НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

КИЇВСЬКИЙ УНІВЕРСИТЕТ ПРАВА

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

ІНТЕЛЕКТУАЛЬНИЙ ФОРУМ «ЄДИНА ЄВРОПА»

INTERNATIONAL POLICE ASSOCIATION UA

П.Д. Біленчук
Л.В. Борисова
І.М. Неклонський
В.О. Собина

ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

монографія

Харків 2018

УДК 35.078.3(075.8)
ББК 67.404.3я73
Б 82

Рецензенти:

В.В. Поповський - доктор технічних наук, професор, академік Академії наук прикладної радіоелектроніки, академік Академії зв'язку України, дійсний член IEEE, завідуючий кафедрою інфокомунікаційної інженерії Харківського національного університету радіоелектроніки

Г.С. Семаков - академік Міжнародної кадрової академії, професор кафедри галузевих правових наук Київського університету права Національної академії наук України, заслужений юрист України

Правові засади інформаційної безпеки України: монографія / П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука – Харків: 2018. – 289 с.
ISBN

Затверджено Вченою радою Національного університету цивільного захисту України від 20.11.2018 протокол №3

У монографії систематизовано сукупність відомостей про інформаційну безпеку людини і громадянина, суспільства і держави та шляхи її забезпечення.

Розглянуті особливості інформації як об'єкта правового регулювання інформаційної безпеки, юридичної відповідальності за порушення правових норм.

Для науковців, правників, економістів, безпекознавців, спеціалістів правоохоронних органів і спецслужб, працівників цифрових технологій і медіасфери, здобувачів вищої освіти і аспірантів, які вивчають право, економіку, інформацієзнавство, комунікацієзнавство, безпекознавство, сискознавство, детективознавство, поліцієзнавство, експертознавство, інфокомунікаційну інженерію.

Зміст

1.1.1. Витоки забезпечення регулювання захисту інформації
1.1.2. Правове забезпечення захисту інформації в XIX-XX столітті
Розділ 2. Правове регулювання захисту державної таємниці в Україні
2.2.1. Становлення державних органів, що захищають державну таємницю
2.2.2 Результати діяльності Держкомсекретів України
2.2.3. Державна таємниця як особливий вид інформації, що захищається
2.2.4. Державна служба спеціального зв'язку та захисту інформації
2.2.5. Законодавство регулювання обігу інформації в Україні
2.2.6. Формування системи та органів захисту інформації в Україні
Контрольні питання
Розділ 3. Правове регулювання захисту конфіденційної інформації
3.1. Службова інформація з обмеженим доступом
3.1.1. Поняття і сутність службової інформації
3.1.2. Законодавче забезпечення захисту конфіденційної інформації в Україні
3.2. Професійна таємниця
3.2.1. Поняття і сутність професійної таємниці
3.2.2. Законодавче обмеження доступу до інформації в інтересах правосуддя та судочинства
3.2.3. Комерційна таємниця
3.2.4. Банківська таємниця
3.2.5. Адвокатська таємниця
3.2.6. Нотаріальна таємниця
3.2.7. Лікарська таємниця
3.2.7.1. Історичні витоки формування лікарської таємниці
3.2.7.2. Правовий порядок розголошення лікарської таємниці
3.2.7.3. Етичні принципи психіатричної допомоги
3.3. Охорона інтелектуальної власності
3.3.1. Історіографія формування правової охорони інтелектуальної власності
3.3.2. Сучасний стан правової охорони і захисту інтелектуальної власності у світі
3.3.3. Законодавче забезпечення регулювання правовідносин у сфері інтелектуальної власності в Україні
3.4. Персональні дані та захист права на невтручання в особисте життя
3.4.1. Правове забезпечення захисту прав суб'єктів персональних даних у світі
3.4.2. Правовий захист персональних даних в Україні
Контрольні питання

Частина III. Інноватика: засоби, методи і технології ? захисту інформації
Розділ 1. Правові основи захисту інформації з використанням технічних засобів
1.1. Правовий захист комп'ютерних програм

ПЕРЕДНЄ СЛОВО: КОНЦЕПТУАЛЬНІ ЗАСАДИ СТРАТЕГІЇ, ТАКТИКИ І МИСТЕЦТВА ПРАВОВОГО ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

> Право можна визначити як етичне управління, застосоване до повідомлення і до мови як форми повідомлення, особливо в тому випадку, коли ця нормативна сторона підпорядкована відомій владі, досить сильній, щоб надати своїм рішенням ефективної суспільної санкції. Право являє собою процес регулювання «зчеплень», що поєднують поведінку різних індивідуумів, з метою створення умов, у яких можна справляти так звану справедливість і які дозволяють уникнути спорів або принаймні дають можливість вирішити їх.
>
> *Норберт Вінер*
> *Кібернетика і суспільство*

За останні десятиліття інформація стала настільки потужним фактором розвитку суспільства, що призвела до утворення нового інформаційного укладу, що сприяє внутрішньодержавній і світовій інтеграції та реінтеграції[1].

Нормальне функціонування суспільних інститутів та інших форм соціальної діяльності пов'язують із безпекою: для забезпечення безпеки суспільства створюються органи законодавчої, виконавчої та судової влади, силові структури забезпечення безпеки; у сфері підприємницької діяльності самі фірми створюють спеціальні структури забезпечення своєї безпеки, розробляють відповідний комплекс управлінських заходів і дій; у сфері екологічної та техногенної безпеки застосовуються як адміністративно-організаційні, техніко-технологічні засоби і системи, так і системи, котрі не допускають негативного впливу на навколишнє середовище.

Актуальність проблеми правового регулювання суспільних відносин у сфері інформаційної безпеки зумовлена підвищенням ролі інформації в усіх сферах і видах діяльності особистості та держави в умовах впливу зовнішніх і внутрішніх викликів, загроз, ризиків і небезпек, а також розвитком нових інфо-

[1] Реінтеграція – об'єднання елементів раніше існуючої структури на основі нових методів у нову структуру з новими ієрархічними зв'язками.

рмаційних відносин, котрі вимагають дотримання і захисту конституційних прав, законних інтересів суб'єктів в інформаційно-комунікаційній сфері.

Національні інтереси України в інформаційній сфері полягають у дотриманні конституційних прав і свобод під час отримання інформації і користування нею, у розвитку сучасних телекомунікаційних технологій, захисті державних і приватних інформаційних ресурсів від несанкціонованого доступу.

Національні інтереси України забезпечуються інститутами державної влади і поділяються на:

– інтереси особистості, котрі полягають у реалізації конституційних прав і свобод, забезпеченні особистої безпеки, підвищенні якості та рівня життя, фізичному, духовному та інтелектуальному розвитку людини і громадянина;

– інтереси суспільства, які зводяться до подальшого формування суверенної і незалежної, демократичної, соціальної, правової держави, досягнення та підтримки суспільної згоди, духовного оновлення;

– інтереси держави, що полягають у непорушності конституційного ладу, суверенітету та територіальної цілісності України, політичної, економічної, соціальної стабільності, безумовному забезпеченні законності та підтримки правопорядку, розвитку рівномірного і взаємного партнерського міжнародного співробітництва.

Важливе місце у вирішенні проблеми забезпечення інформаційної безпеки займає реалізація системи комплексного захисту інформації, котра є поєднанням у єдине ціле окремих елементів, механізмів, процесів, явищ, заходів, засобів і програм захисту інформації, взаємозв'язок яких сприяє реалізації цілей, концептуального підходу до питань тимчасового функціонування і структурної побудови системи інформаційного забезпечення охорони і захисту.

Особлива роль у реалізації інформаційної безпеки належить правовому захисту, що визначається:

– підвищенням ролі інформації (інформаційних ресурсів) і засобів її опрацювання в єдиному інформаційному просторі;

– трансформацією традиційних для права соціально-економічних, політичних та інших норм і відносин, що склалися;

– розвитком і появою нових суспільних відносин, що відображають специфіку, особливості і правила взаємовідносин суб'єктів інформаційної сфери.

Зміст наукового видання «Правові засади інформаційної безпеки України» включає наступні питання:

– напрями державної політики України в інформаційній сфері та інформаційній безпеці;

– зміст понять інформації та інформаційних ресурсів як об'єктів правовідносин процесу автоматизації, комп'ютеризації, інформатизації;

– зміст державної системи і концепції правового забезпечення інформаційної діяльності та безпеки в інформаційно-комунікаційній сфері;

– основні положення правового захисту конфіденційної інформації;

– основні положення чинного законодавства про інтелектуальну власність;

– організація правового захисту комерційної таємниці;

– система правового забезпечення державного регулювання діяльності фізичних і юридичних осіб з проведення робіт, пов'язаних із захистом інформації та інформаційної безпеки;

– зміст юридичної відповідальності за порушення у сфері забезпечення інформаційної безпеки.

В умовах складних економічних і політичних процесів, що відбуваються в Україні, першочергового значення набула необхідність написання монографії з сучасної стратегії, тактики і мистецтва забезпечення інформаційної безпеки через призму новітніх досягнень науки і техніки, реалій сьогоденної практики.

Відомо, що особливо важливе місце в сучасному індустріальному цифровому світі належить інформаційній безпеці.

Тому ці аспекти (як теоретичні, так і практичні) інформаційного безпекознавства знайшли відображення в цій праці.

ЧАСТИНА 1. ІНФОРМАЦІЯ, КОМУНІКАЦІЯ І БЕЗПЕКА – СТРАТЕГІЧНІ РЕСУРСИ РОЗВИТКУ СУСПІЛЬСТВА ЗНАНЬ

РОЗДІЛ 1. ІНФОРМАЦІЄЗНАВСТВО І КОМУКАЦІЄЗНАВСТВО – СТРАТЕГІЧНІ РЕСУРСИ РОЗВИТКУ СУСПІЛЬСТВА ЗНАНЬ

1.1. Інформація – основа розвитку суспільства знань

1.1.1. Ера цифрових комунікацій: історіографія формування інформаційно-комунікаційного суспільства знань

Інформаційно-комунікаційні технології є одними з найважливіших чинників, які впливають на формування пріоритетних напрямів розвитку XXI ст.: надаються безпрецедентні можливості доступу до інформації, колективного її використання і взаємного обміну, а також для розвитку освіти, науки, культури, економіки. Їх вплив стосується способу життя людей, освіти та роботи, взаємодії уряду і громадської спільноти. У Декларації про використання науково-технічного прогресу в інтересах миру і для добробуту людства, яка проголошена Резолюцією 3384 (XXX) Генеральної Асамблеї ООН від 10 листопада 1975 р., зазначається, що всі держави сприяють міжнародному співробітництву в цілях використання результатів науково-технічного прогресу в інтересах укріплення міжнародного миру і безпеки, свободи і незалежності з метою економічного і соціального розвитку народів та забезпечення прав і свобод людини у відповідності з Уставом ООН[2].

Процеси перетворення та реалізації знань через матеріалізацію інформаційного ресурсу отримують розвиток за рахунок високих інформаційних технологій, а для отримання і збереження переваг в умовах конкуренції кожна дія в інформаційному середовищі буде мати значний вплив у світі фізичних ресурсів: предметних, фінансових – і в різних абстрактних галузях.

За останні сорок років завдяки надзвичайно могутнім інформаційним технологіям почався процес переходу від індустріальної епохи до цифрового інформаційного суспільства, яке характеризується значною кількістю циркулюючої комунікаційними каналами зв’язку інформації, а також наявністю необхідних

[2] Организация Объединенных Наций. Генеральная Ассамблея. Официальные отчеты. Тридцатая сессия. – Дополнение № 34(A/10034). – С. 111-112.

засобів її збереження, передання, оброблення, використання та захисту, поліграфії, обчислювальної техніки, програмного забезпечення.

Термін «постіндустріальне суспільство» введено у науковий обіг ще у 1958 р. американським соціологом Д. Рісменом. У 1959 р. Професор Гарвардського університету Д. Белл під час виступу на міжнародному соціологічному семінарі в Зальцбурзі (Австрія) вперше використав термін «постіндустріальне суспільство». Це визначення і сьогодні повністю відповідає реаліям – його можна вважати класичним.[3] Префікс *пост-* допускає неоднозначність при тлумаченні основної сутності суспільства. Доступ до інформації є умовою свободи. Збільшення значущості інформації в суспільному житті людини сприяло появі в науковому світі терміну «інформаційне суспільство».

Термін «інформаційне суспільство» започатковано в Японії як головний конструкт локального технологічного розвитку, що було підтверджено звітами професора Токійського технологічного інституту Ю. Хаяші у 1969 – 1971 рр. Японському уряду: «Японське інформаційне суспільство: теми і підходи», «Контури політики сприяння інформатизації японського суспільства», «План інформаційного суспільства».

Народившись завдяки роботі Д. Белла «Настання постіндустріального суспільства» (1973 р.)[4], концепція «інформаційного суспільства» розкрила важливі риси постіндустріального суспільства і збагатила його розуміння, підкресливши значущу роль інформації.[5] Інші дослідники датують появу терміну дещо раніше, акцентуючи увагу на тому, що фактично одночасно було введено в науковий обіг термін «інформаційне суспільство» на початку 60-х років Ф. Махпом у США і Т.Умесао в Японії, поклавши тим самим початок теорії за цією назвою.[6]

---

[3] Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования / В.Л. Иноземцев (пер. с англ.). – М.: Academia, 1999. – 787с.

[4] Белл Д. Грядущее постиндустриальное общество / Д. Белл. – М.: Наука, 1999. – 221с.

[5] Иноземцев В. Современное постиндустриальное общество: природа, противоречия, перспективы. – М.: Логос, 2000. – 302 с.

[6] 5.Мельник О.Л. Інформаційне суспільство та суспільство знань – становлення та розвиток понять. / О.Л. Мельник // Вісник НТУУ «КПІ». Філософія. Психологія. Педагогіка: збірник наукових праць. –2007. – № 2 (20). – ч.2. – С.57-60

«Інформаційне суспільство» виражає ідею нової фази в історичному розвиткові передових країн. Тобто не прихід «постіндустріального» суспільства, а створення нового соціального зразка, що є результатом «другої індустріальної революції», яка, в основному, ґрунтується на мікроелектронній технології. Зростаюча кількість людей з необхідністю втягується в безпрецедентне розмаїття інформаційно-орієнтованих типів робіт. Наукові й технічні працівники збирають і продукують інформацію, менеджери й фахівці опрацьовують її, викладачі й працівники комунікаційної сфери поширюють її. Цей процес «інформатизації» не залишає недоторканою жодну сферу соціальної активності: від повсякденного життя до міжнародних відносин та від сфер дозвілля до виробничих відносин.[7]

Канадський вчений М. Маклюен називає чотири відкриття в історії людства, які зумовили інформаційну революцію. Це – винайдення мови, писемності, друкування, новітніх інформаційних технологій та Інтернет. Інтернет називають «вектором демократизації» «вільним середовищем», хоча на початку функціонування головними завданнями цієї технології спочатку виступали саме контроль над віддаленими об'єктами і управління інформаційним потоком.

Цікавим є прогноз цього процесу, зроблений О. А. Гавриловим: «Згідно з прогнозами соціологів, XXI ст. буде століттям глобальної інформатизації та комп'ютеризації всіх країн. На хвилі «електронної революції» планету покриють сотні та тисячі національних, регіональних і планетарних комп'ютерних систем та мереж. У більшості країн буде створено інформаційне суспільство та інформаційна економіка. Виникне планетарна система телекомунікації»[8].

Окремі дослідники пов'язують нове суспільство з розвитком комунікаційних мереж: з'являються концепції суспільства мережевого інтелекту (Д. Та-

[7] Лайон Д. Інформаційне суспільство: проблеми та ілюзії //Сучасна зарубіжна соціальна філософія. - К., 1996. - С.362-380.

[8] Гаврилов О. А. Компьютерные технологии в правотворческой деятельности : учеб. пособие / Акад. правовой ун-т при Ин-те гос-ва и права РАН. – М. : ИНФРА-М, 1999. – С. 1. Гаврилов О. А. Курс правовой информатики: Учебник для вузов. – М.: Издательство НОРМА (Издательская группа НОРМА – ИНФРА • М), 2002. – 432 с. С.

пскотт), підкреслюється мережевий характер майбутніх соціальних структур (М. Кастельс) та ін. В науці з'явилися концепції суспільства мережевого інтелекту (Д. Тапскотт, А. Лоуи, М. Кастельс).

Концепція постіндустріального суспільства як загально-соціологічна та філософська теорія розвитку розроблена закордонними дослідниками. Д. Белл, Дж. Гелбрейт, Е. Тоффлер, М. Кастельс, Д. Рісмен визначають постіндустріальне суспільство як «цивілізацію послуг».

У Білій книзі Делора, документі Комісії ЄС (Брюссель, від 5 грудня 1993 р.), який визначає завдання і шляхи розвитку інформатизації на XXI ст., уперше введено термін «інформаційне суспільство» і відмічено: «*Інформаційне суспільство* – це суспільство, у якому підґрунтям діяльності людей є використання послуг, які надаються за допомогою інформаційних технологій та технологій зв'язку».

Розвиваючи положення документа Комісії ЄС у плані розвитку конкуренції і зайнятості на саміті Ради Європи 1994 р., було затверджено доповідь М. Бенджеміна «Європа і світове інформаційне співтовариство. Рекомендації Ради Європи», яка вважається основною директивою для організації конкретних дій відповідних органів Ради Європи, спрямованих на взаємодію держав-учасниць у становленні Світового інформаційного співтовариства. Також було прийнято рішення про створення постійно діючого координаційного органу – Ради з проблем Інформаційного Співтовариства. З 1995 р. у Раді Європи почав роботу щорічний Форум з питань Світового інформаційного співтовариства.

Соціолог М. Кастельс відзначає, що «глобальні мережі інструментального обміну селективно підключають або відключають індивідів, групи, райони і навіть країни у відповідності до їхньої значущості для виконання цілей, що обробляються в мережі, у безперервному потоці стратегічних рішень»[9].

Експерти в галузі інформатики відмічають: інформаційне суспільство не має політичних, соціальних та економічних границь.

[9] Кастельс Мануель. Информационная епоха: экономика, общество и культура / Пер. С англ., под науч. ред. О.И. Шкаратана. – М., 2000. – С. 27.

Загальноприйняті *особливості та характеристики інформаційного суспільства* такі:

– наявність інформаційної інфраструктури, що складається з телекомунікаційних[10] мереж та розподілених у них інформаційних ресурсів як запасів знань;

– масове використання персональних комп'ютерів, підключених до телекомунікаційних мереж;

– підготовленість членів суспільства до роботи на персональних комп'ютерах і в телекомунікаційних мережах;

– нові форми і види діяльності в телекомунікаційних мережах чи у віртуальному[11] просторі;

– можливість кожному, практично миттєво, отримувати з телекомунікаційних мереж повну, точну і достовірну інформацію;

– трансформація діяльності засобів масової інформації, інтеграція засобів масової інформації і телекомунікаційних мереж, створення єдиного середовища розповсюдження масової інформації – мультимедіа;

– відсутність географічних і геополітичних границь держав-учасників телекомунікаційних мереж;

– зіткнення і руйнування національних законодавств держав у телекомунікаційних мережах і становлення нового міжнародного права і законодавства.

П. Друкер, професор американських університетів і консультант найбільших фірм США, який у 1966 р. увів у науковий обіг термін «суспільство знань» (knowledge society), що визначає тип економіки, в якій знання відіграють вирішальну роль, а їх виробництво стає джерелом розвитку. В основе общества

---

[10] Телекомунікації – будь-яке передання знаків, сигналів, записів, образів, звуків, інформації чи свідчень будь-якого характеру, що передаються повністю або частково за допомогою телефонного зв'язку, радіо, електромагнітної, фотоелектронної чи фотооптичної системи (Див. Резолюцію Ради Європейського Союзу від 20 червня 2001 р. про оперативні запити правоохоронних органів стосовно телекомунікаційних мереж загального користування).

Телекомунікаційна мережа загального користування означає системи передавання і, у відповідних випадках, комунікаційне обладнання та інші ресурси, що дозволяють передавати сигнали між визначеними кінцевими пунктами за допомогою телеграфу, радіо, оптичних чи інших електромагнітних засобів, які використовуються повністю чи частково, для надання загальнодоступних телекомунікаційних послуг. Телекомунікаційна послуга означає послуги, надання яких повністю чи частково полягає в переданні та маршрутизації сигналів у телекомунікаційних мережах, за винятком радіо- та телевізійного мовлення (Див. Директиву Європейського парламенту і Ради від 15 грудня 1997 р. № 97/66/ЄС стосовно оброблення персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі).

[11] Віртуальний (від лат. *virtualis* – можливий, такий, що може або повинен проявитися при певних умовах, але в реальності не існуючий) – створений на екрані комп'ютера, відтворений комп'ютерним обладнанням.

