту : Закон УРСР від 23.05.1991 р. № 1060-XII. – Режим доступу : www.rada.gov.ua

23. Про наукову і науково-технічну діяльність : Закон України від 13.12.1991 р. № 1977-XII. – Режим доступу : www.rada.gov.ua

24. Про авторське право та суміжні права : Закон України від 23.12.1993 р. № 3792-XII. – Режим доступу : www.rada.gov.ua

25. Про науково-технічну інформацію : Закон України від 25.06.1993 р. № 3322-XII. – Режим доступу : www.rada.gov.ua

26. Про телебачення і радіомовлення : Закон України від 21.12.1993 р. № 3759-XII. – Режим доступу : www.rada.gov.ua

27. Про наукову і науково-технічну експертизу : Закон України від 10.02.1995, № 51/95-ВР. – Режим доступу : www.rada.gov.ua

28. Про зв'язок : Закон України від 16.05.1995 р. № 160/95-ВР. – Режим доступу : www.rada.gov.ua

29. Про Концепцію Національної програми інформатизації : Закон України від 04.02.1998 р. № 75/98-ВР. – Режим доступу : www.rada.gov.ua

30. Про Національну програму інформатизації : Закон України від 04.02.1998 р. № 74/98-ВР. – Режим доступу : www.rada.gov.ua

31. Про приєднання України до Статуту Ради Європи : Закон України від 31.10.1995 р. № 398/95-ВР. – Режим доступу : www.rada.gov.ua

32. Про громадянство України : Закон України від 18.01.2001 р. – Режим доступу : www.rada.gov.ua

33. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV. – Режим доступу : www.rada.gov.ua

34. Про електронний цифровий підпис : Закон України від 22.05.2003 р. № 852-IV. – Режим доступу : www.rada.gov.ua

35. Про телекомунікації : Закон України від 18.09.2003 р. № 1280-IV. – Режим доступу : www.rada.gov.ua

36. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 31.05.2005 р. № 2594-IV. – Режим доступу : www.rada.gov.ua

37. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.2007 р. № 537-V. – Режим доступу : www.rada.gov.ua

38. Про заходи державної політики України в області прав людини : Постанова Верховної Ради України від 17.06.1999 р. № 757-XIV. – Режим доступу : www.rada.gov.ua

39. Про підсумки парламентських слухань "Суспільство, засоби масової інформації, влада: свобода слова і цензура в Україні" : Постанова Верховної Ради України від 16.01.2003 р. № 441-IV // Правова інформатика. – 2004. – № 2. – С. 86-87.

40. Про рішення Ради національної безпеки і оборони України від 17 червня 1997 року "Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин" : Указ Президента України від 21.07.1997 р. № 663/97. – Режим доступу : www.rada.gov.ua

41. Про забезпечення виконання Угоди про партнерство та співробітництво між Україною та Європейськими Співтовариствами (Європейським Союзом) і вдосконалення механізму співробітництва з Європейськими співтовариствами (Європейським Союзом) : Указ Президента України від 24.02.1998 № 148/98. – Режим доступу : www.rada.gov.ua

42. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 р. № 1229/99. – Режим доступу : www.rada.gov.ua

43. Програма інтеграції України до Європейського Союзу : Указ Президента України від 14.09.2000 р. № 1072/2000. – Режим доступу : www.rada.gov.ua

44. Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України" : Указ Президента України від 06.12.2001 р. № 1193/2001. – Режим доступу : www.rada.gov.ua

45. Про Стратегію національної безпеки України : Указ Президента України від 12.02.2007 р. № 105/2007. – Режим доступу : www.rada.gov.ua

46. Про заходи щодо створення електронної інформаційної системи "Електронний Уряд" : Постанова Кабінету Міністрів України від 24.02.2003 р. № 208. – Режим доступу : www.rada.gov.ua

47. Про затвердження Державної програми інформатизації та комп'ютеризації професійно-технічних навчальних закладів на 2004-2007 роки : Постанова Кабінету Міністрів України від 20.08.2003 р. № 1300. – Режим доступу : www.rada.gov.ua

48. Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади : Постанова Кабінету Міністрів України від 10.09.2003 р. № 1433. – Режим доступу : www.rada.gov.ua

49. Про затвердження Програми розвитку системи дистанційного навчання на 2004-2006 роки : Постанова Кабінету Міністрів України від 23.09.2003 р. № 1494. – Режим доступу : www.rada.gov.ua

50. Про затвердження Положення про Національний реєстр електронних інформаційних ресурсів : Постанова Кабінету Міністрів України від 17.03.2004 р. № 326. – Режим доступу : www.rada.gov.ua

51. Про затвердження Порядку обов'язкової передачі документованої інформації : Постанова Кабінету Міністрів України від 28.10.2004 р. № 1454. – Режим доступу : www.rada.gov.ua

52. Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади : Постанова Кабінету Міністрів України від 28.10.2004 р. № 1453. – Режим доступу : www.rada.gov.ua

53. 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 28.10.2004 р. № 1452. – Режим доступу : www.rada.gov.ua

54. Концепція реформування законодавства України у сфері інформаційних відносин : Затверджено рішенням Урядової комісії з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади : [протокол Урядової комісії від 06.10.2000 р. № 7, м. Київ] : [зареєстровано авторське право на твір у Держдепартаменті інтелектуальної власності МОН України, № 25472 від 05.06.2008 р.)] // Правова інформатика. – 2007. – № 4(16). – С. 80-87. (Відповідно до Закону України "Про авторське право та суміжні права" від 23.12.1993 р. № 3792-XII робота засвідчена Свідоцтвом про реєстрацію авторського права на твір № 25784 від 24.09.2008 р. (заявка від 06.06.2008 р. № 25472). Автори: Швець М., Калюжний Р., Брижко В., Павловський В., Цимбалюк В.)

55. Конвенція Ради Європи "Про захист прав людини і основоположних свобод" (Рим, 04.XI.1950 р.) та Протокол № 11 // Голос України. – 2001. – № 3 (2503). – С. 6-8.

56. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних. – Переклад : Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Amendment to Convention ETS No.108 allowing the European Communities to accede) : Конвенція Ради Європи від 28.01.1981 р. № 108, Страсбург. – Режим доступу : www.convention.coe.int/tre aty/en/Treaties/Html/108.htm. – (Офіційний переклад засвідчено МЗС України від 01.07.2002 р.).

57. Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних : Директива Європейського парламенту та Ради Європейського Союзу від 24.10.1995 р. № 95/46/СС. - Режим доступу : www.evtopa. eu.int/ISPO/legal/en/ dataprot /directiv/directiv.html

58. Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі : Директива Європейського парламенту та Ради Європейського Союзу від 15.12.1997 р. № 97/66/СС. - Режим доступу : www.evropa.eu. int/ISPO/legal/en/datap rot/protec tion.html

59. Про правові аспекти інформаційних послуг щодо електронної комерції на внутрішньому ринку : Директива Європейського Парламенту і Ради від 08.06.2000 р. № 2000/31/СС // Правова інформатика. – 2005. – № 2(6). – С. 72-89.

60. Об информации, информатизации и защите информации : Федеральний Закон Российской Федерации от 20.02.1995 г. № 24-ФЗ. – Режим доступу : www.duma.gov.ru

Наукова та науково-практична література

61. Городова О. Информационное право : учебник / О. Городова. – М. : "Проспект", 2008. – 239 с.

62. Ковалева Н. Информационное право России : учебное пособие / Н. Ковалева. – М. : "Дашков и К°", 2008. – 357 с.

63. Бобир В. І. Правознавство : навчальний посібник / В. І. Бобир, С. Е. Демський та ін.; За ред. В. В. Копейчикова. – К. : Юрінком Інтер, 1998.

64. Юридична енциклопедія : В 6 т. / [редкол. : Ю. С. Шемшученко (голова редкол.) та ін.]. – К. : Укр. енцикл., 2003. – Т. 5 : П-С. – 736 с.

65. Рабинович П. М. Основи загальної теорії права та держави / П. М. Рабинович. – К., 1994; Алексеев С. С. Теория права / С. С. Алексеев. – М., 1995; Теория государства и права. – М., 1995; Котюк В. О. Теорія права / В. О. Котюк. – К., 1996; Загальна теорія держави і права. – К., 1997.

66. Веллер Михаил. Понимать / Михаил Веллер. – С-Пб., 2006. – 384 с.

67. Белл Д. Социальные рамки информационного общества / Д. Белл. – М., 1998.

68. Баранов А. А. Права человека и защита персональных данных / А. А. Баранов, В. М. Брижко, Ю. К. Базанов. – Харьков : Фолио, 2000. – 280 с.

69. Ашпілогов О. В. Захист прав та свобод громадянина прокурором в адміністративному судочинстві : монографія / О. В. Ашпілогов. – К. : Видавничий Дім "Ін Юре", 2008. – 168 с.

70. Бачинін В. А. Філософія права : підручник / В. А. Бачинін, В. С. Журавський, М. І. Панов. – К. : Концерн "Видавничий Дім "Ін Юре", 2003. – 472 с.

71. Добрянський С. Права людини як специфічна форма буття (існування) моралі / С. Добрянський : матеріали X регіон. наук.-практ. конф. ["Проблеми державотворення і захисту прав людини в Україні"], (Львів, 5 – 6 лютого 2004 р.). – Львів : Юрид. ф-т ЛНУ, 2004. – С. 530.

72. Пальцева Л. А. Суд у Гомера и Гесиода / Л. А. Пальцева ; под ред. проф. З. Д. Фролова. – СПб. : Изд-во Санкт-Петерб. гос. ун-та, 2002. – С. 428. – (Исследования и публикации по истории античного мира).

73. Васильева Т. В. Афинская школа философии. Философский язык Платона и Аристотеля / Т. В. Васильева. – М. : Наука, 1985. – 160 с. – (Серия "Из истории мировой культуры").

74. Платон : сочинение в 3 томах ; под общ. ред. А. Ф. Лосева и В. С. Асмуса; [пер. с древнегреч.]. – М. : "Мысль", 1968. – Т. 1. – 624 с.

75. Мусский И. А. 100 великих мыслителей / И. А. Мусский. – М. : Вече, 2000. – 688 с.

76. Баландин Н. К. 100 великих гениев / Н. К. Баландин. – М. : Вече, 2000. – 480 с.

77. Аврелий Марк. Наедине с собой. Размышления / Марк Аврелий ; [пер. с древнегреч.] ; под общ. ред. А. В. Добровольского. – Киев-Черкасы : Collegium Artium Ing. Ltd; РИЦ "Реал", 1993. – 148 с.