знаний должна лежать концепция образованной личности. Образованный человек должен уметь проецировать свои знания в настоящее, не говоря уж о том, чтобы заставить их работать на будущее. [12]

На думку Е. Тоффлера вся структура суспільства змінюється, коли однорідність суспільства Другої Хвилі замінюється різнорідністю цивілізації Третьої Хвилі. Взагалі, в економіці Третьої Хвилі знання замінюють і ресурси, і транспортування, те ж можна сказати і про енергію. Знання зменшують потребу в сировині, роботі, часі, просторі, капіталі, та інших ресурсах. Вони стають незамінним засобом – основним ресурсом сучасної економіки, цінність якого постійно зростає.[13]

Знання – єдине, що взагалі являє цінність в умовах «кіберпросторової економіки». Люди мають потребу одержувати інформацію тоді, коли вона їм знадобиться, причому на робочому місці. Тепер, це навчання, що є невід'ємною частиною виробництва.[14] Некваліфікованими в XXI столітті будуть не ті, хто не вміє читати і писати, а ті, хто не вміє вчитися, відмовлятися від вивченого і перенавчатися.[15]

Беручи до уваги сформовані ідеї та концепції інформаційного суспільства, ЮНЕСКО висловила стурбованість обмеженістю та однобокістю концепцій інформаційного суспільства, прийнявши на 32-й Генеральній конференції ЮНЕСКО (Париж, 2003 р.) рекомендації щодо використання терміну «суспільство знань», а не «інформаційне суспільство».[16] ЮНЕСКО стоїть на позиції просування та розвитку концепції «суспільства знань»[17], яка ґрунтується на врахуванні змін у суспільстві, що постійно зростають, та на динамічності навколишнього світу. Цю концепцію умовно називають «стратегією випереджаючого розвитку». Позиція ЮНЕСКО з питань співвідношення інформаційного

[12]Друкер П. Энциклопедия менеджмента: Весь Питер Друкер в одной книге: лучшие работы по менеджменту, написанные за 60 лет / О.Л. Пелявский (пер. с англ.). — М.; СПб.; К.: Издательский дом «Вильямс», 2004. – 421с.
[13] Тоффлер Е. Третя хвиля / Пер. з англ. А. Євси. – К.: Всесвіт, 2000. – 453 с.
[14] Там само.
[15] Там само.
[16] От информационного общества – к обществам знания. ЮНЕСКО // Всемирный саммит по информационному обществу: Информационное издание/ Сост. Е.И. Кузьмин, В.Р. Фирсов. – СПб., 2004. – С.82-84.
[17] Там само.

суспільства та суспільства знань представлена в інтерв'ю заступника Генерального директора ЮНЕСКО з питань комунікації та інформації А.В. Хана, в якому він зазначив, що ці два поняття доповнюють одне одного: інформаційне суспільство є функціональним блоком суспільства знань.[18]

Широке впровадження досягнень науково-технічного прогресу в усі соціально-економічні і виробничі процеси обумовило переведення інформації в розряд економічних і політичних категорій. Процес цей об'єктивно-суб'єктивний, оскільки:

– відбувається підвищення ролі інформації не тільки в житті людини, а й у процесах прийняття державних управлінських рішень, що визначається її головним чинником – одержанням економічних переваг;

– спостерігаються якісно-кількісні зміни інформаційних потреб суспільства, збільшення частки людських ресурсів у роботі з інформацією, що підтверджує необхідність і реалії побудови інформаційної економіки;

– інформація вносить суттєві зміни в характер розроблення стратегії розбудови державності.

1.1.2. Інформація як базовий елемент сучасного інформаційно-комунікаційного суспільства знань

Майже дев'яносто років минуло з того часу, як «інформація» із буденного терміна перетворилася на одну з провідних наукових категорій. Першу спробу уточнити термін «інформація» зробив у 1921 р. Р. Фішер, який хотів підвести «інформацію» під «імовірність»; через сім років Р. Хартлі вводить поняття «логарифмічна міра кількості інформації»; у 1929 р. Л. Сциллард пов'язує інформацію з ентропією. У кінці 1940-х років К. Шенон математично обґрунтував поняття кількості інформації як міри зменшення невизначеності, що перевело слово «інформація» в ряд наукових термінів. «Теорія інформації», створена К. Шеноном, була

[18] На пути к обществам знаний: Интервью с заместителем Генерального директора ЮНЕСКО по вопросам коммуникации и информации г-ном А.В. Ханом // Наука в информационном обществе: Информационное издание / Сост. Е.И. Кузьмин, В.Р. Фирсов. – СПб., 2004. – С.22-26.

першою науковою дисципліною, безпосередньо зв'язаною з переосмисленням феномена інформації.

Ідея про те, що інформацію можна розглядати як щось самостійне, виникла разом з новою наукою – кібернетикою, яка вивчає закономірності управління системами з перероблення інформації (кібернетичними системами), довівши, що інформація має безпосереднє відношення до процесів управління і розвитку, забезпечуючи стійкість і виживання будь-яких систем.

На стадії розвитку інформаційного суспільства інформація перетворюється на ключовий фактор виробництва і стає базовим елементом сучасного суспільства.

Інформація – один із найважливіших феноменів, органічно і фундаментально «вбудованих» у сучасні парадигми наукового пізнання людини, суспільства, світу.

Інформація і є інформація, а не матерія і не енергія. Інформація, за визначенням В. М. Бехтерєва, – «це нематеріальна субстанція, на відміну від речовини або енергії, але від них невід'ємна, як від своїх носіїв»[19].

Вставши в один ряд із такими категоріями як матерія та енергія, інформація перетворилася на надзвичайно широке поняття. Залежно від галузі знань, у якій проводилось дослідження, інформація отримала чималу кількість визначень.

Першим сформулював поняття «інформація» математик Н. Вінер: «Інформація – це визначення змісту, отриманого із зовнішнього світу в процесі нашого пристосування до нього і пристосування до нього наших почуттів. Процес отримання та використання інформації є процесом нашого пристосування до випадковостей зовнішнього середовища нашої життєдіяльності в цьому середовищі»[20].

З свого боку Л. М. Беккер, як і Н. Вінер, підкреслює в цьому понятті ознаку впорядкованості та зазначає, що «інформація» може бути охарактеризована як

[19] Баранов А. А. Права человека и защита персональных данных / А. А. Баранов, В. М. Брыжко, Ю. К. Базанов. – К.: Гос. комитет связи и информатизации Украины, 2000. – С. 51.
[20] Винер Н. Кибернетика и общество/пер. Е. Г. Панфилова ; общ. ред. и предисл. Э. Я. Кальмана. – М. : Сов. радио, 1958. – С. 31.

збереження і відновлення її носієм упорядкованості станів і її джерела, яке впливає на цього носія.

В. Ровенський, А. Уймов під «інформацією» розуміють «повідомлення про події, що відбуваються як у зовнішньому, стосовно системи середовищі, так і в самій системі».

В. Р. Ешбі та А. Д. Урсул пов'язують інформацію з різноманітністю, а також з процесами відображення, котрі завжди супроводжують будь-які взаємодії матеріальних систем; це є підґрунтям уважати, що інформація може існувати там, де є різноманіття.

Інформаційне право на цей час визнає інформацію як третій основоположний фактор після матерії та енергії.

1.1.3. Соціальна роль інформації

Інформація пов'язана з існуванням людства, і тому все, що народжене діяльністю людини, тим чи іншим чином має свою інформаційну сторону.

Найвищим, найбільш складним і різноманітним типом є *соціальна інформація*, оскільки вона створюється і використовується в суспільстві. Отримуючи цю інформацію в процесі комунікації[21], люди застосовують її для цільового впливу на суспільство і управління ним.

Усі види інформації, що циркулюють у суспільстві, об'єднані поняттям «соціальна інформація» і є найвищим типом інформації; а інформаційні відносини отримують соціальний зміст, виступаючи як форми інформаційних процесів. Академік В. Г. Афанасьєв визначив соціальну інформацію як таку, що циркулює в соціальних, суспільного порядку системах, у соціальному управлінні. Це повідомлення, знання про соціальну форму руху матерії тією мірою, якою вона використовується суспільством і людиною.

Інформація відповідає на питання *що трапилось?*. Знання перетворюють інформацію на ресурс і відповідає на запитання *що це означає?*. Таким чином на думку одного спостерігача з його особистими інтересами та підходами ін-

[21] У роботах Г. Ласуелла вперше одержала теоретичне обґрунтування структурна схема руху інформації в процесі комунікації: хто повідомляє, що, кому, з яким успіхом. Г. Ласуелл розробив метод тонкого кількісно-якісного вивчення текстів – контент-аналіз, без якого неможливо обчислити ефективність впливу комунікативних систем на соціальні процеси і скорегувати їх діяльність для більш якісного досягнення результату.

формація – це могутній продукт сучасної реальності. Отже, якщо знання – це відображення дійсності, то інформація – форма подання цієї дійсності. Знання – продукт суспільної, матеріальної та духовної діяльності людей; ідеальне вираження інформації в знаковій формі об'єктивних властивостей та зв'язків світу.

Очевидно, що якісна складова передбачає розуміння смислу, необхідність інформації для певних користувачів. Значущість інформації визначається через імовірність досягнення деякої мети після отримання інформації. Для людини зміст інформації є важливішим за її об'єм. На думку А. П. Єршова, інформація як сукупність знань про фактичні дані та залежність між ними стає стратегічним ресурсом суспільства в цілому і в більшості зумовлює його здатність до успішного розвитку.[22]

1.1.4. Інформаційні ресурси ери цифрових комунікацій

Інформаційні ресурси формуються і використовуються на основі всіх соціальних процесів, усіх форм власності та різних способів організації суспільно корисної діяльності.

Сучасне чинне інформаційне законодавство не дає повного і всебічного юридичного трактування поняття «інформаційні ресурси».

Закон України «Про Національну програму інформатизації» визначає *інформаційний ресурс* як сукупність документів у інформаційних системах (бібліотеках, архівах, банках і базах даних тощо).

Складовою стратегічних ресурсів країни і одночасно національної інфраструктури є державні інформаційні бази даних. Останнім часом були створені такі державні бази даних: «Законодавчі та нормативні акти України», «Податки України» (внесено близько 10 тис. документів), «Ресурси України» (постійно актуалізується інформація про 260 тис. підприємств та організацій України), «Єдиний державний реєстр підприємств та організацій України» (внесено з присвоєнням унікального коду більше ніж 600 тис. суб'єктів господарської діяльності) та ін.

[22] Ершов А.П. Информация: от информационной грамотности учащихся к информационной культуре общества // Коммунист, 1988. – № 2. – С. 82-92.

На цей час діяльність державних установ та організацій щодо формування та використання інформаційних ресурсів є неузгодженою, що спричиняє виникнення певних труднощів у процесі формування єдиного інформаційного середовища і, як наслідок, низький рівень інформаційного та аналітичного забезпечення діяльності державних органів та установ. У 23 міністерствах і відомствах уже існують або створюються електронні інформаційні ресурси, в саме яких зацікавлені органи виконавчої, судової та законодавчої влади. Невизначеність правової та фінансово-економічної основи діяльності різних суб'єктів у сфері інформатизації спричиняє інформаційний монополізм управлінських та комерційних структур на відкриті інформаційні ресурси загального користування, а також обмеження права на використання інформаційних ресурсів держави для більшості громадян.

1.1.5. Інформаційне середовище сучасного суспільства знань: інфраструктурна інформатизація цивілізації

Цілісність сучасного світу забезпечується в основному за рахунок інтенсивного інформаційного обміну. Виробництво, управління, оборона, зв'язок, транспорт, енергетика, фінанси, наука та освіта, засоби масової інформації – усе залежить від інтенсивності інформаційного обміну, повноти, своєчасності, достовірності інформації. Зупинка глобальних інформаційних потоків, навіть на деякий час, здатна спричинити кризу не меншу, ніж розірвання міждержавних економічних відносин. Іншою стороною цих процесів є збільшення кількості цінної інформації, яка обробляється в автоматизованих системах. І саме від якості, достовірності та оперативності одержання цієї інформації залежить більшість важливих рішень.

Закон України «Про Національну програму інформатизації» формулює стратегію розв'язання проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержав-

ного значення. Національна програма інформатизації[23] включає: Концепцію Національної програми інформатизації; сукупність державних програм з інформатизації; галузеві програми та проекти інформатизації; регіональні програми та проекти інформатизації; програми та проекти інформатизації органів місцевого самоврядування.

Національна програма інформатизації формується, виходячи з довгострокових пріоритетів соціально-економічного, науково-технічного, національно-культурного розвитку країни з урахуванням світових напрямів розвитку та досягнень у сфері інформатизації, і спрямована на розв'язання найважливіших загальносуспільних проблем (забезпечення розвитку освіти, науки, культури, охорони довкілля та здоров'я людини, державного управління, національної безпеки та оборони держави і демократизації суспільства) та створення умов для інтеграції України у світовий інформаційний простір відповідно до сучасних тенденцій інформаційної геополітики. Національна програма інформатизації становить комплекс взаємопов'язаних окремих завдань (проектів) інформатизації, спрямованих на реалізацію державної політики та пріоритетних напрямів створення сучасної інформаційної інфраструктури України (див. табл. 1) за рахунок концентрації та раціонального використання фінансових, матеріально-технічних та інших ресурсів, виробничого і науково-технічного потенціалу держави, а також координації діяльності органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій усіх форм власності і громадян у сфері інформатизації.

Таблиця 1 *Клаус Шваб*

Основні напрями інформатизації України

Напрям	Система заходів
Розроблення політики та організаційно-правове забезпечення інформа-	Захист авторського права, прав і свобод громадян щодо інтенсивної інформаційної взаємодії держави та громадянина відповідно до Конституції України; економічне стимулювання створення національного інформаційного ресурсу; доступ фізичних та юридичних осіб до міжнародних інформа-

[23] Інформатизація – сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки.

Напрям	Система заходів
тизації	ційних ресурсів; розроблення системи державних стандартів у галузі інформатизації; сертифікація технічного і програмного забезпечення; розроблення нормативних актів про діяльність та взаємодію державних та комерційних структур в аспекті виконання програми інформатизації
Формування національної інфраструктури інформатизації	Створення міжнародних та міжміських телекомунікаційних і комп'ютерних мереж; систем інформаційно-аналітичних центрів різного рівня; інформаційних ресурсів; інформаційних технологій; систем науково-дослідних установ з проблем інформатизації; виробництво та обслуговування технічних засобів інформатизації; впровадження системи підготовки висококваліфікованих фахівців у сфері інформатизації
Інформатизація стратегічних напрямів розвитку державності, безпеки та оборони	Створення комплексу інформаційних технологій та засобів інформатизації для збирання, зберігання, аналізу і оброблення інформації про стан соціально-економічних процесів в Україні для забезпечення інформаційно-аналітичної підтримки прийняття рішень органами державної влади, інформаційно-аналітичної системи Верховної Ради України, інструментально-технологічного комплексу підтримки прийняття рішень у штатних і нештатних ситуаціях в умовах інформаційної протидії; Урядової інформаційно-аналітичної системи з питань надзвичайних ситуацій тощо
Інформатизація пріоритетних галузей економіки	Створення комплексу автоматизованих систем оброблення даних та управління різного рівня і призначення, які взаємопов'язані на принципах технологічної, організаційної, документаційної, програмної та інформаційної сумісності та утворюють інформаційну інфраструктуру
Інформатизація процесів соціально-економічного розвитку	Створення баз даних і знань, а також засобів їх оброблення, орієнтованих на ефективну інформатизацію органів державної статистики і точне прогнозування процесів соціально-економічного розвитку, зокрема інформаційно-довідкових систем ринку праці, товарів і послуг, контролю за якістю споживчих товарів та ін., з подальшим використанням їх для формування систем електронної комерції
Інформатизація соціальної сфери	Створення єдиної структурованої інформаційної системи обліку стану здоров'я громадян України на основі автоматизованої реєстрації пацієнтів у лікувальних установах, збирання даних профілактичних обстежень з метою подальшого використання в статистичних, аналітичних та експертних системах; створення системи дистанційного консультування та діагностики на основі комп'ютерних мереж, що об'єднують великі лікувальні та наукові заклади, створення для управлінських і регіональних структур програмних систем та засобів обліку всіх рівнів, аналізу і моделю-

Напрям	Система заходів
	вання зайнятості населення, запобігання масовому безробіттю та для широкого залучення населення до нових галузей матеріального виробництва та інших сфер
Міжнародне співробітництво	Організація та постійне вдосконалення взаємозв'язку національних телекомунікаційних систем із комп'ютерними мережами інших країн та глобальною мережею Інтернет, забезпечення доступу до міжнародних інформаційних масивів та баз даних і геоінформаційних систем, створення системи інформаційно-телекомунікаційного забезпечення міждержавного співробітництва у сфері торгівлі, охорони здоров'я, боротьби з міжнародною злочинністю, гідрометеорології; створення системи зовнішньоторговельної інформації стосовно міжнародних, національних державних і регіональних програм співробітництва, міжнародного та українського законодавства, інформаційно-телекомунікаційної бази для системного вивчення стану світових ринків товарів (продукції, послуг) і маркетингового забезпечення діяльності українських експортерів
Інформатизація науки, освіти і культури	Розвиток інформаційної культури людини (комп'ютерної); розвиток змісту, методів і засобів навчання до рівня світових стандартів; скорочення терміну та підвищення якості навчання і тренування на всіх рівнях підготовки кадрів; інтеграція навчальної, дослідницької та виробничої діяльності; удосконалення управління освітою, створення комп'ютерних інформаційних систем для поширення культурних еталонів, стандартів і досягнень вітчизняної культури, насамперед створення електронних копій творів та архівів видатних діячів національної культури, представлення їх у системах глобальних комп'ютерних комунікацій для їх ефективного використання у сфері освіти та виховання, що дасть змогу у будь-якій точці України отримувати не тільки необхідну інформацію з економічних, агробіологічних, зоотехнічних, медичних, маркетингових, технологічних, юридичних питань, а і відповідні знання з історії та культури України, культури інших народів через автоматизовані бібліотеки; створення національної системи комп'ютерної лексикографії; формування національної лінгвістичної мережі та інтеграції її до аналогічних міжнародних мереж у рамках проектів розвитку *multylingual society*; розроблення інтелектуальних унормованих лінгвістичних україномовних комп'ютерних систем (автоматичні коректори та редактори, системи автоматичного перекладу, реферування, екстракції знань з природомовних текстів, розуміння природної мови як у писемному, так і в усному варіантах)

Напрям	Система заходів
Інформатизація фінансової та грошової системи, державного фінансово-економічного контролю	Створення класифікаторів, уніфікованих систем документообігу, Державного реєстру фізичних та юридичних осіб – платників податків на основі єдиної бази даних населення України; єдиної автоматизованої системи державного контролю за виконанням Державного бюджету України, фінансування загальнодержавних програм, збереження і використання об'єктів прав державної власності, використання кредитних ресурсів, контролю за діяльністю установ банківської системи
Інформатизація в галузі екології та використання природних ресурсів	Створення на основі картографічних баз даних багатоцільової інформаційно-технологічної бази з використанням геоінформаційних технологій збирання, зберігання, аналізу всієї сукупності відомостей для моделювання і подальшого прогнозування екологічного стану територій; створення комплексу програмно-апаратних засобів для вирішення питань прогнозування забруднення навколишнього середовища, аналізу та оцінки ризику еколого-економічних конфліктів, прогнозування наслідків техногенного впливу і природних катастроф для надійного захисту екологічного простору України, раціонального використання природних ресурсів на основі підвищення узгодженості управління різними видами виробничої діяльності

Відповідно до ст. 5 Закону України «Про Національну програму інформатизації», головною метою Національної програми інформатизації є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави.

Програма спрямована на вирішення таких основних завдань:

– формування правових, організаційних, науково-технічних, економічних, фінансових, методичних та гуманітарних передумов розвитку інформатизації;

– застосування та розвиток сучасних інформаційних технологій у відповідних сферах суспільного життя України;

– формування системи національних інформаційних ресурсів;

– створення загальнодержавної мережі інформаційного забезпечення науки, освіти, культури, охорони здоров'я тощо;

– створення загальнодержавних систем інформаційно-аналітичної підтримки діяльності органів державної влади та органів місцевого самоврядування;

– підвищення ефективності вітчизняного виробництва на основі широкого використання інформаційних технологій;

– формування та підтримка ринку інформаційних продуктів і послуг;

– інтеграція України у світовий інформаційний простір.

Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 9 січня 2007 р. № 537-V визначив основні стратегічні цілі розвитку інформаційного суспільства в Україні:

– прискорення розроблення та впровадження новітніх конкурентоспроможних інформаційно-телекомунікаційних технологій в усі сфери суспільного життя, зокрема в економіку України і в діяльність органів державної влади та органів місцевого самоврядування;

– забезпечення комп'ютерної та інформаційної грамотності населення, насамперед, шляхом створення системи освіти, орієнтованої на використання новітніх інформаційно-телекомунікаційних технологій у формуванні всебічно розвиненої особистості;

– розвиток національної інформаційної інфраструктури та її інтеграція зі світовою інфраструктурою;

– державна підтримка нових «електронних» секторів економіки (торгівлі, а також підтримка фінансових і банківських послуг тощо);

– створення загальнодержавних інформаційних систем насамперед у сферах охорони здоров'я, освіти, науки, культури, охорони довкілля;

– збереження культурної спадщини України шляхом її електронного документування;

– державна підтримка використання новітніх інформаційно-комунікаційних технологій засобами масової інформації;

– використання інформаційно-телекомунікаційних технологій для вдосконалення державного управління, відносин між державою і громадянами, ста-

новлення електронних форм взаємодії між органами державної влади та органами місцевого самоврядування і фізичними та юридичними особами;

– досягнення ефективної участі всіх регіонів у процесах становлення інформаційного суспільства шляхом децентралізації та підтримки регіональних і місцевих ініціатив;

– захист інформаційних прав громадян, насамперед, щодо доступності інформації, захисту інформації про особу, підтримки демократичних інститутів та мінімізації ризику «інформаційної нерівності»;

– удосконалення законодавства з регулювання інформаційних відносин;

– покращення стану інформаційної безпеки в умовах використання новітніх інформаційно-комунікаційних технологій.