78. Джонс А. Х. М. Правосудие поздней Римской империи. Гибель античного мира / А. Х. М. Джонс ; [пер. с англ. Т. Горяйновой]. – Ростов-на-Дону : Изд-во "Феникс", 1997. – 576 с.

79. Бельсон Я. М. История государства и права США / Я. М. Бельсон, К. Е. Ливанцев. – Л. : Лениздат, 1982. – С. 168.

80. Баранов А. А. Защита персональных данных / А. А. Баранов, В. М. Брижко, Ю. К. Базанов. – К. : Национальное агентство по вопросам информатизации при Президенте Украины, 1998. – 128 с.

81. Брижко В. Системна інформатизація правоохоронної діяльності : європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв'язку з автоматизованою обробкою даних у правоохоронній діяльності : посібник. – Книга 2 / В. Брижко, Б. Романюк, В. Цимбалюк, М. Швець ; за ред. члена-кореспондента АПрН України М. Швеця та к.ю.н. Б. Романюка. – К. : ТОВ "НаІТот", 2006 р. – 509 с.

82. Конквест Роберт. Большой террор : в 2-х кн. / Роберт Конквест ; [пер. с англ. Л. Владимирова]. – Рига : "Ракстниекс", 1991. – кн. 1. – 414 с. – кн. 2. – 429 с.

83. Брижко В. е-майбутнє та інформаційне право / В. Брижко, В. Цимбалюк, М. Швець, М. Коваль, Ю. Базанов ; за ред. доктора економічних наук, професора, члена-кореспондента АПр Н України М. Швеця. – [2-е вид., доп.]. – К. : ТОВ "Пан Тот", 2006. – 234 с.

84. Макаренко С. А. Європейська інформаційна політика : монографія / С. А. Макаренко. – К. : Наша культура і наука, 2000. – 368 с.

85. Хайек Ф. А. Дорога к рабству / Ф. А. Хайек ; [пер. с англ. и предисловие И. Я. Петраковой]. – М. : "Экономика", 1992. – 176 с.

86. Каутский К. Происхождение христианства / К. Каутский [пер. с нем.]. – М. : Политиздат, 1990. – 463 с.

87. Корнєєва Т. Права людини в інформаційному суспільстві. Комунікаційні права : четверте покоління прав людини : тлумачний словник української мови / Т. Корнєєва ; за ред. проф. В. С. Калачника. – Х. : Прапор, 2002. – 992 с.

88. Червякова О. Б. Актуальні питання застосування законодавства про адміністративне судочинство / О. Б. Червякова ; матеріали міжнар. наук.-практ. конф. ["Захист права на інформацію в порядку адміністративного судочинства"], (Київ, 25 – 26 січня 2007). – К. : Нац. юрид. акад. України, 2007. – 300 с.

89. Мусский И. А. 100 великих дипломатов / И. А. Мусский. – Вече, 2001. – 608 с. ; Комиссаренко С. Шарль-Морис Талейран: "Язык дан нам для того, чтобы скрывать свои мысли!" // "Дипломатический мир", 2007. – (Киев, изд. ТОВ "Мега-полиграф")

90. Теоретико-правовая оценка развития сферы информационно-электронных технологий // Право и политика. – 2001. – № 2.

91. Конюхов В. А. Информационное право : учебное пособие / В. А. Конюхов. – М. : Юристъ, 1997. – 472 с.

92. Конюхов В. А. Информационное право : учебник / В. А. Конюхов. – М. : Юристъ, 2002. – 512 с.

93. Рассолов М. М. Правова інформатика и управление в сфере предпринимательства / М. М. Рассолов, В. Д. Эльянов, И. М. Рассолов. – М. : Юристъ, 1996.

94. Рассолов М. М. Информационное право : учебное пособие / М. М. Рассолов. – М. : Юристъ, 1999. – 400 с.

95. Питання вдосконалення законодавства України у сфері інформації та інформатизації / авт. кол.: Л. М. Задорожня, М. І. Коваль, В. М. Брижко ; за ред. члена-кореспондента АПрН України М. Я. Швеця. – К., 2005. – 31 с. – (Додаток до журналу "Правова інформатика")

96. Фромм Э. Бегство от свободы / Э. Фромм. – М., 1989.

97. Грачев Г. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г. Грачев. – М. : Изд-во РАГС, 1998. – 125 с.

98. Шостром Э. Анти-Карнеги, или Человек-манипулятор / Э. Шостром. – Минск, 1992.

99. Ермаков Ю. А. Манипуляция личностью: смысл, приемы, последствия / Ю. А. Ермаков. – Екатеринбург, 1995.

100. Гальперин Я. Г. Технология психологической самозащиты. Стресс-дистресс – проблема XX века / Я. Г. Гальперин, О. И. Жданов. – Горький, 1997.

101. Кара-Мурза С. Манипуляция сознанием / С. Кара-Мурза. – М., 2000. – Режим доступу : www.duma.gov.ru www.lib.ru POLITOLOG kara-mur za.txt

102. Паркинсон С. Н. Законы Паркинсона / С. Н. Паркинсон ; [пер. с англ. ; сост. и авт. предисл. В. С. Муравьев]. – М. : Прогресс, 1989. – 448 с.

103. Грачев Г. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г. Грачев. – М. : Изд-во РАГС, 1998. – 125 с.

104. Грачев Г. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия / Г. Грачев, И. Мельник. – Режим доступу : www.gumer.info bibliotek_Buks.Psihol Grach intro.php

105. Почепцов Г. Информационные войны / Г. Почепцов. – К. : "Ваклер", 2000. – 574 с.

106. Расторгуев С. Информационная война / С. Расторгуев. – М. : Радио и связь, 1999. – (Рекомендовано к печати Комитетом по безопасности Государственной думы Российской Федерации и секции "Военно-технические проблемы" Российской инженерной академии). – Режим доступу : www.pobeda.ru content_view 185.142

107. Макиавелли Н. Государь / Н. Макиавелли. – М., 1990.

108. Словарь иностранных слов. – М., 1980.

109. Черных Л. Я. Историко-этимологический словарь / Л. Я. Черных. – М., 1994. Т. 1.

110. Великий тлумачний словник сучасної української мови : уклад. і голов. ред. В. Т. Бусел. – К. ; Ірпінь : ВТФ "Перун", 2002. – 1440 с.

111. Словарь русского языка. – М., 1981. – Т. 1.

112. Лекарев С. В. Бизнес и безопасность. Толковый терминологический словарь / С. В. Лекарев, В. А. Порк. – М., 1995.

113. Мясников В. Імперія Цин і російська держава XVII в. / В. Мясников. – М., 1980.

114. Политология : энциклопедический словарь ; ред. и сост. Ю. И. Аверьянов. – М., 1993.

115. Сахнова Т. В. Зачем суду психолог? / Т. В. Сахнова. – М. : "Знание", 1990.

116. Пинзова З. Н. "Два тела" Президента : Модели репрезентации власти на пороге третьего тысячелетия // Полис. – 1999. – № 2.

117. Зеньковский В. Психология детства / В. Зеньковский. – М. : Academia, 1996. – С. 215.

118. Дюпра Ж. Ложь / Ж. Дюпра ; [пер. с франц.]. – Саратов, 1905.

119. Шопенгауэр А. Полн. собр. соч. / А. Шопенгауэр. – Изд. Д. И. Ефимова. – М. : Типография Вильде, 1910. – Т. 4.

120. Поварнин С. Спор. О теории и практике спора / С. Поварнин. – Петроград : Изд. О. Богдановой, 1918.

121. Знаков В. В. Психология понимания правды / В. В. Знаков. – СПб., 1999.

122. Питер Л. Дж. Принцип Питера, или Почему дела идут вкривь и вкось / Л. Дж. Питер. [пер. с англ. А. В. Степанова]. – М. : ООО "Издательство АСТ", 2002. – 283 с.

123. Методология теории государства и права. – Режим доступу : www.lintcona.ru/yurfakt.html

124. Цветков А. Управление социально-политическими процессами: технология избирательных кампаний, лоббирования, общественной деятельности / А. Цветков. – М., 1996.

125. Низ А. Язык жестов / А. Низ ; [пер. с анг.]. – Воронеж : НПО "Модэк", 1992.

126. Закатов А. Ложь и борьба с нею / А. Закатов. – Волгоград : Нижне-Волжское книжное издательство, 1982.

127. Желев Ж. Фашизм / Ж. Желев. – М., 1991.

128. Амелин В. Социология политики / В. Амелин. – М., 1992.

129. Блуммер Р. Колективное поведение / Р. Блуммер. – Самара, 1998.

130. Московичи С. Век толпы / С. Московичи. – М., 1996.

131. Котлер Ф. Основы маркетинга / Ф. Котлер. – М., 1990.

132. Морозова Е. Г. Политический рынок и политический маркетинг : концепции, модели, технологии / Е. Г. Морозова. – М., 1999.

133. Блек С. Паблик Рилейшнз : что это такое? / С. Блек. – М., 1990.

134. Зверинцев А. Коммуникационный менеджмент / А. Зверинцев. – СПб., 1997.

135. Психологические операции и противодействие им. – М., 1993.

136. Бэндлер Р. Используйте свой мозг для изменения / Р. Бэндлер. – СПб., 1994.

137. Секреты психологической войны (цели, задачи, методы, формы, опыт). – Минск, 1999.

138. Зазыкин В. Г. Психологические основы проницательности : учебно-методическое пособие / В. Г. Зазыкин. – Кострома, 1994.

139. Інформаційне суспільство. Дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція / [В. М. Брижко, В. С. Цимбалюк, А. М. Чорнобров та ін.] ; за ред. доктора юридичних наук, професора Р. А. Калюжного, доктора економічних наук, професора М. Я. Швеця. – К. : "Інтеграл", 2002 р. – 220 с.

140. Ожегов С. И. Словарь русского языка: 70000 слов / С. И. Ожегов, под ред. Н. Ю. Шведовой. – [21-е изд., перераб. и доп.]. – М. : "Русский язык", 1989. – 924 с.

141. Баранов О. А. Понятійний апарат інформаційного права // Правова інформатика. – № 3(15)/2007. – С. 33-39.

142. Теорія держави і права : підручник / [за ред. С. Л. Лисенкової] – К. : Юрінком Інтер, 2005. – 448 с.

143. Юридична енциклопедія : в 6 т. / [редкол. Ю. С. Шемшученко (голова редкол.) та ін.] – К. : Укр. енцикл., 1998. – Т. 1: А–Г. – 672 с.