Слід зазначити, що членство України в Раді Європи зобов'язує гарантувати дотримання прав людини і в інформаційній сфері та сприяти розвитку інформаційного суспільства. Відповідно до Резолюції ПАРЄ № 1466 та Пояснювального меморандуму до числа зобов'язань України в інформаційній сфері належать:

– перетворення державних ТРК на канали суспільного мовлення;
– приватизація друкованих ЗМІ, заснованих органами публічної влади;
– гарантування прозорості власності ЗМІ;
– створення рівних умов для діяльності усіх ЗМІ шляхом перегляду Закону України 1997 р. «Про державну підтримку ЗМІ та соціальний захист журналістів»;
– ратифікація Європейської конвенції про транскордонне телебачення;
– забезпечення відповідності нової редакції Закону України «Про телебачення і радіомовлення» до стандартів Ради Європи і рекомендацій її експертів;
– вдосконалення законодавства щодо запобігання концентрації медіавласності відповідно до стандартів РЄ;
– вилучення із Закону України «Про Національну раду з питань телебачення і радіомовлення» положення щодо можливості висловлення Президентом

та Верховною Радою недовіри Національній раді, що спричинить відставку її складу;

– ліквідація Держкомтелерадіо під час перегляду Конституції України;

– вилучення з Цивільного кодексу України положення (ч. 3 ст. 277) щодо презумпції недостовірності негативної інформації, поширеної про особу.

– Інформація як повноправна загальнонаукова категорія і базовий елемент інформаційного суспільства відіграє важливу роль у розвитку сучасної цивілізації. Проблеми підвищення інформаційного потенціалу напряму пов'язані із перспективами зростання держави та укріплення її позицій на світовій арені. Розвиток інформаційних ресурсів на цей час визначає місце держави в міжнародних політичних, економічних, соціальних та інших процесах, формуючи єдиний багатофакторний процес глобалізації

1.2. Формування законодавства про інформацію в Україні

1.2.1. Інформація як об'єкт правових відносин

Право є найдавнішим механізмом саморегуляції суспільства, що адаптує все нове у сформовану й налагоджену систему відносин і правового регулювання. Уся правова система відносин ґрунтується на двох початках: функції вираження владної волі, що представлена законодавчою галуззю державної влади, і на інформаційній функції права і законодавства.

Право і його система зазнають впливу нових технологій, використовуючи можливості технічного і наукового прогресу.

Право є керуючою інформацією, яка підкріплена владно-організаційними механізмами політичної системи, що забезпечує порядок дії, невідворотність дії й впливу цієї (правової) інформації.

У науковій літературі виділяють такі *ознаки інформації*, що обумовлені її специфічними властивостями і мають значення для права:

1. Певна самостійність інформації по стосовно свого носія. Для інформації характерною є наявність матеріального носія, фізико-хімічні властивості якого не чинять визначального впливу на організацію інформації. В інформаційних

процесах ця властивість дозволяє встановлювати правовий статус матеріальних носіїв інформації, на яких закріплено її зміст та реквізити, що дозволяють встановити джерело, повноту інформації, ступінь її вірогідності, належності, наявності внесених змін тощо.

2. Можливість багаторазового використання однієї й тієї ж самої інформації, тобто вона зберігається, незалежно від того, скільки разів вона була використана. Нематеріальна природа дозволяє розповсюджувати її серед невизначеного кола осіб, незалежно від місця знаходження матеріального носія.

3. Невичерпність інформації під час використання.

4. Збереження переданої інформації в суб'єкта, який передає, означає, що юридично передання інформації неможливо порівнювати з переданням речей, і з цієї причини не може бути кваліфіковане як крадіжка, протизаконне привласнення (копіювання) машинної інформації.

5. Непідлеглість інформації фізичному зносу. У цьому випадку говорять про моральний знос (старіння).

6. Здатність до збереження, інтегрування, накопичування та стискання. Стискання, тобто запис великої кількості інформації на відповідному носії, здійснюється як шляхом перетворення форми подання інформації (реферування), так і шляхом підвищення ємності носіїв інформації (мікрофільмування, запис на магнітні носії інформації, диски тощо). Стискання інформації передбачає її впорядкування, надає можливість більш ефективно здійснювати її пошук, допомагає забезпечувати своєчасність, повноту, точність видання інформації.

7. Кількісна визначеність інформації.

8. Системність інформації.

Дані ознаки обов'язково слід враховувати у процесі формування законодавства про захист інформації.

У випадку з інформаційними відносинами головна проблема полягає в тому, що їхній розвиток на базі вдосконалення технічних засобів відбувається настільки швидко, що суспільство не встигає усвідомити набуті результати, а вже

отримує наступні. А. Б. Венгеров зазначає, що не сама інформація, а відносини з приводу інформації стають *предметом правового регулювання*.

Інформація як об'єкт правових відносин, за визначенням В. О. Копилова, повинна бути конкретизована, організована, певним чином прив'язана до ситуації та конкретного виду відносин, класифікована за видами і тому подібним чином підготовлена для здійснення з її приводу дій, що регулюються нормами права.

Формування законодавства про інформацію відповідає завданням створення національних систем правової інформації. Як записано у ст. 19 Загальної декларації прав людини, яка прийнята і проголошена Резолюцією 271А (III) Генеральної Асамблеї ООН 10 грудня 1948 р., кожний має право шукати, отримувати, розповсюджувати інформацію. У ст. 10 Європейської конвенції про захист прав людини і основних свобод від 4 листопада 1950 р. відмічається, що свобода отримувати й розповсюджувати інформацію реалізується без будь-якого втручання з боку держави і незалежно від кордонів та «здійснення цих свобод, оскільки воно [це здійснення] пов'язане з правами і обов'язками, може бути предметом таких формальностей, умов, обмежень або покарань, які встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для захисту здоров'я і моралі, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримки авторитету і неупередженості правосуддя».

Дотримання основних міжнародних принципів права доступу громадян до інформації передбачає:

– презумпцію відкритості та вільного доступу до інформації;

– її повноту та достовірність;

– своєчасність надання інформації;

– обмеження права доступу до неї тільки відповідно до законних режимів доступу до інформації;

– право судового оскарження у разі заборони доступу громадян до інформації.

Відповідно до міжнародних домовленостей основними джерелами права, що регулюють інформаційні відносини та забезпечують захист суб'єктів і об'єктів інформаційних технологій від злочинних посягань, є: Європейська конвенція про захист осіб щодо автоматизованого оброблення даних особистого характеру від 28 січня 1981 р. № 108; директиви Європейського парламенту і Ради: про захист фізичних осіб під час оброблення персональних даних і про вільне переміщення таких даних від 24 жовтня 1995 р. № 95/46/ЄС, про правовий захист даних від 11 березня 1996 р № 96/9/ЄС, про спільну базу для загальних дозволів та індивідуальних ліцензій у сфері телекомунікаційних послуг від 10 квітня 1997 р. № 97/13/ЄС щодо оброблення персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі від 15 грудня 1997 р. № 97/66/ЄС, про систему електронних підписів, що застосовуються в межах Співтовариства від 13 грудня 1999 р. № 1999/93/ЄС, про відкриття і ведення діяльності установ-емітентів електронних грошей, а також про здійснення розумного нагляду за цією діяльністю від 18 вересня 2000 р. № 2000/46/ЄС та інші міжнародні угоди.

1.2.2. Правове регулювання захисту та обмеження доступу до інформації

Розвиток в Україні відносин власності та визнання інформації як об'єкта права власності, підвищення цінності інформації як товару зумовили вдосконалення законодавчого процесу й тактики регулювання інформаційно-правових відносин з метою узгодження вітчизняного законодавства із загальноприйнятими міжнародними нормами, закріпленими у ст. 9 Конституції України, що дозволяє стверджувати: наша держава стимулює розвиток інфраструктури на основі новітніх технологій. Прикладом цього можуть служити закони стосовно інформатизації всіх сфер суспільної діяльності в Україні, які прийняла Верховна Рада України 4 лютого 1998 р.; національне (державне, публічне) право України прямо чи опосередковано регулює інформаційні відносини в суспільс-

тві; Концепція Національної програми інформатизації, у розд. VI якої визначаються основні напрями інформатизації (див. табл. 1); Указ Президента «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні».

Основою правового регулювання захисту та обмеження доступу до інформації є:

– норми ч. 1 ст. 32 Конституції України, згідно з якими 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;

– норми ч. 2 ст. 34 Конституції України, що передбачають можливість обмеження свободи інформації на основі закону в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Аналіз правового регулювання інформаційних відносин в Україні та міжнародної практики дозволяє визначити низку методологічних, принципових положень інформаційного законодавства, яке виступає публічно-правовою основою такої юридичної інституції, як інформаційне право:

– основний *об'єкт регулювання* – суспільні відносини;

– основний *предмет суспільних відносин* – інформація (відомості, дані, знання, таємниця тощо);

– *метод правового регулювання* – системне, комплексне застосування методів конституційного (публічно-правового регулювання) та застосування методів приватноправового регулювання (на рівні правочинів, угод, звичаїв, традицій, норм суспільної моралі, професійної ділової етики);

– за правовою природою походження як міжгалузевий комплексний інститут національного права України має приватно-правову і публічно-правову природу;

– через предмет суспільних відносин інформаційне право має зв'язок з іншими міжгалузевими інститутами права: авторським правом, правом власності, правом інтелектуальної власності тощо та утворює складну агреговану гіперсистему права.

Аналіз чинного публічно-правового регулювання суспільних інформаційних відносин дозволяє сформувати структуру законодавства України у сфері інформаційних правовідносин на основі положень теорії гіперсистеми права[24]. Інформаційні правовідносини на рівні законодавства регулюються двома групами законодавчих актів:

1) *загальноправові акти*, дія яких поширюється на всіх суб'єктів інформаційних відносин відповідно до поділу права України на правові галузі: конституційне, адміністративне, цивільне, трудове, кримінальне (Конституція України, Цивільний кодекс України, Цивільний процесуальний кодекс України, Кодекс про адміністративні правопорушення України, Кодекс законів про працю України, Кримінальний кодекс України та Кримінально-процесуальний кодекси України);

2) *спеціально-правові акти*, дія яких поширюється тільки на суб'єктів, які беруть безпосередню участь у конкретній соціальній діяльності (наприклад, Закон України «Про авторське право і суміжні права»).

Спеціально-правові акти розподіляються на дві категорії, котрі мають відповідні *системоутворюючі* законодавчі акти (у теорії права вони формують синтетичні міжгалузеві комплексні інститути права):

– *системоутворюючі загальні норми* публічно-правового регулювання інформаційних відносин (інформаційне право): в Україні – Закон України «Про інформацію»;

– *системоутворюючі окремі інституції* інформаційного права – закони України «Про наукову і науково-технічну діяльність», «Про державну таємницю», «Про державну статистику», «Про Національний архівний фонд та архівні

[24] Відповідно до теорії гіперсистеми права інформаційне законодавство існує як міжгалузевий комплексний інститут у загальній системі національного законодавства. Категорія «гіперсистема права» відносно нова і виникла на основі здобутків кібернетики та інформатики стосовно вивчення права як соціальної гіперсистеми. У теорії гіперсистем висувається теза про існування права у вигляді великих, складних, ієрархічних підсистем, що формуються з галузевих інститутів права.

установи», «Про друковані засоби масової інформації (пресу) в Україні», «Про інформаційні агентства» тощо.

У системі загальноправових норм умовно виділяють комплекс публічно-правових норм, що регулюють інформаційні відносини у сфері інформатизації, включаючи технічні засоби комунікації. До них належать такі системоутворюючі закони України: «Про телекомунікації», «Про Національну програму інформатизації», «Про систему Суспільного телебачення і радіомовлення України», «Про Концепцію Національної програми інформатизації».

Окремі загальнообов'язкові положення щодо інформаційних відносин розміщені в галузевих (за сферами правовідносин) законодавчих актах, наприклад, у законах України «Про державну податкову службу в Україні», «Про оперативно-розшукову діяльність», «Про Службу безпеки України», «Про прокуратуру» та ін.

Серед спеціальних виділяють підсистеми публічного права, що регламентують інформаційні відносини в окремих сферах економічних відносин: це закони України «Про банки і банківську діяльність», «Про захист від недобросовісної конкуренції», «Про захист економічної конкуренції», нормативні акти у сфері антимонопольної політики держави тощо.

1.2.3. Інформаційне право як система норм, що регулюють відносини в інформаційній сфері

Провідні функції інформаційного права визначаються на основі загальних функцій права:

– *нормативна* – визначення норм, правил поведінки суб'єктів інформаційних відносин (правового поля);

– *комунікативна* – зазначення в окремих статтях посилань на законодавчі акти, які є системоутворюючими різних міжгалузевих інститутів права (або необхідність у яких може виникнути);

– *регулятивна* – визначення прав та обов'язків, зобов'язань суб'єктів щодо регулювання суспільних інформаційних відносин;

– *охоронна* – визначення гарантій та меж правомірної поведінки суб'єктів, які здійснюють заходи щодо недопущення та профілактики правопорушень, а також контроль за дотриманням правомірної поведінки;

– *захисна* – визначення правових умов, процедур та суб'єктів, які здійснюють захист від скоєних правопорушень (поведінки, за якою діяння утворюють делікти), та відповідальності за ці правопорушення згідно з нормами цивільного, адміністративного, трудового та кримінального права;

– *інтегративна* – системне поєднання комплексу визначених юридичних норм, котрі регулюють інформаційні відносини в Україні в різних підсистемах права (інформаційне право є поєднуючою ланкою між провідними традиційними галузями права і застосовує їх методи у сфері інформаційних відносин).

За сутністю правового походження як міжгалузевий комплексний інститут національного права України інформаційне право має приватноправову і публічноправову природу, тобто норми інформаційного права формуються як на публічному (державному), так і на приватному рівнях суспільних відносин.

Визначення статусу інформаційного права як міжгалузевого комплексного інституту права зумовлює визначення співвідношення його з іншими інститутами права, предметом яких є суспільні відносини щодо інформації (твір, винахід, корисна модель, масова інформація, архіви, бібліотеки тощо). Через предмет суспільних відносин (інформацію) інформаційне право має зв'язок з іншими міжгалузевими інститутами права: авторським правом, правом інтелектуальної власності, винахідницьким правом, рекламним правом тощо.

Інформаційне право утворює з ними велику складну агрегативну гіперсистему права третього порядку: відповідно до теорії гіперсистем права інформаційне право ґрунтується на засадах правових систем другого порядку, якими є п'ять галузей права: конституційне, адміністративне, цивільне, трудове, кримінальне. У своїй єдності вони утворюють систему першого порядку – право України. Важливим аспектом теорії інформаційного права є проблематика його підсистем – спеціальних субінститутів – сфер правового регулювання інформаційних правовідносин, а саме:

– визначення та правове закріплення провідних напрямів і методів державної політики у сфері вибору мов спілкування, комунікації в державі тощо;

– регулювання суспільних відносин у сфері засобів масової інформації, визначення їх подібностей та відмінностей, систематизація їх через агрегацію (преса, видавнича справа, радіо, телебачення, комп'ютерні мас-медіа тощо);

– забезпечення умов для розвитку механізму захисту всіх форм власності на інформацію та інформаційні ресурси (право власності на інформацію);

– організація та управління створенням і розвитком державних інформаційних систем і мереж, забезпечення їх сумісності та взаємодії в єдиному інформаційному просторі України;

– 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, складовою якої є інформаційна безпека, визначення загроз суспільним інформаційним відносинам, регулювання захисту інформації, у тому числі в автоматизованих системах;

– забезпечення реалізації конституційних прав осіб (приватних немайнових) на режим доступу до персональних даних – інформації про громадян та їх організації за умов інформатизації державних органів управління та створення приватних (недержавних) автоматизованих баз даних;

– державно-правове сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем, технологій із пріоритетами для вітчизняних виробників інформаційної продукції, засобів, технологій;

– забезпечення правового режиму формування і використання національних інформаційних ресурсів, збирання, оброблення, накопичення, зберігання, пошуку, поширення та надання споживачам інформації.

1.2.4. Правове регулювання відносин в інформаційній сфері

Інформаційні відносини, оскільки суб'єктами передання інформації в них виступають як індивіди, так і соціальні групи, є різновидом суспільних відносин. Тому держава встановлює відповідні правові норми, якими регламентуються права, обов'язки та правила поведінки їх учасників.

Сучасне інформаційне законодавство України має характер змішаної системи права: зберігши галузевий підхід традиційної континентальної системи права, воно стало на шлях публічно-правового законотворення за доктриною загального права (англо-американської системи права), коли окремі проблеми на законодавчому рівні вирішуються на рівні окремих законів.

Правове регулювання інформаційних правових відносин в Україні забезпечується низкою нормативних актів, у тому числі: Конституцією України, Кримінальним кодексом України, Цивільним кодексом України, законами України «Про інформацію» від 2 жовтня 1992 р. № 2657-XII, «Про науково-технічну інформацію» від 25 червня 1993 р. № 3322-XII, «Про державну таємницю» від 21 січня 1994 р. № 3855-XII, «Про авторське право і суміжні права» від 23 грудня 1993 р. № 3792-XII, «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 р. № 80/94-ВР, «Про доступ до публічної інформації» від 13 січня 2011 р. № 2939-VI та іншими нормативними документами.

Інформаційні відносини, в яких названі суб'єкти (індивіди, соціальні групи) «беруть участь як носії прав і обов'язків, встановлених нормами інформаційного права, називаються *інформаційно-правовими відносинами* (інформаційними правовідносинами)»[25]. Ці правові норми регламентують параметри інформаційних процесів, за якими відбувається обіг інформації в суспільстві. Залежно від виду інформації законодавство передбачає відсутність тих чи інших обмежень або заборон.

Першим законодавчим актом, що стверджує інформаційний суверенітет України, закріплює право громадян на інформацію, закладає правові основи інфо-

[25] Рассолов М. М. Информационное право / М. М. Рассолов. – М. : Юристъ, 1999. – С. 41.

рмаційної діяльності і визначає правові форми міжнародного співробітництва у сфері інформації, став Закон України «Про інформацію».

Згідно зі ст. 1 цього Закону, під інформацією розуміють «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі».

Особливістю правового регулювання обігу інформації є те, що залежно від типу інформації існують і відповідні специфічні правила поведінки у процесі здійснення інформаційної діяльності, що встановлені правовими нормами.

Стаття 28 Закону України «Про інформацію» визначає режим доступу до інформації як передбачений правовими нормами порядок отримання, використання, поширення і зберігання інформації і поділяє інформацію на відкриту та інформацію з обмеженим доступом (див. рис. 1).

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну й таємну.

Стаття 30 Закону України «Про інформацію» дає таке визначення *конфіденційної інформації*: це «відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їхнім бажанням відповідно до передбачених ними умов».

Відповідно до ст. 7 Закону України «Про доступ до публічної інформації», *конфіденційна інформація* – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

До *таємної інформації* належить інформація, що містить відомості, які становлять державну таємницю, а також іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі (ст. 30 Закону України «Про інформацію»).

Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю слідства та іншу передбачену законом таємницю (ст. 8 Закону України «Про доступ до публічної інформації»).

Тип правового регулювання обігу інформації є однією з визначальних юридичних характеристик інформації.

За диспозитивного методу умови обігу інформації її використання, розповсюдження, передання прав на неї третім особам визначаються або власником цієї інформації особисто, або на основі договору з іншими зацікавленими особами, що не означає відсутності нормативно-правового регулювання обігу цієї інформації, але в рамках цього регулювання існує відповідна свобода дії (законодавство про авторські права, про право інтелектуальної власності, законодавство, що охороняє інформацію про особисте життя, зазначають, що відповідна інформація може бути оприлюднена тільки за згодою особи).

Специфічним є обіг інформації, який регулюється імперативним методом, що характеризується наявністю чітких законодавчих приписів і норм поведінки, відміна яких за згодою сторін неможлива. Це стосується встановлених законом прямих обмежень щодо державної, лікарської, адвокатської таємниці, певних видів статистичної інформації, персональних даних тощо.