144. Юридична енциклопедія: в 6 т. / [редкол. Ю. С. Шемшученко (голова редкол.) та ін.] – К. : Укр. енцикл., 1998. – Т. 2: Д–Й. – 744 с.

145. Юридична енциклопедія: в 6 т. / [редкол. Ю. С. Шемшученко (голова редкол.) та ін.] – К. : Укр. енцикл., 1998. – Т. 4: П–Я. – 720 с.

146. Декарт Р. Рассуждения о методе : избранные произведения / Р. Декарт. – М., 1950.

147. Тодыка Ю. Н. Конституционно-правовой статус человека и гражданина в Украине / Ю. Н. Тодыка. – К. : Концерн "Видавничий Дім "In Юре", – 2004. – 368 с.

148. Кориссва Т. Права людини в інформаційному суспільстві. Комунікаційні права: четверте покоління прав людини : тлумачний словник української мови / Т. Кориссва ; за ред. проф. В. С. Калачника. – Х. : Прапор, 2002. – 992 с.

149. Черданцев А. Ф. Теория государства и права : учебник для вузов / А. Ф. Черданцев. – М. : Юрайт, 2000. – 422 с.

150. О. А. Гаврилов. Курс правовой информатики : учебник для вузов / О. А. Гаврилов. – М. : Издательство "НОРМА", 2000. – 432 с.

151. Програмування. Терміни та визначення (ISO/IES 2382-7:1989): ДСТУ 2873-94. – К. : Держспоживстандарт України, 1994.

152. Бази даних. Терміни та визначення (ISO/IES 2382-17:1996): ДСТУ 2874-94. – К. : Держспоживстандарт України, 1994.

153. Основні поняття. Терміни та визначення (ISO/IES 2382-13:1996): ДСТУ 2938-94. – К. : Держспоживстандарт України, 1994.

154. Швець М. Я., Брижко В. М. До питання огляду інформаційного законодавства щодо захисту персональних даних в країнах Європи // Правова інформатика. – 2004. – № 3. – С. 23-32.

155. Михайлов А. И. Основы научной информации / А. И. Михайлов, А. И. Черный, Р. С. Гиляревский. – М. : "Наука", 1965. – 655 с.

156. Шеннон К. Работы по статистической теории связи / К. Шеннон. – М., 1960.

157. Винер Н. Кибернетика и общество / Н. Винер. – М., 1958.

158. Кочових І. Головний Закон Всесвіту / І. Кочових. – Вінниця: "Антекс", 2001. – 48 с.

159. Глушков В. М. О кибернетике как науке / В. М. Глушков. – М., 1964.

160. Манеев А. К. Философский анализ антиномий науки / А. К. Манеев. – Минск, 1972.

161. Юзвишин И. И. Информациология или закономерности информационных процессов и технологий в микро- и макромирах Вселенной / И. И. Юзвишин. – [4-е изд.]. – М., 1996. – С. 15.

162. Бобир В. І. Правознавство: навчальний посібник / [В. І. Бобир, С. Е. Демський та ін.], за ред. В. В. Копєйчикова. – К. : Юрінком Інтер, 1998.

163. Моль А. Теория информации и эстетическое восприятие / А. Моль. – М. : 1996. – 154 с.

164. Юзова Д., Цимбалюк В. До питання вдосконалення механізмів забезпечення принципу верховенства права в Україні // Правова інформатика. – 2006. – № 4(12). – С. 38-41.

165. Шевчук С. Формальна та органічна характеристика принципу верховенства права до методів тлумачення Конституції / С. Шевчук // Українське право. – 1998. – Спецвипуск.

166. Вейцман Е. М. Великий английский материалист Томас Гоббс / Е. М. Вейцман. – М. : Знание, 1960.

167. Михайленко Ю. П. Ф. Бэкон и его учение / Ю. П. Михайленко. – М., Наука, 1976.

168. Гончаренко В. Г. Концептуальні питання політико-правової реформи в Україні: академічні читання / В. Г. Гончаренко. – К. : АПрН України, 2007. – (Академічні читання від 14.02.2007).

169. Інформаційний бюлетень ХПГ "Права людини". – 2007. – 4 (440). – С. 2-3.

170. Брижко В. М. е-боротьба в інформаційних війнах та інформаційне право : монографія / В. М. Брижко, М. Я. Швець, В. С. Цимбалюк. – К. : ТОВ "Пан Тот", 2007 р. – 234 с.

171. Кириллов В. И. Логика : учеб. для юридич. вузов и фак. ун-тов / В. И. Кириллов, А. А. Старченко. – [2-е изд., испр. и доп.]. – М. : Высш. шк., 1987. – С. 118-121.

172. Брижко В. М. Ліцензування прав на інформаційні ресурси / В. Брижко, Ю. Базанов, Л. Харченко. – К. : Національне агентство з питань інформатизації при Президентові України, 1997. – 132 с.

173. Системна інформатизація законотворчої та правоохоронної діяльності : монографія / кер. авт. кол. М. Швець. – К. : Навчальна книга, 2005. – 639 с.

174. Валькман Ю. Р. Информационные ресурсы: семиотический подход : материалы III международной научно-практической конференции "Электронные информационные ресурсы: проблемы формирования, обработки, распространения, защиты и использования - 2002". – К. : УкрИНТЭИ, 2002. – С. 11.