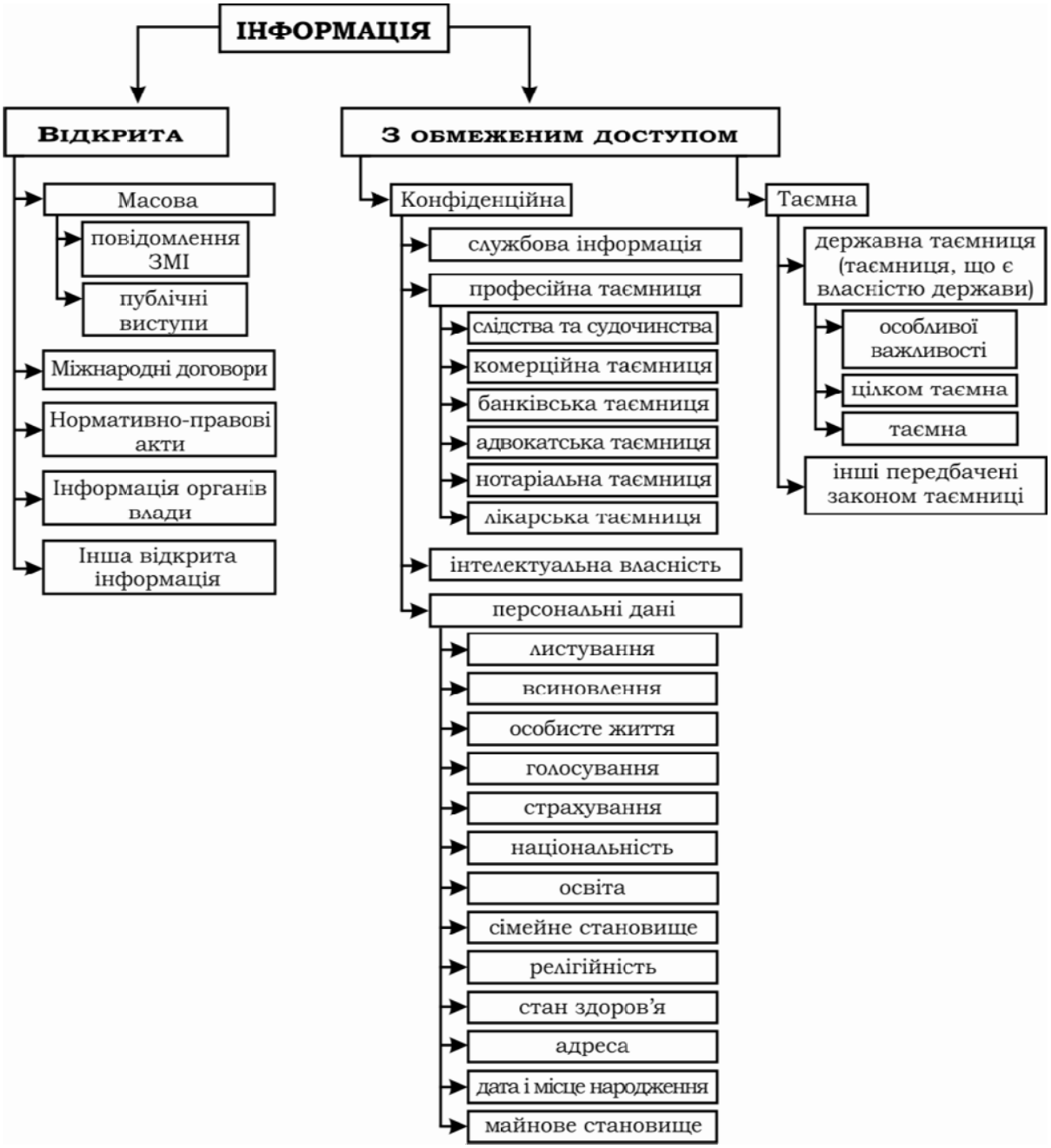

Рис. 1-1. Класифікація інформації за режимом доступу до неї

Отже, режим доступу є однією з головних юридичних характеристик інформації, якою визначаються конкретні групи правових норм, що застосовуються до тієї чи іншої документованої або публічно виголошеної інформації.

Правові режими існують у рамках багатьох галузей права, а оскільки захист інформації в цілях інформаційної безпеки відбувається на основі імперативного методу правового регулювання, то відповідні режими доступу до інформації

за своїми характеристиками є найбільш близькими до адміністративно-правових режимів.

РОЗДІЛ 2. БЕЗПЕКОЗНАВСТВО – СТРАТЕГІЧНИЙ РЕСУРС РОЗВИТКУ СУСПІЛЬСТВА ЗНАНЬ

2.1. Національна безпека: поняття, сутність, характеристика

2.1.1. Безпекознавство

Безпека звичайно пов'язується зі станом нормального функціонування суспільних інститутів та інших форм соціальної діяльності, зі станом захищеності об'єкта (системи) від зовнішніх та внутрішніх негативних впливів, загроз, небезпек тощо. При цьому основними об'єктами, на які направлені заходи із забезпечення безпеки, тобто, передусім, захисні заходи, є людина і громадянин, суспільство і держава.

У наш час небезпека є об'єктивною і очевидною субстанцією, що має місце в реальній дійсності. Прагнення людини убезпечитися від загрожуючих чинників, явищ і процесів є природним і надзвичайно актуальним. Безпека, тобто стан захищеності життєво важливих інтересів громадянина, суспільства, держави, людства і цивілізації від небезпек, – це одна з найважливіших цінностей соціального буття людей, обов'язкова передумова існування і подальшого розвитку людства. Безпека повинна створювати гармонію і переборювати протиріччя у відносинах «людина – техніка», «техніка – техніка», «людина – навколишнє середовище», у взаєминах між людьми, особою і державою, націями і державами.

Усі соціальні науки, у тому числі філософія, соціологія, культурологія, політологія, правознавство тощо, розробляючи проблеми гуманної безпеки або забезпечення безпеки людини, держави, народів, повинні спиратися у своїх дослідженнях на загальнонаукову категорію «безпека». Це поняття має світоглядно-філософську методологічну функцію, тому що виступає як концептуальна ідея, інновація, «ноу-хау» для пояснення тих чи інших конкретних процесів і явищ соціальної реальності та побудови окремих теоретичних і праксеологічних моделей, котрі описують певні суспільні моделі в суспільстві та реалізують в практичній діяльності.

2.1.2. Категорія «безпека» у правознавстві

Категорію «безпека» у правознавстві (правову безпеку) доцільно трактувати як суспільну безпеку безвідносно до того, чи забезпечує безпека захист публічного або приватного права. Право може розглядатися в системі управління як засіб (інструмент) забезпечення безпеки (безпечного існування) особистості, суспільства і держави, тобто застосовується нормативно-інструментальний підхід у тлумаченні співвідношення категорій «суспільна безпека» і «правова безпека». Правову безпеку потрібно розглядати як фундаментальну категорію: категорія «суспільна безпека» важлива для розуміння права і багато в чому визначає його сутність та основні риси, значною мірою впливає на зміст і сутність праворозуміння, нормотворчості та правозастосування. Правову безпеку варто розглядати як загальну людську цінність, оскільки вона є однією з постійних потреб, яка детермінована природними умовами життя людини, суспільства, людства, а також як суспільне благо, котре покликане забезпечити існування інших благ.

Вплив суспільної безпеки на форму та зміст права повинен знаходити найбільш повне відображення у правотворчості, котра передбачає:

– високу якість нормативних актів правових систем, що виявляється у високому рівні техніки нормотворчості, однозначності, простоті та єдності термінології;

– логічність, чіткість та доступність текстів законів та нормативних актів, що виключає неоднозначне їх тлумачення; зведення до мінімуму оціночних компонентів права (оціночних термінів);

– виключення неясності і розпливчатості правових приписів.

Розглядаючи фактор безпеки у сучасній політиці Української держави, важливо окреслити значення відповідних термінів, більшість з яких охарактеризовані у чинній Конституції України: визначення поняття екологічної безпеки, економічної, інформаційної та державної безпеки, інтересів національної безпеки (ст. 32, 34, 36, 39), забезпечення національної безпеки (ст. 44), основ національної безпеки (ст. 92), національної безпеки, сфери національної безпе-

ки, небезпеки (ст. 106), особистої безпеки (ст. 126), громадської безпеки (ст. 138).

2.1.3. НАЦІОНАЛЬНА БЕЗПЕКА

У сучасній світоглядно-філософській думці існують два основні підходи до розуміння поняття «національна безпека». Фундатором першого, реалістичного підходу до розуміння даного поняття, є американський фахівець у галузі політичних наук Г. Моргентау, який визначив національну безпеку як недоторканність території та інститутів держави, зробивши наголос на воєнну і політичну безпеку, що складає традиційне розуміння. Другий підхід – *Human Security* – розвивався в межах ідеалістичної теорії міжнародних відносин і позначався аналізом воєнних, політичних, економічних, соціальних, гуманітарних, екологічних проблем.[26]

Український законодавець, виходячи з другого підходу, за роки державної незалежності сформував потужну правову базу політики національної безпеки, основою для якої є чинна Конституція України. Зокрема, в ст. 3 Конституції України сформульовано концептуальні засади забезпечення безпеки людини: «людина, її життя і здоров'я, честь і гідність, недоторканість і безпека визначаються в Україні найвищою цінністю». А в ст. 17 чітко передбачено, що: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу».

Правові засади національної безпеки України містяться в Законі України «Про основи національної безпеки України» від 19 червня 2003 р. № 964-IV, якими визначено понятійний апарат у сфері національної безпеки.

Основними категоріями, які становлять зміст національної безпеки, є: «національна безпека»; «національні інтереси»; «об'єкти національної безпеки»; «суб'єкти національної безпеки»; «принципи національної безпеки»; «функції національної безпеки»; «система (складові) національної безпеки»; «загрози, ризики і небезпеки національній безпеці»; «характеристика національної

[26] Блюменау Д. И. Информация: миф или реальность? (О состоянии понятий «знание» и «социальная информация») / Д. И. Блюменау // НТИ. Сер. 2. – 1985. – № 2. – С. 1–4.

безпеки»; «фактори забезпечення національної безпеки»; «форми, засоби, методи та технології забезпечення національної безпеки» та ін.

Національна безпека – це 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 у сферах правоохоронної діяльності, запобігання і протидії корупції, прикордонної діяльності та оборони, міграційної політики, охорони здоров'я, освіти та науки, науково-технічної та інноваційної політики, культурного розвитку населення, забезпечення свободи слова та інформаційної безпеки, соціальної політики та пенсійного забезпечення, житлово-комунального господарства, ринку фінансових послуг, захисту прав власності, фондових ринків і обігу цінних паперів, податково-бюджетної та митної політики, торгівлі та підприємницької діяльності, ринку банківських послуг, інвестиційної та інноваційної політики, ревізійної діяльності, монетарної та валютної політики, захисту інформації, ліцензування, промисловості та сільського господарства, транспорту та зв'язку, інформаційних цифрових технологій, енергетики та енергозбереження, функціонування природних монополій, використання надр, земельних та водних ресурсів, корисних копалин, захисту екології і навколишнього природного середовища та в інших сферах державного управління при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам.

Об'єктами національної безпеки є: людина і громадянин – їхні конституційні права і свободи та обов'язки; суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси; держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність (див. рис. 1).

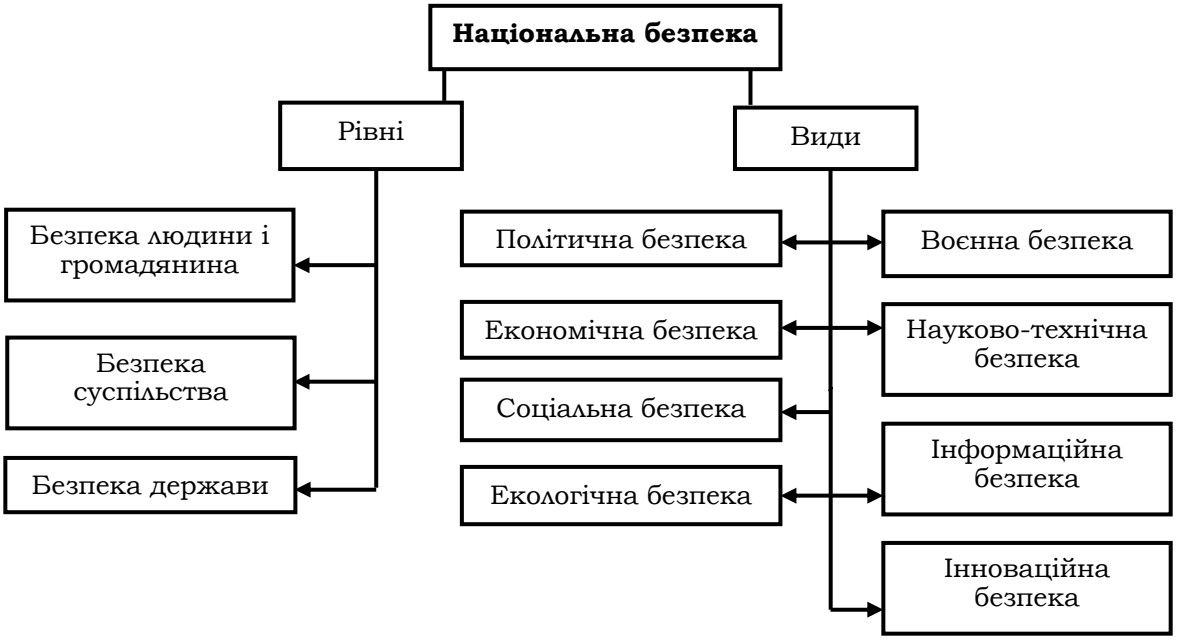

Рис. 1. Рівні та види національної безпеки

Основними ***принципами*** забезпечення національної безпеки є:

– пріоритет прав та свобод і обов'язків людини і громадянина;

– верховенство права;

– пріоритет договірних (мирних) засобів у розв'язанні конфліктів;

– своєчасність і адекватність заходів захисту національних інтересів реальним і потенційним загрозам, ризикам і небезпекам;

– чітке розмежування повноважень та взаємодія органів державної влади в забезпеченні національної безпеки;

– демократичний цивільний контроль над Воєнною організацією держави та іншими структурами в системі національної безпеки;

– використання в інтересах України міждержавних систем та механізмів міжнародної колективної безпеки.

Система національної безпеки – множина потреб, інтересів і цінностей особи, суспільства, держави, загроз та небезпек, внутрішніх і зовнішніх, об`єктивних і суб`єктивних, природних, техногенних та антропогенних чинників, що впливають на стан національної безпеки, умови їх виникнення та розвитку, а також державні та недержавні інституції, об'єднані цілями і завданнями щодо просування потреб нації, національних інтересів і цінностей, які взаємо-

діють один з одним і здійснюють відповідну діяльність у межах законодавства України.

Елементами системи національної безпеки є:

– національна ідея та загальна парадигма національної безпеки, на яких базуються світоглядні аспекти, методологічні засади та ідеологія національної безпеки, яка виражається в концепції, доктрині та стратегії національної безпеки; об'єкти, суб'єкти і предмет національної безпеки в конкретній сфері національної безпеки;

– національна ідентичність, національні цінності, національні інтереси та цілі; система забезпечення національної безпеки та її потенціал (сили і засоби), за допомогою якого можлива матеріалізація державно-управлінських впливів системи державного управління національною безпекою на відповідні суспільні відносини; політична, економічна, соціальна, інформаційна, інноваційна, військова, міжнародна, науково-технологічна та екологічна підсистема системи національної безпеки;

– множина зовнішніх і внутрішніх факторів національної безпеки;

– реальні та потенційні, нормативні і не визначені в законодавстві виклики, ризики, загрози й небезпеки національній безпеці та їх джерела в кожній конкретній сфері;

– масив чинного законодавства, принципи та концептуальні підходи щодо забезпечення національної безпеки;

– світоглядно-філософські, правові, організаційно-управлінські та морально-етичні відносини у сфері національної безпеки.

Атрибутивними рисами національної безпеки, які характеризують її як систему, є незалежність, стійкість і стабільність та здатність до удосконалення саморозвитку і прогресу. Антиподом системи національної безпеки є система дестабілізації національної безпеки, діяльність якої може призвести до деструктивних дій, а то і загибелі нації та держави, або слугувати стимулом їх розвитку та самовдосконалення.

Принципова різниця між цими двома визначеннями полягає у різних рівнях співпраці, партнерства, взаємодії по лінії «людина – громадянин – суспільство – держава».

Правовою основою функціонування системи національної безпеки України є «Загальна декларація прав людини», Конституція України, закони України «Про Раду національної безпеки», «Про основні засади забезпечення кібербезпеки України» інші нормативно-правові акти, а також визнані Україною міжнародні конвенції, договори та угоди. Передусім наголосимо на законах України «Про основи національної безпеки України», «Про Раду національної безпеки і оборони України», «Про поліцію», «Про внутрішні війська МВС України», «Про Службу безпеки України», «Про контррозвідувальну діяльність», «Про розвідувальні органи України», «Про державну прикордонну службу України», «Про державний кордон України», «Про державну митну службу України», «Про збройні Сили України», «Про оборону України», «Про Військову службу правопорядку в Збройних Силах України», «Про державну охорону органів державної влади України та посадових осіб», «Про війська Цивільної оборони України», «Про Цивільну оборону України», «Про надзвичайний стан», «Про правовий режим воєнного стану», «Про дипломатичну службу», «Про прокуратуру», «Про судоустрій України», «Про пожежну безпеку», «Про боротьбу з тероризмом», «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом», «Про державну таємницю», «Про недержавне забезпечення національної безпеки України», «Про приватну детективну та охоронну діяльність», Кримінальний, Кримінально-процесуальний, Цивільний, Цивільно-процесуальний, Митний, Бюджетний, Господарський кодекси України тощо, які безпосередньо стосуються регулювання відносин у сфері національної безпеки.

Загрози національній безпеці – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим інтересам України.

Пріоритетами національних інтересів України є:

– гарантування конституційних прав та свобод людини і громадянина;

– розвиток громадянського суспільства, його демократичних інститутів;

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

– зміцнення політичної і соціальної стабільності в суспільстві;

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

– створення конкурентоспроможної, соціально орієнтованої ринкової економіки та забезпечення постійного зростання рівня життя і добробуту населення;

– збереження та зміцнення науково-технологічного потенціалу, утвердження інноваційної моделі розвитку;

– забезпечення екологічно та техногенно безпечних умов життєдіяльності громадян і суспільства, збереження навколишнього природного середовища та раціональне використання природних ресурсів;

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

– інтеграція України у європейський політичний, економічний, правовий простір; розвиток рівноправних взаємовигідних партнерських відносин з іншими державами світу в інтересах України.

Отже, визначені засоби і шляхи забезпечення національної безпеки держави ґрунтуються на засадах демократичної, правової, соціальної держави.

Сучасний рівень розвитку світоглядно-філософської та соціально-політичної думки виділяє такі основні положення щодо забезпечення національної безпеки:

– верховенство права, законність і дотримання балансу інтересів громадянина, суспільства і держави;

– взаємна гармонійна відповідальність громадянина, суспільства і держави за забезпечення національної безпеки;

– взаємозв'язок національної та міжнародної безпеки.

Реалізація вказаних положень можлива за рахунок створення потужної системи безпеки, основними функціями якої є:

– виявлення, моніторинг і прогнозування внутрішніх і зовнішніх загроз життєво важливим інтересам об'єктів національної безпеки;

– здійснення комплексу дієвих оперативних і довгочасних заходів щодо попередження загроз та їх ефективної і своєчасної нейтралізації;

– створення і підтримання в постійній готовності сил і засобів забезпечення національної безпеки в повсякденних типових умовах або при надзвичайних ситуаціях;

– участь у заходах із забезпечення безпеки за межами держави згідно з міжнародними конвенціями, договорами і угодами.

Оскільки національна безпека є комплексною системою, то вона має свої чисельні підсистеми, елементи, складові. До основних елементів національної безпеки можна віднести політичну, економічну, воєнну, соціальну, екологічну, інноваційну, науково-технологічну, інформаційну безпеку (див. рис. 1).

Політична безпека є одним із центральних елементів системи національної безпеки. Будь-які обмеження можливостей держави як самостійного, суверенного і активного суб'єкта міжнародних відносин з боку її сусідів або коаліції держав призводять до обмеження її суверенітету, до політичної залежності і не можуть не мати негативного впливу на її функціонування і розвиток і в результаті не приносити збитків державі.

Основними напрямами державної політики з питань національної безпеки України є:

1) у зовнішньополітичній сфері:

– створення сприятливих зовнішньополітичних умов для прогресивного економічного і соціального розвитку України;

– запобігання втручанню у внутрішні справи України і відвернення посягань на її державний суверенітет і територіальну цілісність з боку інших держав;

– забезпечення повноправної участі України в загальноєвропейській та регіональних системах колективної безпеки, набуття членства у Європейському Союзі при збереженні добросусідських відносин і стратегічного партнерства з іншими державами світового співтовариства;

– сприяння усуненню конфліктів, насамперед у регіонах, що межують з Україною;

– участь у міжнародній миротворчій діяльності під егідою ООН, ОБСЄ, інших міжнародних організацій у сфері безпеки;

– участь у заходах щодо боротьби з міжнародними організованими злочинними угрупованнями та міжнародним тероризмом, протидія поширенню ядерної та іншої зброї масового ураження і засобів її доставки;

– адаптація чинного законодавства України до законодавства Європейського Союзу;

2) у сфері державної безпеки:

– реформування судової і правоохоронної системи з метою підвищення ефективності її діяльності на основі оптимізації структури, підвищення рівня координації діяльності судових і правоохоронних органів, покращення їх фінансового, матеріально-технічного, організаційно-правового і кадрового забезпечення;

– зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби з організованою злочинністю та наркобізнесом, кібертероризмом і кіберзлочинністю;

– участь України в міжнародному співробітництві у сфері боротьби з міжнародною транскордонною, транснаціональною, трансконтинентальною, планетарною злочинністю, тероризмом, кібертероризмом, ядерним тероризмом, наркобізнесом, нелегальною міграцією;

– відпрацювання ефективно діючої системи контролю за поставками продукції і технологій оборонного призначення і подвійного використання;

3) у внутрішньополітичній сфері:

– забезпечення неухильного додержання конституційних прав і свобод та обов'язків людини і громадянина, захист конституційного устрою, удосконалення системи політичної влади з метою зміцнення демократії, духовних та моральних підвалин суспільства; підвищення ефективності функціонування політичних інститутів влади;

– створення дієвих, у тому числі судових, механізмів захисту конституційних прав і основних свобод та обов'язків людини;

– забезпечення політичної стабільності, громадянського миру та взаєморозуміння в суспільстві, запобігання проявам екстремізму;

– забезпечення прозорості в діяльності державних органів, прийнятті ефективних управлінських рішень, інформованості населення, зміцнення на цій основі його довіри до владних інститутів;

– створення повноцінного, ефективно діючого місцевого і регіонального самоврядування;

– формування і вдосконалення політико-правових, соціально-економічних та духовно-культурних засад етнонаціональної стабільності, відпрацювання ефективних механізмів узгодження інтересів етнічних спільнот та розв'язання міжнаціональних конфліктних ситуацій та суперечностей;

– забезпечення міжконфесійної стабільності та запобігання конфліктним загостренням на релігійній основі, недопущення протистояння різних конфесій, церков, у тому числі щодо розподілу сфер впливу на території України.