175. Брижко В. Організаційно-правові питання захисту персональних даних : дис. ...канд. юрид. наук : 12.00.07 – теорія управління; адміністративне право і процес; фінансове право; інформаційне право / НДЦПІ АПрН України, НАДПС України. – К., 2004. – 251 с.

176. Брижко В. Упорядкування суспільних відносин у сфері захисту персональних даних // Правова інформатика. – 2003. – № 1. – С. 37-46 ; Брижко В., Швець М. До питання е-торгівлі та захисту персональних даних // Правова інформатика. – 2007. – № 1(13). – С. 12-25.

177. Брижко В. Про прийняття Верховною Радою України в цілому Закону України "Про захист персональних даних" // Правова інформатика. – 2006. – № 3(11). – С. 80-90.

178. Брижко В. Про зняття з розгляду Верховною Радою України законопроекту "Про інформацію персонального характеру" // Правова інформатика. – 2005. – № 2(6). – С. 52-64.

179. Лист Інституту законодавства Верховної Ради України Голові Комітету Верховної Ради України з питань науки і освіти від 02.11.2004 р. № 22/438-6-2 (додатково від 05.11.2004 р. № 06-6/9-2760. – С. 4).

180. Повідомлення Харківської правозахисної групи. – Режим доступу – www.khpg.org/index.php?id=1186147137.

181. Верховна Рада проголосувала Закон "Про захист персональних даних", ветований Президентом у квітні 2006 року. Інститут Медіа Права, 17.01.2007. – Режим доступу : www.telekritika.kiev.ua/articles/138/0/8423/verkhovna_rada_progo_losuvala_pro_zakhist_personalnikh_danikh_vetovanij_prezidento.

182. Тихомиров Ю. Л. Публичное право / Ю. Л. Тихомиров. – М., 1995. – С. 339.

183. Рассолов М. М. Правовая информатика и управление в сфере предпринимательства / М. М. Рассолов, В. Д. Элькин, И. М. Рассолов. – М. : Юристъ, 1996. – С. 22. Рассолов М. М. Информационное право: анализ и решение практических задач / М. М. Рассолов. – М., 1998. – С. 4.

184. Атапов А. Б. Основы государственного управления в сфере информатизации в Российской Федерации / А. Б. Атапов. – М. : Юристъ, 1997. – С. 284-285.

185. Баранов О. А. Основи класифікації інформаційного законодавства // Правова інформатика. – 2006. – № 4(12). – С. 23-30.

186. Кудрявцев Ю. В. Нормы права как социальная информация / Ю. В. Кудрявцев. – М., 1987. – С. 6-7.

187. Аграрное право ; под ред. Г. Е. Быстрова и М. И. Козыря. – М., 1996. – С. 13.

188. Баранов О. А. Методи інформаційного права // Правова інформатика. – 2007. – № 4(11). – С. 8-12.

189. Баранов О. А. Система принципів інформаційного права // Правова інформатика. – 2006. – № 2(10). – С. 3-13.

190. Поленина С. В. Комплексные правовые институты и становление новых отраслей права // Правоведение. – 1995. – № 3. – С. 71-79.

191. Райхер В. К. Общественно-исторические типы страхования / В. К. Райхер. – М.-Л., 1947. – С. 189-190.

192. Толстой Ю. К. О теоретических основах кодификации гражданского законодательства // Правоведение. – 1957. – № 1. – С. 42-45.

193. Иоффе О. С. Вопросы теории права / О. С. Иоффе, М. Д. Шаргородский. – М., 1961. – С. 362-365.

194. Алексеев С. С. Общие теоретические проблемы системы советского права / С. С. Алексеев. – М., 1961. - С. 93-101.

195. Алексеев С. С. Проблемы теории права / С. С. Алексеев. – Свердловск, 1972. – Т. 1. – С. 142-148.

196. Красавчиков О. А. Советская наука гражданского права (понятие, предмет, состав и система) / О.А. Красавчиков. – Свердловск, 1961. – Т. 6. – С. 250, 251, 258-263. – (Учен. труды Свердловского юрид. инст-та).

197. Салтевский М. В. Электронные документы в информационном обществе: проблемы формирования юридической концепции : науч.-прак. пособие / М. В. Салтевский, В. П. Гаенко, А. П. Литвинов. – Харьков : Эспада, 2006. – 96 с.

198. Інформаційне право та правова інформатика у сфері захисту персональних даних : монографія / [В. Брижко, М. Гуцалюк, В. Цимбалюк, М. Швець] ; за ред. члена-кореспондента АПрН України М. Швеця. – К. : ТОВ "Пан Тот", 2005 р. - 333 с.

199. Брижко В. М. Патентознавство як самостійна наукова дисципліна / В. М. Брижко. – К. : Національне агентство з питань інформатизації при Президентові України, 1996 р. – 184 с.

200. Про невідкладні заходи щодо розвитку інформаційного суспільства в Україні : доповідь Президенту України Громадської ради з питань інформаційно-комунікаційних технологій. – К., 2005. – Режим доступу : www.ict-forum.in.ua

201. Миников А. М. Международная охрана интеллектуальной собственности. – С-Пб : Питер, 2001. – 720 с. : ил. – (Серия "Закон и практика").

202. Основи інтелектуальної власності. – К. : "Ін-Юре", 1999. – 578 с.

203. Патентное право капиталистических и развивающихся стран. – М. : ВНИИПИ ПНО "Поиск", 1981. – 129 с.