Економічна безпека полягає у спроможності держави створювати необхідні матеріальні передумови для всебічного розвитку суспільства, виступити самостійним і рівноправним суб'єктом системи мікрогосподарських зв'язків.

Економічна безпека передбачає:

– забезпечення умов для сталого економічного зростання і підвищення конкурентоспроможності національної економіки;

– прискорення прогресивних структурних та інституціональних змін в економіці, поліпшення інвестиційного клімату, підвищення ефективності інвестиційних процесів;

– стимулювання випереджувального розвитку наукоємних високотехнологічних виробництв;

– удосконалення антимонопольної політики; створення ефективного механізму державного регулювання природних монополій;

– подолання «тінізації» економіки через реформування податкової і фіскальної системи, оздоровлення фінансово-кредитної сфери та припинення відпливу капіталів за кордон, зменшення позабанківського обігу грошової маси;

– забезпечення збалансованого розвитку бюджетної сфери, внутрішньої і зовнішньої захищеності національної валюти, її стабільності, захисту інтересів вкладників, фінансового ринку;

– здійснення виваженої світоглядної політики внутрішніх та зовнішніх запозичень;

– забезпечення енергетичної безпеки на основі сталого функціонування і розвитку паливно-енергетичного комплексу, у тому числі послідовного і активного проведення політики енергозбереження та диверсифікації джерел енергозабезпечення;

– забезпечення продовольчої безпеки;

– захист внутрішнього ринку від недоброякісного імпорту – поставок продукції, яка може завдавати шкоди національним виробникам, здоров'ю людей та навколишньому природному середовищу;

– посилення участі України в міжнародному поділі праці, розвиток експортного потенціалу високотехнологічної продукції, поглиблення інтеграції у європейську і світову економічну систему та активізація участі в міжнародних економічних і фінансових організаціях.

Воєнна безпека і безпека державного кордону України є основними компонентами, що характеризують зовнішній аспект національної безпеки держави, забезпечувати яку покликані збройні сили.

Забезпечення воєнної безпеки держави передбачає:

– прискорення реформування Збройних сил України та інших військових формувань з метою забезпечення їх максимальної ефективності та здатності давати адекватну відповідь реальним та потенційним загрозам Україні; перехід до комплектування Збройних сил України на контрактній основі;

– здійснення державних програм модернізації наявних, розроблення та впровадження новітніх зразків бойової техніки та озброєнь;

– посилення контролю за станом озброєнь і захищеністю військових об'єктів; активізація робіт з утилізації зброї;

– впровадження системи демократичного цивільного контролю над Воєнною організацією[27] та правоохоронними органами держави[28];

– забезпечення соціального захисту військовослужбовців та членів їх сімей;

– прискорення процесу делімітації та демаркації кордонів України;

– боротьба з організованими злочинними угрупованнями, у тому числі міжнародними, які намагаються діяти через державний кордон України, у пунктах пропуску та виключній (морській) економічній зоні України;

– поглиблення транскордонного співробітництва з суміжними державами.

Соціальна безпека базується на психічному і психологічному стані населення держави і залежить від інших видів безпеки (економічної, політичної, інформаційної тощо) та чинників (наявність безробітних, багатодітних родин, кримінальних угруповань, судових і правоохоронних органів тощо).

Забезпечення безпеки в соціальній та гуманітарній сферах включає наступні основні напрями:

– істотне посилення соціальної складової економічної політики, реальне підвищення життєвого рівня населення, передусім на основі піднесення вартості оплати праці, своєчасної виплати заробітної плати та гарантованих законом соці-

[27] Воєнна організація держави – сукупність органів державної влади, військових формувань, утворених відповідно до законів України, діяльність яких перебуває під демократичним цивільним контролем з боку суспільства і безпосередньо спрямована на захист національних інтересів України від зовнішніх та внутрішніх загроз.

[28] Правоохоронні органи – органи державної влади, на які Конституцією і законами України покладено здійснення правоохоронних функцій.

альних виплат, посилення цільової спрямованості матеріальної підтримки, зниження рівня безробіття;

– створення умов для подолання бідності і надмірного майнового розшарування в суспільстві;

– збереження та зміцнення демографічного і трудоресурсного потенціалу країни; подолання кризових демографічних процесів;

– створення ефективної системи соціального захисту людини, охорони та відновлення її фізичного і духовного здоров'я, ліквідації алкоголізму, наркоманії, інших негативних явищ;

– ліквідація бездоглядності, безпритульності та бродяжництва серед дітей і підлітків.

Екологічна безпека – це стан гармонійного розвитку системи «природа – техніка – людина», який забезпечує взаємодію природних, технічних та соціальних систем при збереженні природно-ресурсного та екологічного потенціалу природних систем і здатності біосфери до саморегулювання та самозбереження.

Безпека в екологічній сфері передбачає:

– здійснення комплексу заходів, які гарантують екологічну безпеку ядерних об'єктів і надійний радіаційний захист населення та довкілля, зведення до мінімуму впливу наслідків аварії на Чорнобильській АЕС;

– впровадження у виробництво сучасних, екологічно безпечних, ресурсо- та енергозберігаючих технологій, підвищення ефективності використання природних ресурсів, розвиток технологій перероблення та утилізації відходів;

– поліпшення екологічного стану річок України, насамперед басейну р. Дніпро, та якості питної води;

– запобігання забрудненню Чорного та Азовського морів та поліпшення їх екологічного стану;

– стабілізація та поліпшення екологічного стану в містах і промислових центрах Донецько-Придніпровського регіону;

– недопущення неконтрольованого ввезення в Україну екологічно небезпечних технологій, речовин і матеріалів, збудників хвороб, небезпечних для людей, тварин, рослин, організмів;

– реалізація заходів щодо зменшення негативного впливу глобальних екологічних проблем на стан екологічної безпеки України, розширення її участі в міжнародному співробітництві з цих питань.

Науково-технологічна безпека визначається станом фундаментальних, пошукових і прикладних досліджень для забезпечення стабільного розвитку науково-технічного, технологічного і соціально-економічного потенціалу держави на світовому рівні.

Забезпечення безпеки в науково-технологічній сфері передбачає:

– посилення державної підтримки розвитку пріоритетних напрямів науки і техніки як основи створення високих технологій та забезпечення переходу економіки на інноваційну модель розвитку, створення ефективної системи інноваційної діяльності в Україні;

– поетапне збільшення обсягів бюджетних видатків на розвиток освіти і науки, створення умов для широкого залучення в науково-технічну сферу позабюджетних асигнувань;

– створення економічних і суспільно-політичних умов для підвищення соціального статусу наукової та технічної інтелігенції;

– забезпечення необхідних умов для реалізації прав інтелектуальної власності;

– забезпечення належного рівня безпеки експлуатації промислових, сільськогосподарських і військових об’єктів, споруд та інженерних мереж.

Безпека інформаційної сфери – ужиття комплексних заходів щодо захисту свого інформаційного простору та входження України у світовий інформаційний простір.

Безпека в інформаційній сфері передбачає:

– забезпечення інформаційного суверенітету України;

– удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

– активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;

– забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

– вживання комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

2.1.4. Державна безпека

Даючи визначення держави, як правило, цитують Конвенцію про права і обов'язки держав, яка прийнята на VII Міжнародній конференції американських країн у 1933 році в Монтевідео, в якій йдеться мова про права і обов'язки держав: держава, будучи представником міжнародного права, має право видавати свої закони, управляти, визначати юрисдикцію й компетентність власних служб і організацій та закони, що прийняті в цій державі, є обов'язковими для всіх, хто мешкає на території цієї держави[29].

Уперше поняття «*державна безпека*» на теренах України згадується в ухваленому в серпні 1881 р. Височайше затвердженому Положенні про заходи щодо охорони державного порядку та громадського спокою. При цьому поняття трактувалося як рівноправне з терміном «суспільна безпека».[30]

[29] Туском Жан. Міжнародне право: Підручник. Пер. з франц. – К.: «АртЕк», 1998. – 416 с.

[30] Собрание указов 1881 г., 9 сент., ст. 646 / Полное собрание законов Российской империи : собрание третье, т. 1 со дня восшествия на престол государя императора Александра Александровича по 31 дек. 1881 г. от № 1–385 и дополнения. – СПб., 1885. – С. 261. При цьому поняття трактувалося як рівноправне з терміном «суспільна безпека».

Держава характеризується об'єктивно притаманною їй політико-юридичною властивістю – суверенітетом і «кожна держава зобов'язана поважати суверенітет інших учасників системи, тобто їхнє право в межах власної території здійснювати законодавчу, виконавчу, адміністративну й судову владу без будь-якого втручання з боку інших держав»[31].

Сьогодні поняття «державна безпека», «національна безпека», «національні інтереси», «загрози національній безпеці» і «забезпечення державної безпеки» визначаються в Конституції України (ст. 17), законах «Про основи національної безпеки України» (статті 7, 8), «Про Службу безпеки України» (ст. 24), «Про основні засади забезпечення кібербезпеки України» (статті 1,3,4,6,8).

За результатами досліджень сектора безпеки України, що здійснювалися у 2005–2007 рр. Службою безпеки України, було запропоновано такі визначення понятійно-категоріального апарату у сфері державної безпеки:

Державна безпека – це захищеність державного суверенітету, конституційного ладу, територіальної цілісності і недоторканності, економічного, науково-технічного і оборонного потенціалу, інформаційної сфери та державної таємниці від зовнішніх і внутрішніх загроз, а також розвідувальних, терористичних та інших протиправних посягань спеціальних служб іноземних держав, організацій, окремих груп та осіб.

Забезпечення державної безпеки – спеціальний вид діяльності у сфері національної безпеки, яка здійснюється системою державних органів та військових формувань з використанням комплексу правових, організаційних, режимних, контррозвідувальних, оперативно-розшукових, службово-бойових та військових заходів, спрямованих на захист об'єктів державної безпеки.

Об'єкти державної безпеки – державний суверенітет, конституційний лад, територіальна цілісність, економічний та оборонний потенціал, інформаційна сфера та державна таємниця, які обумовлені існуванням держави.

Суб'єкти забезпечення державної безпеки – державні органи та військові формування, які забезпечують або обумовлюють існування держави.

[31] Международное право: Учебник / Отв.ред. Ю.М. Колосов, В.И. Кузнецов. (Диплом. акад. МИД РФ, МГИ МО МИД РФ). – М.: Международные отношения, 1996. – 608 с.

Безпека завжди пов’язана з певними обмеженнями динаміки системи, зниженням її ступенів свободи в навколишньому середовищі. Це обумовлено тим, що збереження системи безпеки гарантується її певним інформаційно-комунікаційним змістом.

Для забезпечення безпеки в суспільстві створюються відповідні органи, служби та інші засоби забезпечення національної безпеки, передусім органи законодавчої, виконавчої та судової влад, силові структури і спецслужби тощо (див. рис. 2).

Головним суб’єктом забезпечення державної безпеки є Служба безпеки України. На неї покладається в межах визначеної чинним законодавством компетенції щодо захисту державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного, інтелектуального і оборонного потенціалу України, законних інтересів держави та прав і обов’язків громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці.

До завдань Служби безпеки України також входить попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності у сфері управління і економіки та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України.

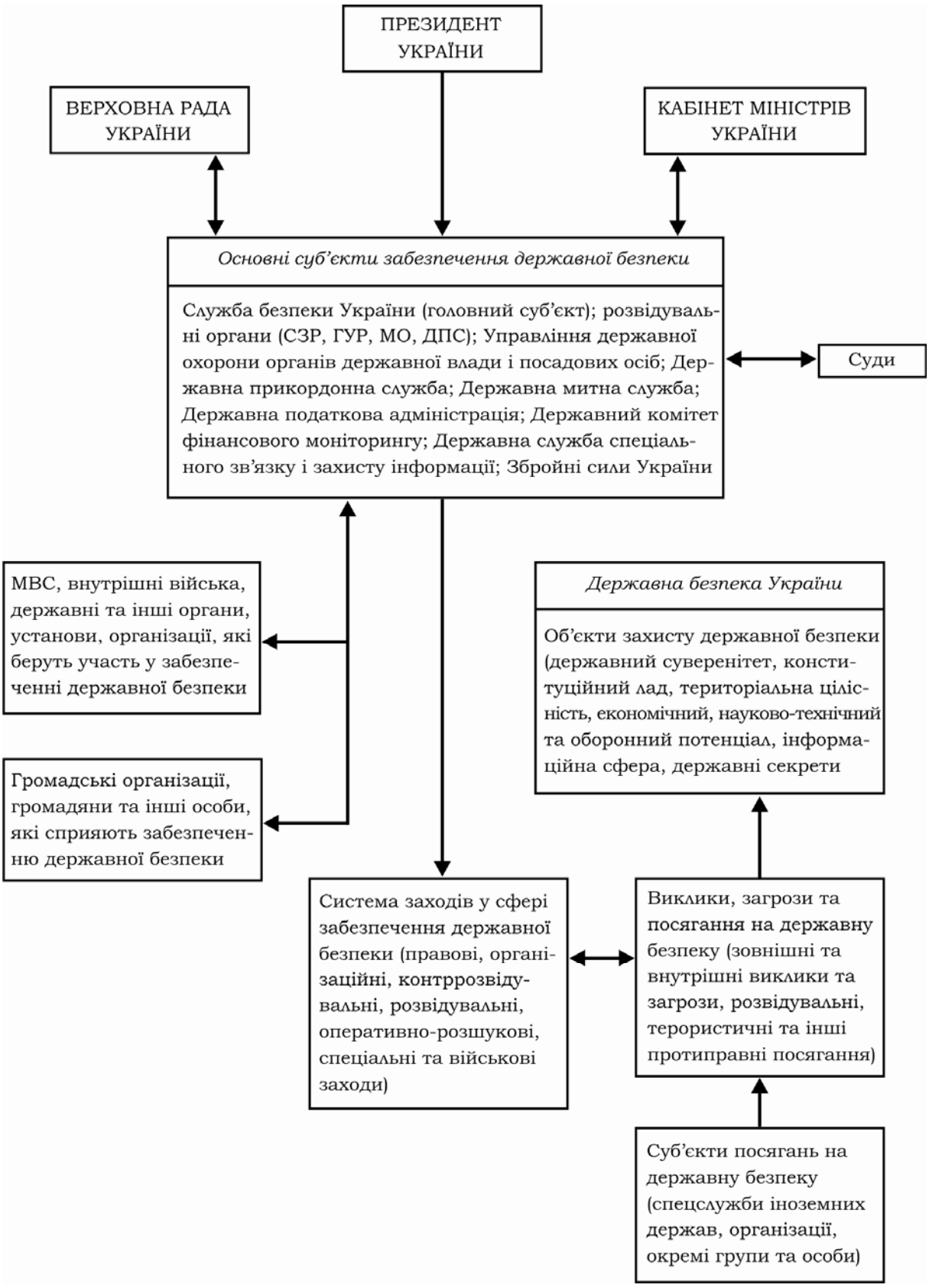

Рис. 2. Система забезпечення державної безпеки України

2.2. Інформаційна безпека як визначальний компонент національної безпеки

2.2.1. Концептуальні засади інформаційної безпеки

Процеси, що відбуваються в суспільному житті, можна охарактеризувати як посилення ролі та значення інформації як у суспільстві в цілому, так і в житті кожної окремої людини зокрема. Інформація отримує реальне матеріально-енергетичне, соціально-економічне, політичне і вартісне вираження. За цих умов одним з першочергових завдань, що постають перед правовою державою, є вирішення протиріччя між реально існуючими і зростаючими потребами особистості, суспільства і держави в якісних інформаційних ресурсах, продуктах та послугах і необхідністю забезпечення їх інформаційної безпеки. Політика у сфері інформаційної безпеки спрямована на досягнення такого рівня духовного та інтелектуального потенціалів країн, який є достатнім для розвитку державності і соціального прогресу.

Визнання проблеми інформаційної безпеки на міжнародному рівні обумовлюється такими чинниками глобалізації:

– у більшості розвинутих країн проводяться дослідження і розроблення нової інформаційної зброї, що дозволяє здійснювати безпосередній контроль над інформаційними ресурсами потенційного противника, а в необхідних випадках впливати на них[32];

– кардинально змінилася оцінка доктрини інформаційної безпеки в цілому і позиції більшості країн світу, які усвідомили потенціал інформаційних загроз і необхідність створення відповідного міжнародного механізму для контролю інформаційного протиборства.

[32] За даними аналітичних центрів США, розроблення такої зброї ведуться в 120 країнах світу. Для порівняння: розроблення в галузі ядерної зброї проводяться не більше ніж у 20 країнах. У деяких країнах завершено розробку засобів інформаційного протиборства (війни) з можливим противником як в умовах воєнних конфліктів різної інтенсивності, так і в мирний час на стратегічному, оперативному, тактичному рівнях та в польових умовах з метою захисту національної інформаційної сфери від агресії і несанкціонованого втручання; у розвинутих країнах концепція інформаційної війни є складовою воєнної доктрини, що обумовлює спеціальну підготовку особового складу і окремих підрозділів для проведення інформаційних операцій; практика міжнародних, регіональних та етнічних конфліктів виявила унікальність застосування інформаційної зброї для впливу на міжнародне співтовариство та для боротьби за геополітичні інтереси. (Міжнародна інформаційна безпеки: Сучасні виклики та загрози. – К.: Центр вільної преси, 2006. – С. 15).

Політичні дискусії на Міжнародному семінарі з проблем інформаційної безпеки (Женева, 1999 р.), який відбувся під егідою Інституту ООН з дослідження проблем роззброєння (*UNIDIR – United Nations institute for disarmament research*) за участю департаменту з питань роззброєння Секретаріату ООН та представників понад 50 країн світу, підтвердили актуальність проблеми та своєчасність її розгляду в рамках ООН. У визначенні підходів до її вирішення виявилися різні позиції, котрі відповідали стратегічним інтересам учасників дискусії. Позиція розвинутих країн передбачала визнання проблеми міжнародної інформаційної безпеки як:

– гіпотетичного силового протистояння;

– перенесення концепції міжнародної інформаційної безпеки на регіональний або тематичний рівень;

– виділення з комплексної проблеми міжнародної інформаційної безпеки таких складових, як кримінальні та терористичні міжнародні інформаційні загрози і створення міжнародного механізму контролю подібних інформаційних злочинів.

Позиція країн, які не належать до західної моделі цивілізації, передбачала такі пропозиції:

– встановлення міжнародно-правової норми про заборону застосування засобів впливу на інформаційні ресурси та інформаційний потенціал міжнародного, регіонального та національного призначення;

– створення спеціального Міжнародного суду з інформаційної злочинності;

– спільне розроблення технології глобального захисту від інформаційної агресії.

У Заяві міжнародної зустрічі було проголошено про узгодження Програми дій з попередження інформаційних війн та обмеження гонки інформаційних озброєнь.

Женевська зустріч виявила стратегічну проблему міжнародної інформаційної безпеки – проблему домінування в глобальній інформаційній сфері із застосуванням інформаційних озброєнь, тобто прагнення до контролю значних терито-

рій та соціумів, проблему інформаційного дисбалансу сил міжнародного світопорядку.

Концепція міжнародної інформаційної безпеки визначає критичні структури, які у першу чергу зазнають впливу в умовах інформаційного протиборства. Найбільш вразливими вважаються політична, суспільна, економічна, військова, науково-технологічна, духовна сфери життєдіяльності суспільства, а саме:

– у політичній сфері інформаційна безпека стосується всіх елементів політичної структури держави та суспільства: структур підготовки та прийняття політичних рішень, структур управління місцевої та регіональної влади, структур виборчих систем, інформаційно-телекомунікаційних урядових систем спеціального призначення;

– для економічної сфери критичними вважаються системи загальноекономічного аналізу та прогнозування економічного розвитку, структури прийняття рішень та координації управлінських дій в економічній сфері, зокрема, в умовах надзвичайного стану, інфраструктури банківських мереж і систем, системи управління в критично важливих для функціонування держави структурах (енергетика, транспортні комунікації, телекомунікаційні та інформаційні мережі);

– у військовій сфері вразливими в умовах інформаційного протиборства вважаються інформаційні ресурси збройних сил, військово-промисловий комплекс, системи управління військами, системи контролю і постійного спостереження, канали надходження інформації стратегічного, оперативного, тактичного, розвідувального характеру;

– глобальними загрозами в науково-технологічній сфері є феномен транскордонного переміщення інтелектуальних ресурсів, тобто вивезення інформації унікального науково-технологічного характеру на біологічних носіях до міжнародних систем спостереження, аналізу і прогнозування тенденцій науково-технологічного розвитку в різних країнах з метою доступу до об’єктів критичної інфраструктури, до конфіденційних баз і банків даних; критичними для без-

пеки у сфері науки і технологій є структури накопичення науково-технічної інформації, інструкції та структури фундаментальних і прикладних досліджень, об'єкти інтелектуальної власності, ноу-хау;

– суспільна сфера є найбільш вразливою для інформаційних впливів, оскільки включає системи формування громадської думки, структури засобів масової комунікації, інформаційно-організаційні структури політичних партій, громадських рухів, національно-культурних та релігійних інституцій, структури забезпечення основних прав і свобод, плюралізму і незалежності виявлення поглядів, вільного обміну думками, ідеями та інформацією;

– духовна сфера стає критичною в умовах конфесійного протистояння, релігійного фанатизму, трансформації духовних ідеалів та морально-етичних цінностей. Так, проявом критичності духовної сфери (Ірландія, Алжир, Ізраїль, Афганістан, Китай, Іран) на міжнародному рівні стала проблема, пов'язана з рішенням керівництва ісламського радикального руху «Талібан» (Афганістан) про руйнування неісламських релігійних пам'яток, що внесені до глобальної культурної спадщини і перебувають під охороною ЮНЕСКО.

2.2.2. Міжнародна інформаційна безпека як актуальна проблема сучасності

Інформація, як глобальне явище, утворює глобальні проблеми в міжнародній інформаційній сфері, складовим елементом якої є національна інформаційна сфера, яку кожна країна до останнього часу намагалася регулювати відповідно до своїх правових традицій, звичаїв та суспільної моралі.

Стає зрозуміло, що неможливо забезпечувати економічне зростання і розвиток, швидке і якісне виконання державою своїх функцій без широкого використання швидкозростаючих інформаційних засобів, методів і технологій. Як зазначається в Доповіді ЮНЕСКО «Інформаційні та комунікаційні технології в понятті розвиток: перспективи ЮНЕСКО», що інформаційні та комунікаційні технології дають можливість драматичним чином трансформувати, надавати людям новий вид засобам, для організації власного життя, взаємодії між собою, участі в різних сферах суспільного життя. Ці технології формують новітню ос-

нову для радикальної зміни від індустріальних до постіндустріальних визначень розвитку[33].

Інформаційна безпека як чинник міжнародних відносин, вплив якої має універсальний характер на поведінку багатьох акторів міжнародних відносин. До того ж трансформація самої сутності понять проблеми безпеки після закінчення «холодної війни» і розпаду біполярної міжнародної системи, потребує концептуального перегляду принципів функціонування міжнародних та національних інститутів, що відповідають за безпеку, а також врахування в нових доктринах інформаційної складової міжнародної безпеки[34]

Зважаючи на глобальність складових інформаційної безпеки, розвинуті країни світу розпочали реалізацію довгострокових державних програм, спрямованих на забезпечення захисту критично залежних від інформації структур.

У 1996 р. проблему міжнародної інформаційної безпеки було винесено на політичний та міжнародно-правовий рівень, зокрема:

– Концепцію міжнародної інформаційної безпеки було обговорено на міжнародній конференції з проблем становлення інформаційного суспільства та глобальної цивілізації (ПАР, 1996 р.);

– у спільному комюніке зустрічі на найвищому рівні США-Російська Федерація у 1997 р. було підкреслено загрозу створення інформаційної зброї і визнано наявність воєнної складової глобального процесу інформатизації;

– на 52-ій сесії Генеральної Асамблеї ООН прийнято Резолюцію 53/70 від 4 грудня 1998 р., в якій зазначалося, що міжнародна спільнота визнає проблему інформаційної безпеки як багатоаспектний стратегічний напрям взаємодії держав у світі. Було запропоновано ООН розглянути конкретну типологію інформаційних загроз, визначити критерії цієї проблеми, включаючи розробку міжнародних принципів безпеки глобальних інформаційних систем та внести пропозиції до комплексної доповіді Генерального секретаря ООН для створен-

[33] Федоров А.В. Информационная безопасность в мировом политическом / Федоров А.В. – М. : МГИМО-Университет, 2006. – 220 с.
[34] Міжнародна інформаційна безпека: Сучасні виклики та загрози. – К. : Центр вільної преси, 2006. – С. 9.

ня міжнародного механізму з протидії використанню інформаційних озброєнь та розпалюванню інформаційних війн[35].

Міжнародна інформаційна безпека визначається як взаємодія акторів міжнародних відносин з операцій підтримання сталого миру на основі захисту міжнародної інфосфери, глобальної інфраструктури та суспільної свідомості світової спільноти від реальних і потенційних інформаційних загроз[36].

Інформаційна безпека, як поняття в міжнародних відносинах залежно від його використання розглядається у декількох ракурсах. У найзагальнішому вигляді – інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави[37].

Інформаційна безпека включає в себе сукупність організаційних, соціально-економічних, правових заходів, спрямованих на забезпечення стабільності розвитку суспільства і держави та цивілізації.

Сьогодні Інтернет, як і будь-яка технічна система, потребує координації для зв'язкової роботи в глобальному масштабі. В Інтернеті є декілька технічних «позицій контролю». Це насамперед система доменних імен та і-адрес, вироблення параметрів інтернет-протоколів. Зараз контроль над простором імен і адрес Інтернету, а також координацію робіт з вироблення параметрів інтернет-протоколів здійснює приватна некомерційна організація ICANN (Internet Corporation for Assigned Names and Numbers), зареєстрована в штаті Каліфорнія і підкоряється законам США. Подібна ситуація не може не викликати заклопотаності у інших держав, що виступають за інтернаціоналізацію функцій ICANN і передачу їх Міжнародному союзу електрозв'язку, спеціалізованої організації «сім'ї ООН».

При цьому управління інтернетом включає в себе не тільки технічну координацію, а й більш широке коло питань, пов'язаних із захистом прав людини

[35] Міжнародна інформаційна безпека: Сучасні виклики та загрози. – К. : Центр вільної преси, 2006. – С. 13-14.
[36] Раймон А. Мемауры: 50 лет размышления о политике / Раймон А. Memoires: 50 Ands de Reflexion Politique ; пер. с фр. Г.А. Абрамова, Л.Г. Лариновой.– М. : Ладомир, 2002.– 873с.
[37] Юдін О.К. Інформаційна безпека держави : навч. посіб. / О.К.Юдін, В.М. Богуш. – Х. : Консум, 2005. – С. 38.

в інтернеті, захистом прав інтелектуальної власності, протидією злочинності та ін. Згідно з визначенням Робочої групи ООН з питань управління інтернетом, таке управління представляє собою розробку і застосування урядами, приватним сектором і громадянським суспільством, при виконанні ними своєї відповідної ролі, загальних принципів, норм, правил, процедур прийняття рішень і програм, регулюючих еволюцію і застосування Інтернету.

На міжнародному рівні технічна координація здійснюється в рамках ICANN, але окремі питання, такі як захист прав інтелектуальної власності в інтернеті, вирішуються в рамках міжнародних організацій, зокрема, СОТ і ВОІВ. Деякі питання вирішуються на рівні окремих держав.

Багато країн давно займаються політикою захисту інформаційних потоків та систем – не тільки як джерел державних секретів, але і як джерел економічного прибутку. Франція, наприклад, відзначилися у створенні власного сегменту інтернету на французькій мові. Вона взяла під свій контроль прибутковий ринок комп'ютерної техніки, програмного забезпечення та інформаційних потоків на всьому франкомовному просторі. Відомий досвід Китаю, який досяг суттєвого економічного росту за рахунок переорієнтації інформаційних потоків та акумуляції капіталів в інформаційній сфері.

Найчастіше соціальні мережі змушені надавати інформацію про своїх користувачів спецслужбам, причому мова йде не тільки про такі країни, як Китай, який широко відомий своєю обмежувальною політикою в інтернеті, але і США, а також низці країн ЄС.

Після подій 11 вересня 2001 р. в США були прийняті закони, що обмежують безпеку користувачів інтернету на користь безпеки держави, що позитивно сприйнято суспільством, так як складно забезпечити особисту безпеку в умовах, коли безпека держави під реальною загрозою.

Стратегії глобального інформаційного протиборства лежать в основі аналітичних розробок дослідницьких інституцій різних країн світу, метою яких є саме забезпечення інформаційного лідерства у сфері міжнародної безпеки. За

результатами досліджень аналітики виділяють такі моделі системи глобальної інформаційної безпеки:

Модель А – створення абсолютної системи захисту країни-інформаційного лідера проти будь-якого виду наступальної інформаційної зброї, що обумовлює об'єктивні переваги в потенційній інформаційній війні, змушує інші країни шукати альянсу у військово-інформаційних діях з країною-інфолідером. При цьому може бути використано систему жорстокого контролю над інформаційним озброєнням противника на підставі потенційних міжнародних документів з інформаційної безпеки.

Модель В – створення значної переваги державами-потенційного ініціатора інформаційної війни в наступальних видах озброєнь, у знешкодженні систем захисту державами-протиника засобами інформаційного впливу, координація дій із союзними державами з використаннями визначених засобів інформаційної зброї для ідентифікації джерел і типів інформаційних загроз.

Модель С – наявність кількох країн-інфолідерів та потенційного протиборства між ними, визначення фактору стримування експансії інформаційних загроз, забезпечення в перспективі домінування однієї з держав у сфері міжнародної інформаційної безпеки з можливостями значного впливу на глобальну інфосферу та переважного права вирішення проблем глобального світопорядку.

Модель D – всі конфліктуючі сторони використовують транспорантність інформації для формування ситуативних альянсів, для досягнення переваг локальних рішень, які спроможні заблокувати технологічне лідерство, для використання можливостей інфоінфраструктури на окремих територіях з метою організації внутрішнього конфлікту між опозиційними силами(політичні, сепаратистські, міжнаціональні конфлікти) для проведення міжнародних антитерористичних інформаційних операцій.

Модель Е – протиборство світової спільноти та міжнародної організованої злочинності, здатної контролювати перебіг політичних, економічних, суспільних і, зрештою, цивілізаційних процесів. Можливість такої моделі передбачена в дослідженні Національної ради розвідки США «Mapping the global

future»- 2020 у версії «Коло страху» («Cycle of fear»), яка є найбільш песимістичним сценарієм майбутнього світової спільноти[38].

Концепція міжнародної інформаційної безпеки визначає критичні структури, які зазнають впливу в умовах інформаційного протиборства. Найбільш вразливими вважаються політична, суспільна, економічна, військова, інноваційна, науково-технологічна, духовна сфери життєдіяльності суспільства.

У політичній сфері інформаційна безпека стосується всіх елементів політичної структури держави та суспільства: структур підготовки та прийняття політичних рішень, структур управління місцевої та регіональної влади, структур виборчих систем, інформаційно-телекомунікаційних урядових систем спеціального призначення.

В економічній сфері критичними є системи загальноекономічного аналізу та прогнозування економічного розвитку, структури прийняття рішень та координації управлінських дій в економічній сфері, зокрема, в умовах надзвичайного стану, системи управління в критично важливих для держави структурах(енергетика, комунікації, інформаційні мережі).

Феномен інформаційної безпеки в міжнародних відносинах обумовлюється стратегічною спрямованістю інформаційних впливів проти критично важливих структур життєдіяльності і функціонування міжнародного співтовариства, визнання їх в якості інформаційної зброї, катастрофічної за наслідками свого застосування, необхідністю створення міжнародного механізму протидії і попередження глобальних інформаційних війн в рамках політичної компетенції ООН, регіональних міжнародних організацій з проблем безпеки та оборони, політичних рішень на національному рівні.

Міжнародна інформаційна безпека – стан міжнародних відносин, який виключає порушення світової стабільності та створення загрози безпеці держав і світової спільноти в інформаційному просторі.

[38] Міжнародна інформаційна безпека: Сучасні виклики та загрози. – К.:Центр вільної преси, 2006. – С. 147.

Усі питання забезпечення інформаційної безпеки держави, крім технічних засобів захисту інформації, повинні регулюватися нормами міжнародного права, так як засоби інформаційного впливу мають деструктивні наслідки не тільки для держави, проти якої вони спрямовані, а й для всієї світової спільноти.

Сьогодні світова спільнота приходить до думки про необхідність створення міжнародних актів, які містили б уніфіковані норми з правового регулювання міжнародної інформаційної безпеки, про що свідчать Загальна декларації прав людини 1948 р.; Міжнародний пакт про громадянські і політичні права 1966 р.; Резолюція 45/95 ГА ООН про керівні принципи регламентації комп'ютеризованих картотек, що містять дані особистого характеру 1990 р.; міжнародна інформаційна безпека на глобальному рівні – Резолюція ГА ООН 53/70 «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки» (1999 р.); Резолюція ГА ООН 53/576 (1998 р.) «Роль науки та техніки в контексті міжнародної безпеки, роззброєння та інших, пов'язаних з цим сфер»; Резолюція ГА ООН 54/49 (1999 р.) «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки»; Резолюція ГА ООН 55/28 (2000 р.) «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» тощо; розповсюдження новітніх технологій – Резолюція ГА ООН 53/73 (1999 р.) «Роль науки і техніки в контексті міжнародної безпеки і роззброєння»; Декларації тисячоліття ООН 2000 р., Декларація ЄКОСОР «Роль інформаційних технологій у контексті глобальної економіки, що базується на знаннях» 2000 р.; Резолюція ГА ООН 57/239 (2002 р.) «Створення глобальної культури кібербезпеки»; Резолюція ГА ООН 60/51 (2005 р.) «Роль науки і техніки в контексті міжнародної безпеки і роззброєння» тощо; боротьба з кіберзлочинністю – Резолюція ГА ООН 56/121 (2001 р.) «Боротьба зі злочинним використанням інформаційних технологій»; Резолюція ГА ООН 56/27 «Заходи з ліквідації міжнародного тероризму» (2003 р.); Деклараціях ООН 2005 р.; збереження інформаційного надбання людства висвітлено в документах спеціалізованої установи ООН – ЮНЕСКО.

Свою позицію країни-члени Ради Європи щодо змісту терміну «інформаційна безпека» висловили при обговоренні питань міжнародної інформаційної безпеки на 56-й сесії Генеральної Асамблеї ООН: «Інформаційна та мережева безпека означає захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації і створення надійного джерела постачання обладнання, послуг та інформації. Інформаційна безпека також охоплює захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. Недостатній захист життєво важливих інформаційних ресурсів і інформаційних і телекомунікаційних систем може створити загрозу для міжнародної безпеки».

Загрози інформаційній безпеці реалізуються через порушення критичної інфраструктури, вільного обігу інформації, неправомірні дії щодо інформації, через невідповідність інформаційної політики, засобів інформування громадськості. Відповідно до критичних сфер міжнародного співробітництва класифікуються *загрози для інформаційної безпеки*. Існують різні типології загроз, але, узагальнюючи, можна виділити такі види загроз:

– інформаційно-технологічні;

– інформаційно-комунікаційні;

– інформаційно-психологічні.

Актуальними проблемами міжнародної інформаційної безпеки вважаються:

1) формування належної соціальної бази інформаційної безпеки та подолання інформаційної нерівності між країнами;

2) практична реалізація потенційних можливостей інформаційної безпеки для різних соціальних верств населення з метою забезпечення їхньої нормальної діяльності та інтеграції у світову систему;

3) ефективне використання національних і наднаціональних структур інформаційної безпеки у системі вільної міжнародної комунікації, співробітництва в різних сферах життя з метою формування взаєморозуміння й довіри та попередження міжнародних і регіональних конфліктів;

4) переорієнтація систем інформаційної безпеки від виконання завдань суто охоронних і захисних на завдання конструктивної модернізації структур національної свідомості та формування єдиної планетарної свідомості як «інфраструктури» збереження цивілізації й забезпечення виживання людства.[39]

Відповідно до своїх видів міжнародна інформаційна безпека включає такі спрямування:

І. Глобальна інформаційна безпека:

1) безпека розвитку міжнародної інформаційної сфери;

2) захист міжнародного інформаційного ринку від незаконних посягань акторів міжнародних інформаційних відносин;

3) захист та обмеження обігу інформації в цілях глобальної інформаційної безпеки;

4) захист міжнародної інформаційної інфраструктури;

5) захист міжнародних інформаційних ресурсів;

6) побудова глобального інформаційного суспільства тощо;

ІІ. Інформаційна безпека окремих держав у міжнародному інформаційному просторі:

1) безпека інформаційного простору держави від інформаційних загроз, інформаційних операцій, інформаційного тиску та інформаційних війн з боку інших акторів міжнародних інформаційних відносин;

2) захист державного інформаційного ринку від незаконних посягань акторів міжнародних інформаційних відносин;

3) захист та обмеження міжнародного обігу інформації в цілях державної інформаційної безпеки;

4) побудова та забезпечення належного функціонування інформаційного суспільства;

5) захист своїх приватних осіб від незаконних посягань акторів міжнародних інформаційних відносин тощо;

[39] Макаренко Є. А., Рижиков М. М., Ожеван М. А., Головченко В. І., Гондюл В. П. Міжнародна інформаційна безпека: Сучасні виклики та загрози. – К.: Центр вільної преси, 2006. – С. 4.

III. Інформаційна безпека установ у міжнародному інформаційному просторі:

1) захист інформації з обмеженим доступом, яка належить установі, від несанкціонованих дій з боку інших акторів міжнародної інформаційної сфери;

2) доступ до загальнодоступної інформації та інформації, доступ до якої не може бути обмежено;

3) захист від випадкового чи навмисного втручання в нормальний процес функціонування автоматизованої інформаційної системи організації (установи) з боку інших акторів міжнародної інформаційної сфери тощо;

IV. Інформаційна безпека людини в міжнародному інформаційному просторі:

1) захист інформаційної і комунікаційної приватності (особливо персональних даних);

2) вільний доступ до масової та суспільно-значущої інформації;

3) захист від негативного інформаційного впливу;

4) захист інформаційних і комунікаційних прав на міжнародному рівні тощо.

2.2.3. Пріоритети державної політики України в інформаційній сфері

Під *національним інформаційним простором* розуміють усю сукупність інформаційних потоків як національного походження, так і іноземних, що доступні на території держави.

Основними *цілями інформаційної політики України* є забезпечення:

– захисту інформаційного суверенітету держави, особливо захисту національного інформаційного простору з інформаційним ресурсом і системи формування масової суспільної свідомості;

– рівня інформаційної достатності для прийняття рішень державними органами, підприємствами і громадянами;

– реалізації конституційних прав і свобод громадян, суспільства і держави.

Серед таких пріоритетів визначальними, на наш погляд, є:

– розробка та впровадження сучасних адекватних методів і засобів захисту національного інформаційного простору від негативних іноземних інформаційних впливів;

– створення якісного національного інформаційного продукту з метою витіснення іноземного інформаційного продукту, який створює передумови для виникнення загроз національній інформаційній безпеці нашої держави; наповнення світового інформаційного простору позитивною інформацією про Україну;

– запровадження суспільного мовлення для задоволення інформаційних потреб суспільства, залучення громадян до обговорення та вирішення найважливіших соціально-політичних питань, сприяння формуванню громадянського суспільства;

– створення якісно нової за статусом, повноваженнями та політичною вагою державної установи з правом розробляти заходи щодо впровадження державної інформаційної політики та координувати процес їх реалізації;

– перегляд засад формування, впровадження та модернізація системи забезпечення інформаційної безпеки держави.

Реалізація державної політики щодо захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах полягає у:

– підготовці пропозицій до визначення загальної стратегії та пріоритетних напрямів діяльності у сфері захисту державних інформаційних ресурсів в інформаційно-телекомунікаційній сфері;

– виконанні обов’язків уповноваженого органу у сфері захисту інформації в інформаційно-телекомунікаційних системах;

– розробленні порядку та вимог до захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також погодження проектів нормативно-правових актів з цих питань;

– розробленні критеріїв та порядку оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо.

Реалізація державної політики забезпечується шляхом виконання низки заходів відповідно до визначених завдань, а саме:

– методичного керівництва та координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності з питань, пов'язаних із запобіганням вчиненню порушень безпеки інформації в інформаційно-телекомунікаційних системах, виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

– накопичення та аналізу даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також про їх наслідки;

– організації та здійснення оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, надання відповідних рекомендацій.

Концептуальні засади реалізації інформаційної політики зазначено в Законі України «Про Національну програму інформатизації України» від 4 лютого 1998 р. № 74/98-ВР та спрямованих на його застосування сформульовані в указах Президента України «Про рішення Ради національної безпеки і оборони України від 17 червня 1997 р. «Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин» від 21 липня 1997 р. № 663/97; «Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади» від 14 липня 2000 р. № 887/2000; «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31 липня 2000 р. № 928/2000; «Про рішення Ради національної безпеки і оборони України від

31 жовтня 2001 року «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» від 6 грудня 2001 р. № 1193/2001; дорученнях Президента України від 12 квітня 2000 р., 5 грудня 2000 р. та 25 квітня 2001 р. щодо створення та забезпечення функціонування національного каналу супутникового іномовлення.

З метою забезпечення єдиного підходу щодо захисту державних інформаційних ресурсів на виконання постанови Кабінету Міністрів України від 24.02.2003 № 208 «Про заходи щодо створення електронної інформаційної системи «Електронний Уряд» в рамках Національної системи конфіденційного зв'язку у м. Києві, створюється окрема підсистема для телекомунікаційного забезпечення функціонування Єдиного веб-порталу органів виконавчої влади.

На виконання завдань Національної програми інформатизації у межах виконання проекту «Забезпечити антивірусний захист державних інформаційних ресурсів» створено Центр антивірусного захисту інформації (ЦАЗІ). Одним із основних завдань ЦАЗІ є впровадження єдиної технологічної політики щодо антивірусного захисту інформації в інформаційно-телекомунікаційних системах органів державної влади, а також централізованого забезпечення їх антивірусними програмними продуктами, сертифікованими у встановленому законодавством України порядку.