204. Дахно И. И. Патентоведение / И. И. Дахно. – Харьков : Ксилон, 1997. – 313 с.

205. Брижко В. Упорядкування суспільних інформаційних відносин в сфері захисту персональних даних // Правова інформатика. – 2003. – № 1. – С. 38.

206. Еременко В. И. Законодательство о пресечении недобросовестной конкуренции капиталистических стран / В. И. Еременко. – М. : ВНИИПИ ПНО "Поиск", 1991. – 171 с.

207. О судебной практике в делах о нарушении авторских прав в Интернете. – Режим доступу : www.medialaw.ru/publications/books/wb-tele/ch3.html#5

208. Решение арбитражного суда по иску корпорации "Кодак" о запрещении использования в названии веб-страницы названия ее товарного знака. – Режим доступу : www.vic.spb.ru/law/caces/case_tm_omain kodak.htm

209. О решении Интернет-корпорации (ICANN) об правилах использования доменних имен. – Режим доступу : www/icannorg/udrp/udrp-polscy-24oct99.htm

210. Первые судебные решения о личном идентификационном коде в Венгрии. – Режим доступу : www.khpg_org/index.php?id=1084718376

211. Прослушивание телефонов в международном праве и законодательстве одиннадцати европейских стран / Харьковская правозащитная группа ; сост. Е.Е. Захаров ; худож.-оформитель И. М. Гаврилюк. – Харьков : Фолио, 1999. – 152 с.

212. Брижко В. М. Персональні дані та право власності // Українське право : Українська правнича фундація. – 2002. – № 1. – С. 152-157.

213. Брижко В. М. Організаційно-правовий захист персональних даних // Бюлетень з обміну досвідом роботи: редакційно-видавничий відділ МВС України. – 2003. – № 144. – С. 27-33.

214. Брижко В. М. Оподаткування електронної комерції : до питання нормативно-правового захисту персональних даних в Україні у зв'язку з їх економічним змістом // Правова інформатика. – 2008. – № 3(19). – С. 47-56.

215. Повідомлення. – Режим доступу : www.gska2.rada.gov.ua/pls/zweb_n/webp roc4_1?id=&pf3511=27270

216. Типовой закон ЮНСИТРАЛ об электронной торговле від 28.05-14.06.1996 г. [принят на 29-ой сессии ЮНСИТРАЛ] // Комиссия ООН по праву международной торговли. Ежегодник, 1996 г. – Том XXVII. – С. 319-323. – Режим доступу : www.uncitral.org/english/ session/unc

217. Нельзина О. Правовой фундамент електронной коммерции в российской и международной практике / О. Нельзина. – Режим доступу : www.relga.ru/Environ /WebObjects/tgu-www.woa/wa/Main?textid=1954&level1=main&level2=arti cles

218. Дрожжинов В. Азиатско-Тихоокеанский регион плывет по волнам э-коммерции / В. Дрожжинов, А. Штрик. – Режим доступу : www.pcweek.ru/themes /det atl.php?ID= 56419

219. Проблемы электронной комерции. – Режим доступу : www apecsec.org.sg/pubs/free pubs.html#1999

220. Иоффе А. Законодательство по электронной торговле нужно совершенствовать. Режим доступу : www.businesspress.ru/newspaper/article_mId_21961_aId_434369.html

221. Бержье Жак. Промышленный шпионаж / Жак Бержье : [пер. с фр.]. – М. : "Международные отношения", 1972.

222. Електронна комерція: правові засади та заходи удосконалення : монографія / [В. Брижко, А. Новицький, В. Цимбалюк, М. Швець] ; за ред. А. Москаленка, к. ф.-м. наук О. Ладиківської. – К. : ТОВ "Пан Тот", 2008 р. – 149 с.

223. Брижко В. Електронний банкінг у контексті захисту персональних даних : наукове видання / В. Брижко, Ю. Базанов, М. Швець ; за ред. члена-кореспондента АПрН України М. Швеця. – К. : ТОВ "Пан Тот", 2008 р. – 141 с.

224. Тедеев А. А. Электронные банковские услуги : учебное пособие / А. А. Тедеев. – М. : Изд-во Эксмо, 2005. – 272 с.

225. Дослідження Комітету експертів Ради Європи з питань захисту даних у межах повноважень Європейського Комітету правового співробітництва : "Введення та використання особистих ідентифікаційних номерів : питання захисту даних" ; [неофіційний переклад зроблено Р. Романовим (ХНТ) з "The introduction and use of personal identification numbers: the data protection issues". Strasbourg, Council of Europe, Publishing and Documentation Service]. 1991

226. Про концепцію Глобальної інформаційної безподаткової інфраструктури США. Режим доступу : www.dol.com/nze137/materials23&5876

227. Попов В. П. Глобальный бизнес и информационные технологии. Современная практика и рекомендации / В. П. Попов, Р. А. Маршавин, С. И. Ляпунов ; под ред. В. П. Попова. – М., 2001.

228. Про платежі з використанням банківських карток. – Режим доступу : www.globo net.net/fast/454/g0/~65/france

229. Халевинский В. В. Сеть Интернет: технологии и право / В. В. Халевинский, А. А. Тедеев, И. А. Лагутин. – Сб. : ИД Новый Экономикс, 2000.