Сьогодні до бази антивірусного програмного забезпечення ЦАЗІ з використанням мережі Інтернет підключено 66 адміністраторів безпеки ІТС органів державної влади. Також з використанням ресурсів ЦАЗІ проводяться державні експертизи антивірусних програмних засобів з метою визначення можливості їх застосування в Україні та експрес-експертизи антивірусних оновлень до них.

З метою проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах відповідно до затвердженого постановою Кабінету Міністрів України від 03.08.2005 р. № 688 Положення утворено Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління. Забезпечення функ-

ціонування цього Реєстру покладено на Департамент безпеки інформаційно-телекомунікаційних систем.

Реалізація вимог Положення створює передумови для:

– запровадження єдиної системи обліку відомостей про ІТС органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління;

– проведення аналізу стану захисту державних електронних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

– надання методичної допомоги і координування діяльності міністерств та інших центральних органів виконавчої влади, пов’язаної із захистом державних електронних інформаційних ресурсів в інформаційно-телекомунікаційних системах.

З метою оптимізації дій щодо недопущення реалізації загроз інформаційним ресурсам держави необхідно здійснювати проведення оцінювання (аудиту) стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, зокрема тих, що мають доступ до мережі Інтернет.

Подальшим кроком у напрямку організації та здійснення оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах має стати розроблення та видання відповідних нормативно-правових актів та нормативних документів, які б, з урахуванням міжнародного досвіду, дозволили оптимізувати вироблення єдиних критеріїв та порядку такого оцінювання.

На сьогодні з метою застосування упереджувальних заходів та розвитку методології запобігання порушенню цілісності, доступності та конфіденційності державних інформаційних ресурсів здійснюються заходи, спрямовані на підготовку до ліквідації наслідків несанкціонованих дій, що порушили безперебійне функціонування інформаційно-телекомунікаційних систем органів державної влади, поширюється інформація щодо наявних та ймовірних загроз, інструментів і засобів забезпечення безпеки інформації тощо.

В Адміністрації Держспецзв'язку України функціонує підрозділ, діяльність якого спрямована саме на вирішення таких завдань (CERT-UA**?**). Надання, в подальшому, відповідних повноважень та реєстрація встановленим порядком українського аналога CSIRT (Computer Security Incident Response Teams – структури швидкого реагування на інциденти, що загрожують безпеці інформаційних ресурсів) сприятиме ефективній реалізації державної політики у сфері захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, та підвищенню загального стану захисту національного інформаційного простору.

2.2.4. Доктрина інформаційної безпеки України

У зв'язку з рішенням Ради національної безпеки і оборони України «Про невідкладні заходи щодо забезпечення інформаційної безпеки України» від 21 березня 2008 р., введеним у дію Указом Президента України від 23 квітня 2008 р. № 377, було затверджено Доктрину інформаційної безпеки України (Указ Президента України від 8 липня 2009 р. № 514/2009).

У Доктрині наголошується, що інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, соціальної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

В інформаційній сфері України вирізняються такі життєво важливі інтереси:

1) особи:

– забезпечення конституційних прав і свобод та обов'язків людини на збирання, зберігання, використання та поширення інформації;

– недопущення несанкціонованого втручання у зміст, процеси оброблення, передання та використання персональних даних;

– захищеність від негативного інформаційно-психологічного впливу;

2) суспільства:

– збереження і примноження духовних, культурних, правових і моральних цінностей українського народу;

– забезпечення суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди;

– формування і розвиток демократичних інститутів громадянського суспільства;

3) держави:

– недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур;

– ефективна взаємодія органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері;

– побудова та розвиток інформаційного суспільства;

– забезпечення економічного та науково-технологічного розвитку України;

– формування позитивного іміджу України;

– інтеграція України у світовий інформаційний простір.

Діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки України має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства і людини за такими трьома головними напрямами:

1) інформаційно-психологічний (зокрема, забезпечення конституційних прав і свобод людини і громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських та національних моральних цінностей);

2) технологічний розвиток (зокрема, розбудова та інноваційне оновлення національних інформаційних ресурсів, впровадження новітніх технологій створення, оброблення та поширення інформації);

3) захист інформації (зокрема, забезпечення конфіденційності, цілісності та доступності інформації, у тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак).

Слід зазначити, що Доктрина інформаційної безпеки України спрямована на забезпечення необхідного рівня інформаційної безпеки України в конкретних умовах даного історичного періоду і є основою для формування державної політики у сфері інформаційної безпеки України.

Державна політика визначається пріоритетністю національних інтересів і має на меті унеможливлення реалізації загроз для інформації.

Основними напрямами такої політики є:

– забезпечення умов для розвитку і захисту всіх форм власності на інформаційні ресурси;

– формування і захист державних інформаційних ресурсів;

– створення і розвиток центральних і регіональних інформаційних систем та мереж, забезпечення їхньої сумісності і взаємодії в єдиному інформаційному просторі держави;

– створення умов для якісного і ефективного інформаційного забезпечення громадян, установ державної влади, органів місцевого самоврядування, організацій і суспільних об’єднань на основі державних інформаційних ресурсів;

– забезпечення національної безпеки у сфері інформатизації, а також забезпечення прав громадян, організацій в умовах інформатизації;

– сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем і технологій, засобів їхнього забезпечення;

– формування і здійснення єдиної науково-технічної промислової політики у сфері інформатизації з урахуванням сучасного світового рівня розвитку інформаційних технологій;

– підтримка проектів і програм інформатизації;

– створення і удосконалення системи інвестування і механізму стимулювання розроблення і реалізації проектів інформатизації;

– розвиток законодавства у сфері інформаційних процесів, інформатизації і захисту інформації.

Важливо підкреслити те, що метою інформаційної політики держави є створення умов для побудови в державі інформаційного суспільства як органічного сегмента глобального інформаційного співтовариства, забезпечення пріоритетного розвитку інформаційних ресурсів та інфраструктури, впровадження новітніх інформаційних технологій, захисту національних моральних і культурних цінностей, забезпечення конституційних прав на вільний доступ до інформації.

ТАЄМНОЗНАВСТВО. СЕКРЕТОЗНАВСТВО. КОНФІДЕНЦІЄЗНАВСТВО

ЧАСТИНА ІІ. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ТАЄМНОЇ, СЕКРЕТНОЇ І КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

РОЗДІЛ 1. ЗАХИСТ ТАЄМНОЇ ІНФОРМАЦІЇ В УКРАЇНІ

1.1. Історіографія становлення та розвитку захисту інформації в Україні

1.1.1. Витоки правового регулювання захисту інформації

Початковий період захисту інформації за часів Київської Русі (VI – середина XVI ст.) пов'язаний з потребами князів у захисті інформації. Як правило, відомості, що потребували захисту, переважно стосувалися військової справи або питань державної політики: про військо племінного князя, дислокацію війська під час походу, зміст невигідно укладених договорів; розташування, укріплення і забезпечення продовольством та оснащення княжого граду. Протягом періоду існування Київської Русі до монголо-татарської навали відомо лише дев'ять випадків успішної облоги міста та сорок два випадки безуспішної. Влада та особа князя охоронялися понад усе: за посягання на владу та життя князя призначалася найвища міра покарання. Передача військової інформації ворогу або втеча з поля бою з метою передання інформації (зрада) були державним злочином і теж жорстоко каралися звичаєвим правом[40] та законами Київської Русі.

За князювання Володимира та Ярослава виняткового розмаху набуває зовнішньополітична, дипломатична діяльність держави, і саме інформація про дипломатичні відносини підлягає охороні. За князювання Ярослава Мудрого зібрання грамот і договорів Русі з іншими країнами розміщувалося в Михайлівському приділі Софійського собору. Одним із найбільш відомих сховищ важливих документів на території України був також Києво-Печерський монастир. Зазначений порядок, по суті, можна віднести до перших режимних заходів, які забезпечували охорону важливих документів (відомостей).

[40] У найбільш розповсюдженому та спрощеному варіанті процес розвитку форм права описується наступним чином: первісним джерелом права був звичай. Більшість феодальних кодифікацій права (від Саксонського зерцала до Руської Правди) були збірками звичаїв.

Прикладом захисту інформації в Київській Русі стала поїздка княгині Ольги до Константинополя, яка, напевне, була настільки важливою, що візантійські й руські джерела не висвітлюють мету цієї поїздки. Істориками висловлювалася думка, що Ольга подолала неблизький шлях до Константинополя з ціллю прийняти святе хрещення від імператора та візантійського патріарха. Однак за історичними документами Ольга вже була християнкою до цієї поїздки, тобто основним був не релігійний мотив. Уважається, що головною метою візиту Ольги до Царгорода було поновлення сплати імперією данини Києву й відновлення привілеїв руським купцям на території Візантії, котрі втратив Ігор за угодою 994 р. Імовірно, поширення цієї інформації для Візантії було невигідним і підривало міць держави, тому її розголошення було заборонено.

Поступово складаються традиції діловодства, відбувається накопичення досвіду документування, оброблення і зберігання документів, захисту від підробки. Одним із методів захисту інформації стала криптографія, котра, на думку дослідників, виникла разом із появою писемності, коли для шифрування писемної інформації слов'янські літери почали замінювати грецькими або латинськими. У давньоруській писемності для визначення таємного письма вживали терміни «хвіоть», або «фіоть», та «еффата». Відомі два методи шифрування: перший полягає в переміщенні літер у тексті, що веде до зміни їхнього порядку при написанні; другий метод залишає порядок літер попереднім, але вони замінюються умовними знаками (іншими літерами, цифрами, знаками).

Захист інформації на території України в період литовсько-польського панування набуває особливого значення: з'являється новий вид інформації – державна таємниця. Починає формуватися нормативна база, що регулює охорону державної таємниці, важливого значення набуває інформація про внутрішньополітичне становище і зовнішню політику. Наприклад, у артикулі 3 розд. 1 Литовського статуту Великого князівства Литовського 1588 р., що діяв на значній території України, за злочини проти маєстату (престолу), за листу-

вання з ворогом і повідомлення йому відомостей, котрі могли б завдати шкоди державі, передбачалася страта[41].

У Запорізькій Січі система діловодства була досить розвиненою: при головній військовій канцелярії та при канцеляріях у паланках існували власні архіви. Є дані, що кількісний склад військової канцелярії Січі у XVIII ст. нараховував 48 чоловік. Особливо цікавою серед посад військових служителів є посада військового тлумача (драгомана), який, окрім іншомовних перекладів документів та переговорів з іноземцями, очолював розвідку та контррозвідку Січі та для виконання цих обов'язків виїздив сам або направляв розвідників у сусідні держави, входив до складу посольств, що відряджалися із Січі до іноземних країн.

З метою запобігання отриманню ворогом відомостей про чисельність війська та оперативно-тактичні плани гетьман, знаючи про наявність польських розвідників у таборі, значно обмежував коло осіб, обізнаних із суттю задуманих операцій, нерідко вдаючись до поширення дезінформації щодо подальшого способу дій. Наприклад, захищаючи військову інформацію під час війни з Польщею, Б. Хмельницький прагнув шляхом дезінформації посіяти в польському війську невпевненість, тобто застосовував принципи ведення «психологічної війни». Цим було започатковано процес становлення в Україні служби внутрішньої безпеки, створено елементи контролю з боку уряду за діяльністю дипломатів.

Першим органом державної безпеки Московського царства вважається Приказ таємних справ, створений у 1654 р., який функціонував з 1654 по 1676 рр. Основною функцією його було здійснення контролю за діяльністю інших органів управління, нагляду за «підозрілими чужинцями» на території російської держави, офіційного та негласного нагляду за діяльністю інших приказів, тобто за діяльністю всього апарату держави.

Задля збереження в таємниці інформації, що стосувалася державних справ, було введено присягу для канцелярських чинів. Починаючи з XVI ст. у Московському царстві для засекречування таємної писемної інформації почали за-

[41] У цій правовій нормі йдеться про умисну форму провини – повідомлення важливих для держави відомостей «з наміром», а також передбачено конкретного адресата – «неприятеля», що за сучасною теорією права дозволяє розглядати цей злочин як державну зраду у формі шпигунства.

стосовувати криптографію, і першим на озброєння такий спосіб захисту інформації взяв Посольський приказ. Значний внесок у розвиток криптографії зробив батько першого царя з династії Романових патріарх Філарет, який особисто займався питаннями зовнішніх відносин Московського царства. За часів Петра I шифруванням та дешифруванням документів займалися співробітники «цифірного відділення» посольської канцелярії.

Український гетьман П. Орлик шифрував свої листи до короля Швеції, представників інших країн, а також до Запорізького Війська. У листуванні П. Орлика застосовувалася передова для початку XVIII ст. технологія шифрування – для зашифрування числових даних використовувалися кодові позначення цифр і чисел.

Починаючи з середини XVII ст. у Росії й на українських землях у складі імперії велика увага приділяється захисту інформації, що регламентується правовими джерелами, у яких закріплюється кримінальна відповідальність за розголошення державної таємниці (Соборне уложення 1649 р., Генеральний регламент (Статут державних колегій) 1720 р., Права, за якими судиться малоросійський народ 1722 р., Уложення про покарання кримінальні і виправні 1743 р., Кримінальне уложення 1845 р., Закон Російської імперії «Про зміну чинних законів про державну зраду шляхом шпигунства» 1912 р.). У цей період розвивається система захисту інформації держави, а саме: створюються законодавчі акти, які регламентували захист інформації, з'являються органи таємної поліції, на які покладалися збирання і захист інформації про військово-політичне становище в державі.

У другій половині XVIII ст. розробкою та розкриттям шифрів займався один із підрозділів Секретної експедиції Колегії іноземних справ.

1.1.2. Правове забезпечення захисту інформації в XIX-XX столітті

Перша чверть XIX ст. характеризується створенням системи вищих і центральних державних органів управління, що зумовлено внутрішніми й зовнішніми обставинами, частиною яких стали міністерства. У міністерстві закордонних справ Росії питаннями захисту інформації у сфері зовнішньої політики за-

ймалися шифрувальний департамент, посли і консули, на яких був покладений підбір технічного персоналу і організація відправлення дипломатичної пошти.

У 1801 р. Олександр I видав указ про ліквідацію Таємної експедиції, натомість у 1802 р. було організовано Міністерство внутрішніх справ з особливою канцелярією, яка займалася політичними справами. 28 січня 1811 р. було видано «Загальне заснування міністерств» – законодавчий акт, який визначав усю систему міністерського устрою, включаючи діловодство.

Спроби побудови дієвої поліцейської організації в Росії продовжувалися: виникає III відділення Власної Його Імператорської Величності канцелярії.

Військово-політичні конфлікти XIX ст. вплинули на розвиток криптографії. Питаннями криптографічного захисту інформації займалися 3 і 4 («цифірні») експедиції Департаменту зовнішніх відносин Міністерства закордонних справ, після створення на базі Департаменту в 1846 р. Особливої канцелярії МЗС – «Цифірна» експедиція Особливої канцелярії, згодом – шифрувальний департамент МЗС. Великий вклад у розвиток російської криптографії вніс барон П. Л. Шиллінг фон Каштадт, який винайшов так званий біграмний шифр, котрий використовувався до кінця XX ст.

З розвитком телеграфного зв'язку значно збільшився обсяг інформації, що передавалася (у тому числі й секретно), з'являється техніка таємного зняття інформації з телеграфних ліній зв'язку і, відповідно, виникає необхідність у розробленні нових шифрів для захисту інформації, починають використовуватися мережі засекреченого зв'язку. У 1903 р. було здійснено першу спробу створення органу, який би виконував контррозвідувальні функції: у травні військове міністерство сформувало Розвідувальне відділення Головного штабу з пріоритетним визначенням організації охорони таємниць.

У 1911 р. військовим відомством було видано «Положення про листування і діловодство у військовому відомстві», яке регламентувало обмін телеграфними повідомленнями, встановлювало чітке значення написів, що обмежували доступ до документів з грифом «Таємно», «Не підлягає оголошенню», «Термі-

ново» тощо. Положення встановлювало застосування друкарських машинок для виготовлення документів, гектографів для копіювання.

Перша світова війна стала підставою для прийняття в Росії двох законодавчих актів – «Про затвердження Тимчасового положення про військову цензуру» від 20 липня 1914 р. і «Перелік відомостей, що становлять військову таємницю» від 20 липня 1914 р. Протягом 1914–1917 рр. у Росії набула подальшого розвитку нормативно-правова база, котра регулювала діяльність контррозвідки у сфері забезпечення державних секретів.

Формування національної системи захисту в період відродження української державності (1917–1921 рр.) полягало в побудові дієвої системи захисту інформації військових та державних секретів, інформації з обмеженим доступом, службової інформації, слідчої інформації, персональної інформації, а також у створенні спеціальних органів, які б займалися цими проблемами. Характер нормативної бази, що регламентував захист інформації, визначався особливостями цього історичного періоду і був малоефективним з таких причин:

– до створення нормативної бази не залучалися висококваліфіковані військові та досвідчені співробітники спеціальних служб, які були в розпорядженні Генерального секретаріату;

– за діяльністю створених комітетів і комісій не здійснювався необхідний контроль.

13 жовтня 1921 р. Декретом РНК був затверджений «Перелік відомостей, які становлять таємницю і не підлягають поширенню», у якому відомості поділяються на дві групи – військового та економічного характеру. Необхідність захисту інформації з обмеженим доступом була усвідомлена не відразу, але питання організації ефективних органів, які б займалися захистом секретної інформації, зрівнялося з питанням виживання для нової влади. У 1922 р. Секретаріат ЦК РКП(б) прийняв Постанову «Про порядок збереження і руху секретних документів», у 1926 р. було видано ряд загальносоюзних інструкцій, що регламентували окремі питання організації і ведення секретного діловодства, наприклад Інструкція з ведення секретного і шифрувального діловодства, Інструкція про по-

рядок підготовки і конвертування кореспонденції, яка надсилається дипломатичною поштою, у 1928 р. – Інструкція із секретного діловодства та Інструкція із шифрувального діловодства. У 1928 р. було прийнято рішення про відділення секретного діловодства від шифрувального.

У 1924–1925 рр. органам Державного політичного управління УРСР ввірявся контроль за додержанням режиму таємності та веденням шифрувальної справи.

24 квітня 1926 р. Постановою Ради народних комісарів СРСР затверджений новий Перелік відомостей, що є за своїм змістом спеціально охоронюваною державною таємницею, у якому всі відомості були розділені на три групи: відомості військового характеру, відомості економічного характеру і відомості іншого характеру, а також введені три категорії таємності: «Цілком таємно», «Таємно», «Не підлягає оголошенню». З урахуванням недоліків цього документа через два місяці було видано секретний Перелік питань цілком таємної, таємної і такої, що не підлягає розголошенню, інформації, усі відомості якого розподілені на чотири категорії: питання військового характеру, питання фінансово-економічного характеру, питання політичного (у тому числі партійного) характеру, питання загального характеру.

2 січня 1940 р. Постановою РНК затверджено нову Інструкцію з ведення секретних і мобілізаційних робіт і діловодства в установах і на підприємствах, метою якої було посилення режиму секретності, вироблення єдиної системи секретного діловодства та забезпечення охорони секретної інформації в установах і на підприємствах СРСР та УРСР. Ще однією формою діяльності щодо захисту інформації з обмеженим доступом стала цензура, яка була як відкрита відносно друкованих видань, так і закрита, що здійснювалася органами Державного політичного управління.

Радянська система захисту інформації в 40–80-х рр. XX ст. підтверджує забезпечення охорони державної таємниці Постановою Ради Міністрів СРСР «Про встановлення переліку відомостей, що складають державну таємницю, розголошення яких карається законом» від 8 червня 1947 р. та Указом Президії

Верховної Ради СРСР «Про відповідальність за розголошення державної таємниці й за втрату документів, що містять державну таємницю» від 9 червня 1947 р. 1 березня 1948 р. Постановою Ради Міністрів СРСР затверджені Перелік найголовніших відомостей, що складають державну таємницю та Інструкція з забезпечення охорони державної таємниці в установах і на підприємствах СРСР, у якій встановлено три ступені секретності («Таємно», «Цілком таємно», «Особливої важливості»), а також затверджено порядок визначення ступеня секретності відомостей, проведено уніфікацію назв секретних органів. У цьому переліку відомості мали такі види:

– мобілізаційні питання і відомості про резерви;

– відомості військового характеру;

– відомості економічного характеру: промисловість, корисні копалини, сільське господарство, транспорт і зв'язок;

– фінанси; зовнішня політика і зовнішня торгівля; питання науки і техніки: атомна енергія, радіолокаційна техніка, реактивна техніка, відкриття і винаходи, відомості з картографії, геології, гідрології;

– відомості про Арктику;

– різні відомості.

У березні 1954 р. функції забезпечення охорони державної таємниці були передані утвореному Комітету державної безпеки при Раді Міністрів СРСР затвердженням Інструкції із забезпечення охорони державної таємниці в установах і на підприємствах СРСР, у якій викладено завдання секретних відділів, секретних частин, описано необхідні вимоги до приміщень секретних відділів, частин та їх охорони; визначено допуск осіб до документів та інформації «Особливої важливості», «Цілком таємної», «Таємної», чітко визначено ступінь таємності.

У 1959 р. Постановою Ради Міністрів СРСР затверджено Інструкцію по забезпеченню збереження державної таємниці в установах і на підприємствах СРСР, яку згодом замінила затверджена в жовтні 1965 р. Інструкція по забезпе-

ченню збереження державної таємниці і режиму секретності робіт, що проводяться.