230. Про проблеми інформаційної безпеки. – Режим доступу : www.klerk_ru/bank/?72111

231. Канали обслуговування електронного банкінгу. – Режим доступу : www.tas-combank.com.ua/index.php?cat=144

232. Беззуб О. О. Яким буде банк XXI століття? / О. О. Беззуб, В. В. Халевинский, А. А. Тедеев, И. А. Лагутин. – Дніпропетровськ : Росток, 2001. – 256 с.

233. Шамраев А. Развитие европейского права электронной коммерции // eCom merse World. – 2000. – № 9.

234. Комплексне порівняльно-правове дослідження відповідності законодавства України законодавству Європейського Союзу у сфері захисту персональних даних : звіт про НДР. – К. : НДЦІІ АПрН України, 2005. – 509 с.

235. Вступ до інформаційної культури та інформаційного права / [В. С. Цимбалюк, В. М. Брижко, В. Д. Гавловський, Р. А. Калюжний та ін.] ; за заг. ред. М. Я. Швеця, Р. А. Калюжного. – Ужгород : ІВА, 2003. – 240 с.

236. Інформаційна культура : навчальний посібник ; за ред. М. Я. Швеця, Р. А. Калюжного. – Ірпінь : Національний університет ДПС України, 2007. – 254 с.

237. Базанов О., Базанов Ю. Про деякі засоби технічного захисту персональних даних // Правова інформатика. – 2004. – № 4. – С. 76-83.

238. Електронне інформаційне суспільство України: погляд у сьогодення і майбутнє : монографія / [В. М. Фурашев, Д. В. Ланде, О. М. Григор'єв, О. В. Фурашев]. – К. : Інжиніринг, 2005. – 164 с.

239. Фейербах Л. История философии : собр. соч. в 3-х т. / Л. Фейербах. – М. : "Мысль", 1967. – Т. 3. – 229 с.

240. До питання адаптації законодавства України до законодавства Європейського Союзу / [від редакційної колегії журналу Правова інформатика] // Правова інформатика. – 2004. – № 2. – С. 58-63.

241. Базанов Ю., Швець М. До питання створення матриці для порівняння інформаційного законодавства // Правова інформатика. – 2004. – № 2. – С. 28-33.

242. Швець М. Методи і засоби інформатики у вирішенні проблем гармонізації законодавства України з європейським правом // Правова інформатика. – 2004. – № 3. – С. 5-7.

243. Тезаурус EUROVOC : посібник / авт. кол. М. Швець, С. Дорогих, В. Брижко ; за ред. академіка НАН України В. Я. Тація та академіка АПН України В. О. Зайчука– К. : Парламентське видавництво, 2004. – 383 с.

244. Дорогих С. Українська версія інформаційно-пошукового тезауруса EUROVOC // Правова інформатика. – 2004. – № 2. – С. 63-76.

245. Швець М., Брижко В. До питання систематизації інформаційного законодавства України // Правова інформатика. – 2007. – № 4(16). – С. 5-7.

246. О первом заседании Совета по развитию информационного общества при Президенте России (2009 г.). – Режим доступу : www.cnews.ru/news/top/ index.shtml?2009/02/12/ 337783.

247. Брижко В. М. Інформаційне право : нормативні та методологічні засади упорядкування інформаційних відносин : монографія / В. М. Брижко, М. Я. Швець. – К.: ТОВ "Пан Тот", 2009 р. – 290 с. – (Рекомендовано до друку вченою радою НДЦПІ АПрН України від 30.10.2008 р., протокол № 10).

248. О. А. Баранов. Правові проблеми конвергенції в інформаційній сфері // Правова інформатика. – 2009. – № 2(22). – С. 5-12.

249. Сергієнко І. В. Уроки академіка Глушкова / І. В. Сергієнко. – К.: Академперіодика, 2008. – 128 с.

250. Сергієнко І. В. Інформаційні та комп'ютерні технології / І.В. Сергієнко. – К.: Наукова думка, 2004. – 432 с. – (НАН України, Ін-т кібернетики ім. В.М. Глушкова).

251. Швець М. Я. Правова інформатика // Правова інформатика. – № 2(18)/2008. – С. 98.

252. Стан та перспективи розвитку інформаційної сфери України: збірник матеріалів з питань становлення інформаційного суспільства в Україні / [за матеріалами Рубана І. А., Семенченко А. І., Трояна П. І., Макарової В. С., Задорожньої Л. М., Брижко В. М.] ; упоряд. та редагування Брижко В. М., Гладківської О. В., Швеця М. Я. – К.: ТОВ "Пан Тот", 2009 р. – 116 с. – (Додаток до наукового журналу "Правова інформатика")

Академія правових наук України
Науково-дослідний центр правової інформатики

НОРМАТИВНО-ПРАВОВІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ УПОРЯДКУВАННЯ ІНФОРМАЦІЙНИХ ВІДНОСИН

НАУКОВО-МЕТОДОЛОГІЧНИЙ ПОСІБНИК

За редакцією
В. Тація, В. Тихого, М. Швеця

* *

Підписано для друку 12.10.2009. Формат 60 х 84/16. Гарнітура Times.
Офсетний друк. Умов. др. арк. 36,6.
Тираж: паперовий варіант – 300 прим., електронний варіант на CD-ROM – 1000 прим.
Виготовлено з оригінал-макета у видавництві ТОВ "ПанТот"
м. Київ, бул. Др. Народів, 28