Стрімкий технічний прогрес створює новітні технічні засоби, за допомогою яких можна знімати важливу інформацію, зокрема інформацію, що містить державну таємницю.

Постановою Ради Міністрів СРСР «Про протидію іноземним технічним розвідкам» від 18 грудня 1973 р. було утворено систему комплексної протидії технічним розвідкам противника на чолі з загальнодержавним органом – Державною технічною комісією СРСР з протидії іноземним технічним розвідкам.

На початку 70-х рр. XX ст. загальнодержавна система захисту державної таємниці повністю сформувалася і проіснувала в такому вигляді до розпаду СРСР.

РОЗДІЛ 2 ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ

2.2.1. Становлення державних органів, що захищають державну таємницю

З часу проголошення 24 серпня 1991 р. державної незалежності України почалося формування системи захисту її інформації: розробляється нормативно-правова база, яка регламентує створення системи та органів захисту інформації з обмеженим доступом.

Першим державним органом, на який були покладені питання захисту інформації, стала Служба безпеки України. Відповідно до Закону України «Про Службу безпеки України» від 25 березня 1992 р. № 2229-XII їй було надано правовий статус державного правоохоронного органу спеціального призначення, який забезпечує державну безпеку України. Серед завдань, які виконувала Служба безпеки України, ст. 24 даного Закону визначає «участь у розробці і здійсненні відповідно до Закону України «Про державну таємницю» та інших актів законодавства заходів щодо забезпечення охорони державної таємниці та конфіден-

ційної інформації, що є власністю держави, сприяти у порядку, передбаченому законодавством, підприємствам, установам, організаціям та підприємцям у збереженні комерційної таємниці, розголошення якої може завдати шкоди життєво важливим інтересам України».

Наступними заходами, спрямованими на удосконалення системи захисту державної таємниці та інститутів збереження державної таємниці, зокрема, стало створення Державної служби України з питань технічного захисту інформації (Указ Президента України «Про Державну службу України з питань технічного захисту інформації» від 1 грудня 1992 р. № 593) та Державного комітету з питань державних секретів (Постанова Кабінету Міністрів України «Про утворення Державного комітету України з питань державних секретів» від 4 травня 1993 р. № 327), а згодом утворення на їхній базі Державного комітету України з питань державних секретів та технічного захисту інформації (Указ Президента України «Про зміни в системі центральних органів виконавчої влади України» від 26 липня 1996 р. № 596/96) – центрального органу виконавчої влади у сфері охорони державної таємниці і технічного захисту інформації на всій території України.

Згідно з Положенням про Держкомсекретів України, затвердженим Указом Президента України Про «Положення про Державний комітет України з питань державних секретів та технічного захисту інформації» від 5 листопада 1996 р. № 1047/96, було утворено колегію Держкомсекретів України, яка розглядала питання щодо:

– програм і планів заходів зі здійснення політики держави щодо охорони державної таємниці у сферах оборони, економіки України, її міжнародних відносин, безпеки та правопорядку;

– розроблення концептуальних основ державної політики, охорони державної таємниці, створення й удосконалення системи охорони державної таємниці, її організаційної та правової основи;

– організаційного та методичного керівництва системою охорони державної таємниці України та забезпечення її функціонування;

– забезпечення контролю за режимом секретності в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях, незалежно від форм власності;

– організації взаємодії з державними експертами з питань таємниць, надання їм методичної допомоги в здійсненні покладених на них функцій з охорони державної таємниці;

– здійснення керівництва уповноваженими органами Держкомсекретів України на місцях, надання їм практичної допомоги у вирішенні покладених на них завдань, контроль за станом службової діяльності структурних підрозділів Держкомсекретів України та заходів щодо її вдосконалення;

– розроблення і обговорення проектів законів України, указів і розпоряджень Президента України і нормативних актів Кабінету Міністрів України, що готувалися Держкомсекретів України;

– роботи з кадрами, організації підготовки спеціалістів для роботи у сфері охорони державної таємниці тощо.

2.2.2. Результати діяльності Держкомсекретів України

За період існування колегія Держкомсекретів України розглянула більше 75 питань, прийнявши відповідні рішення, та визначила шляхи подальшого вирішення найважливіших питань у сфері охорони державної таємниці.

Фахівцями Держкомсекретів України за відповідним рішенням колегії було розроблено та забезпечено введення в дію цілої низки загальнодержавних нормативно-правових актів[42], зокрема: 1) Закон України «Про державну таємницю»; 2) Постанова Кабінету Міністрів України «Про види, розміри і порядок на-

[42] Дані нормативні акти були створені на основі таких документів, котрі на сьогодні втратили чинність: Указ Президента України «Про положення про державного експерта з питань таємниць» від 23 квітня 1994 р. № 185/94; Постанова Кабінету Міністрів «Про затвердження Положення про порядок і механізм формування та опублікування Зводу відомостей, що становлять державну таємницю» від 29 квітня 1994 р. № 278; Постанова Кабінету Міністрів «Про затвердження Положення про порядок і умови надання органам державної виконавчої влади, підприємствам, установам і організаціям дозволу на здійснення діяльності, пов'язаної з державною таємницею, та про особливий режим цієї діяльності» від 20 червня 1994 р. № 426; Постанова Кабінету Міністрів «Про затвердження Положення про порядок надання, скасування та переоформлення допуску громадян України до державної таємниці» від 30 липня 1996 р. № 878; Постанова Кабінету Міністрів «Про затвердження Положення про режимно-секретні органи в міністерствах, відомствах, Уряді Автономної Республіки Крим, місцевих органах державної виконавчої влади, виконкомах Рад, на підприємствах, в установах і організаціях» від 4 серпня 1995 р. № 609; Постанова Кабінету Міністрів «Про затвердження Інструкції про порядок охорони державної таємниці, а також іншої інформації з обмеженим доступом, що є власністю держави, під час прийому іноземних делегацій, груп та окремих іноземців і проведення роботи з ними» від 22 травня 1996 р. № 558.

дання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до державної таємниці» від 15 червня 1994 р. № 414; 3) Постанова Кабінету Міністрів «Про встановлення письмової форми трудових договорів з працівниками, діяльність яких пов'язана з державною таємницею» від 16 листопада 1994 р. № 779.

2.2.3. Державна таємниця як особливий вид інформації, що захищається

Контроль за дотриманням законодавства з питань охорони державної таємниці від розповсюдження в пресі та інших засобах масової інформації був покладений на створене в 1992 р. Головне управління по охороні державних таємниць у пресі та інших засобах масової інформації при Кабінеті Міністрів України, а після його ліквідації у 1993 р. – на Державний комітет України по охороні державних таємниць у пресі та інших засобах масової інформації, на базі якого утворено Міністерство України у справах преси та інформації (Указ Президента України «Про утворення Міністерства України у справах преси та інформації» від 18 листопада 1994 р. № 689/94) У 1996 р. після прийняття Конституції України, ст. 15 якої забороняла цензуру, Міністерство України у справах преси та інформації було ліквідовано, а на його базі було створено Міністерство інформації України (Указ Президента України «Про Міністерство інформації України» від 13 листопада 1996 р. № 1061/96). У 1999 р. був створений Державний комітет інформаційної політики України, що став правонаступником ліквідованого Міністерства інформації України (Указ Президента України «Про Положення про Державний комітет інформаційної політики України» від 19 серпня 1999 р. № 1017/99).

У 2000 р. цей комітет був об'єднаний із Державним комітетом телебачення і радіомовлення України (Указ Президента України «Про Державний комітет інформаційної політики, телебачення і радіомовлення України» від 25 липня 2000 р. № 919/2000), а в 2003 р. перейменований у Державний комітет телебачення та радіомовлення (Держкомтелерадіо України) (Указ Президента України від 31 січня 2003 р. № 54/2003).

Сьогодні *основними завданнями Держкомтелерадіо України* є:

– участь у формуванні та реалізації державної політики в інформаційній і видавничій сферах, у сфері захисту суспільної моралі;

– сприяння реалізації конституційного права на свободу слова;

– координація діяльності в інформаційній та видавничій сферах;

– здійснення державного регулювання і контролю в інформаційній та видавничій сферах;

– сприяння розвитку інформаційного суспільства, розширенню національного інформаційного простору.

Для реалізації державної політики технічного захисту інформації щодо органів державної влади, органів місцевого самоврядування, органів управління Збройних сил України та інших військових формувань, утворених згідно із законодавством України, відповідних підприємств, установ та організацій Указом Президента України «Про Положення про технічний захист інформації в Україні» від 27 вересня 1999 р. № 1229/99 у складі Служби безпеки України створено Департамент спеціальних телекомунікаційних систем та захисту інформації.

2.2.4. Державна служба спеціального зв'язку та захисту інформації

Удосконалення системи охорони державної таємниці відбувалося реформуванням державних інститутів, що проводили діяльність, спрямовану на охорону державної таємниці. Законом України «Про державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 р. № 3475-IV на базі Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України було створено Державну службу спеціального зв'язку та захисту інформації України – орган, призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, криптографічного й технічного захисту інформації.

Основними завданнями Державної служби спеціального зв'язку та захисту інформації України є:

– участь у формуванні та реалізація державної політики у сфері захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації;

– забезпечення в установленому порядку урядовим зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, інших посадових осіб органів державної влади, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного та воєнного стану, а також у разі виникнення надзвичайної ситуації;

– забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку і Національної системи конфіденційного зв'язку;

– визначення вимог і порядку створення та розвитку систем технічного та криптографічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– здійснення державного контролю за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису;

– охорона об'єктів, приміщень, систем, мереж, комплексів, засобів урядового і спеціального зв'язку, ключових документів до засобів криптографічного захисту інформації Державної служби спеціального зв'язку та захисту інформації України.

2.2.5. Законодавче регулювання обігу інформації в Україні

Найважливішим кроком на шляху нормативно-правового закріплення системи та органів захисту інформації з обмеженим доступом стало прийняття Закону України «Про державну таємницю», який регулює суспільні відносини,

пов'язані з віднесенням певних відомостей до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці в інтересах національної безпеки України. Цей Закон визначив орган, що забезпечуватиме охорону одного з найважливіших видів інформації з обмеженим доступом – державної таємниці. Спеціально уповноваженим органом влади стала Служба безпеки України.

Відносини у сфері охорони державної таємниці регулюються Конституцією України, законами України «Про інформацію», «Про державну таємницю», міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, та іншими нормативно-правовими актами.

Закон України «Про державну таємницю» уперше визначив основні поняття у сфері захисту інформації.

Державна таємниця (далі також – секретна інформація) – вид таємної інформації, що охоплює відповідні відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визначені в порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

Віднесення інформації до державної таємниці – процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з визначенням можливої шкоди національній безпеці України в разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього.

Гриф секретності – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації.

Державний експерт з питань таємниць – посадова особа, уповноважена здійснювати відповідно до вимог цього Закону віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин,

державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування.

Допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації.

Доступ до державної таємниці – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

Засекречування матеріальних носіїв інформації – введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифа секретності документам, виробам або іншим матеріальним носіям цієї інформації.

Звід відомостей, що становлять державну таємницю, – акт, у якому зведено переліки відомостей, що згідно з рішенням державних експертів із питань таємниць становлять державну таємницю у визначених цим Законом сферах.

Категорія режиму секретності – категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю і зосереджені в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях.

Криптографічний захист секретної інформації – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Матеріальні носії секретної інформації – матеріальні об'єкти, у тому числі фізичні поля, у яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

Охорона державної таємниці – комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв.

Режим секретності – встановлений згідно з вимогами цього Закону та інших виданих відповідно до нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці.

Розсекречування матеріальних носіїв секретної інформації – зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифа секретності документам, виробам або іншим матеріальним носіям цієї інформації.

Спеціальна експертиза щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею – експертиза, що проводиться з метою визначення в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях наявності умов, визначених цим Законом, для провадження діяльності, пов'язаної з державною таємницею.

Ступінь секретності («Особливої важливості», «Цілком таємно», «Таємно») – категорія, що характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою.

Технічний захист секретної інформації – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Крім основних понять, Закон України «Про державну таємницю» також визначає:

– компетенцію органів державної влади, органів місцевого самоврядування та їхніх посадових осіб у сфері охорони державної таємниці;

– здійснення права власності на секретну інформацію та її матеріальні носії;

– фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею;

– порядок віднесення інформації до державної таємниці;

– порядок засекречування і розсекречування матеріальних носіїв інформації;

– порядок охорони державної таємниці;

– контроль за забезпеченням охорони державної таємниці;

– відповідальність за порушення законодавства про державну таємницю.

Питання віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до державної таємниці, зміни ступеня секретності цієї інформації та розсекречування покладено на державних експертів з питань державної таємниці. Експерти з питань державної таємниці у Верховній Раді України призначаються Головою Верховної Ради, в інших органах державної влади – Президентом України за поданням керівника відповідного державного органу.

Рішення про засекречування інформації приймається державним експертом з питань державної таємниці за власною ініціативою або за зверненням керівника відповідного органу державної влади, виключно на підставах, передбачених у ст. 8 Закону України «Про державну таємницю». Державні експерти з питань таємниць (ст. 9 Закону України) відповідають за віднесення інформації у відповідних сферах до державної таємниці, зміну ступеня секретності цієї інформації та її розсекречування. Виконання функцій державного експерта з питань таємниць покладається на конкретних посадових осіб:

– у Верховній Раді України – Головою Верховної Ради України;

– в інших державних органах, Національній академії наук України, на підприємствах, в установах і організаціях – Президентом України за поданням Служби безпеки України на підставі пропозицій керівників відповідних державних органів, Національної академії наук України, підприємств, установ і організацій.

У рішенні державного експерта з питань державної таємниці щодо засекречення інформації визначається:

– інформація, яка має становити державну таємницю, та її відповідність категоріям і вимогам, передбаченим ст. 8 Закону України «Про державну таємницю»;

– підстави для віднесення інформації до державної таємниці та обґрунтування шкоди національній безпеці України в разі її розголошення;

– ступінь секретності зазначеної інформації;

– обсяг фінансування заходів, необхідних для охорони такої інформації;

– орган державної влади, орган місцевого самоврядування, підприємство, установа, організація чи громадянин, який вніс пропозицію про віднесення цієї інформації до державної таємниці, та орган державної влади (органи), якому надається право визначати коло суб'єктів, які матимуть доступ до цієї інформації;

– строк, протягом якого діє рішення про віднесення інформації до державної таємниці.

Строк дії режиму таємності залежить від ступеня таємності інформації. Згідно зі ст. 13 Закону України «Про державну таємницю», строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України. Цей строк не може перевищувати для інформації із ступенем секретності «Особливої важливості» 30 років, для інформації «Цілком таємно» – 10 років, для інформації «Таємно» – 5 років.

Висновок державного експерта з питань таємниць про засекречування або розсекречування інформації приймається в місячний термін після відповідного звернення керівника органу державної влади.

Інформація, що може бути віднесена до державної таємниці, визначається відповідно до норм ст. 8 Закону України «Про державну таємницю» і викладена у *Зводі відомостей, що становлять державну таємницю України*[43] (ЗВДТ), який «є єдиною формою реєстрації цих відомостей в Україні. З моменту опублікування

[43] Про затвердження Зводу відомостей, що становлять державну таємницю [Електронний ресурс] : наказ Служби безпеки України від 12 серп. 2005 р. № 440. – Режим доступу: http:/zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z0902-05.

ЗВДТ держава забезпечує захист і в правову охорону відомостей, які зареєстровані в ньому».

Звід відомостей є систематизованим переліком відомостей, що становлять державну таємницю, котрі упорядковані за чотирма великими групами (статті) відповідно до сфери державної діяльності:

– сфера оборони;

– сфера економіки, науки і техніки;

– сфера зовнішніх відносин;

– сфера державної безпеки і охорони правопорядку.

Відомості, що належать до цих груп, класифікуються на окремі пункти та підпункти за основними характеристиками:

– зміст відомостей, які становлять державну таємницю;

– ступінь секретності («Особливої важливості», «Цілком таємно», «Таємно»);

– строк дії рішення про віднесення інформації (30 років, 10 років, 5 років).

Реєстрація відомостей у Зводі є підставою для надання документу, виробу чи іншому матеріальному носію інформації, що містить ці відомості, грифа секретності, який відповідає ступеню секретності, встановленому для них у Зводі. Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого включена ця інформація, чи змін до нього у порядку, встановленому Законом України «Про державну таємницю».

Перелік відомостей, котрі становлять державну таємницю, у рамках визначених Законом України «Про державну таємницю» і ЗВДТ чотирьох основних сфер умовно класифікуються за напрямками та видами інформації.

Рівень таємності відомостей, віднесених до Зводу, залежить від змісту цих відомостей та від конкретного об’єкта, інформацію щодо якого ці відомості розкривають.

Державну таємницю можуть становити відомості, що не перелічені у Зводі, – випадки міжнародного передання секретної інформації. Відповідно до ст. 3 Закону України «Про державну таємницю», передані Україні відомості, що

становлять таємницю іноземної держави чи міжнародної організації, охороняються в порядку, передбаченому цим Законом.

Згідно зі ст. 9 Конституції України, чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, є частиною національного законодавства, норми міжнародного гуманітарного права являють собою внутрішні юридичні норми. Норми міжнародного гуманітарного права значною мірою є нормами *jus cogens*[44]. Стаття 19 Закону України «Про міжнародні договори України» від 29 червня 2004 р. № 1906-IV передбачає: «якщо міжнародним договором України, який набрав чинності в установленому порядку, встановлено інші правила, ніж ті, що передбачені у відповідному акті законодавства України, то застосовуються правила міжнародного договору».

Указ Президента України «Про деякі питання передачі державної таємниці іноземній державі чи міжнародній організації» від 14 грудня 2004 р. № 1483/2004 містить Положення про порядок підготовки документів щодо передачі державної таємниці іноземній державі чи міжнародній організації, що визначає порядок підготовки документів щодо здійснення державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями передачі секретної інформації до скасування рішення про віднесення її до державної таємниці та матеріальних носіїв такої інформації до їх розсекречування іноземним державам чи міжнародним організаціям з урахуванням необхідності забезпечення національної безпеки України. Підставою для передачі є міжнародний договір України, згода на обов'язковість якого надана Верховною Радою України, або мотивоване розпорядження Президента України. Дозвіл на передачу секретної інформації відповідно до цього Положення оформляється Службою безпеки України за наявності зобов'язань або письмових гарантій іноземної держави щодо забезпечення охорони секретної інформації, у тому числі недопущення її надання третій стороні.

[44] Англомовний тлумачний юридичний словник визначає jus cogens як «обов'язкову норму міжнародного права, від виконання якої жодна нація не може себе звільнити або не може бути звільнена іншою нацією». Термін jus cogens застосовують для позначення певних «базових принципів міжнародного права».

Режим секретної інформації в таких випадках визначається міжнародним договором і, відповідно, ці режими відрізняються залежно від країни чи міжнародної організації, від якої надійшла інформація, що охороняється, тобто можливе застосування правових режимів захисту інформації інших, ніж ті, що передбачені національним законодавством. Визначення таємної інформації при цьому також різняться.

Щодо визначення режиму захисту таємної інформації визначаються два основних підходи:

1) міжнародною угодою запроваджується класифікація таємної інформації, згідно з якою інформація з певним грифом таємності однієї сторони відповідає певному грифу таємності іншої сторони, і сторони угоди забезпечують стосовно такої таємної інформації щонайменше такий самий захист, який передбачається при поводженні з власною таємною інформацією з відповідним ступенем секретності;

2) у запровадженні на території однієї держави специфічного режиму захисту інформації, який застосовується щодо отриманої інформації іншою державою, з якої цю інформацію було отримано.

Враховуючи значне розширення міжнародного співробітництва України, у тому числі у сферах оборони, боротьби зі злочинністю, військово-технічного співробітництва, питання захисту таємної інформації набувають усе більшого значення. Наслідком цих процесів стало ухвалення протягом 2001–2017 рр. низки законів про ратифікацію угод між Україною та іншими державами у сфері охорони секретної інформації, зокрема були ратифіковані угоди з Республікою Словенія, Алжирською Народною Демократичною Республікою, Соціалістичною Республікою В’єтнам, Королівством Норвегія, Ісламською Республікою Пакистан, Республікою Албанія, Республікою Казахстан, Словацькою Республікою, Угорською Республікою, Європейським Союзом, Республікою Хорватія, Республікою Таджикистан, Азербайджанською Республікою, Республікою Молдова, Республікою Болгарія, Естонською Республікою, Республікою Корея, Латвійською Республікою, Чеською Республікою, Республікою Таджикистан, Литовською Рес-

публікою, Сполученими Штатами Америки, Республікою Індія, Республікою Вірменія, Грузією, Туркменістаном, Словацькою Республікою, Італійською Республікою, Державою Ізраїль, Федеративною Республікою Німеччина, Республікою Узбекистан, Російською Федерацією, Французькою Республікою. У 2010 р. були ратифіковані угоди про взаємну охорону секретної інформації з Великою Соціалістичною Народною Лівійською Арабською Джамагирією та Республікою Екваторіальна Гвінея.

2.2.6. Формування системи та органів захисту інформації в Україні

Останніми роками було внесено ряд змін у національне законодавство з метою впорядкування та попередження зловживань у засекреченні інформації.

Вагомий внесок у правове підґрунтя формування системи та органів захисту інформації зробив Закон України «Про основи національної безпеки України», визначивши загрози національній безпеці в інформаційній сфері:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, яка становить державну та іншу передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації.

У державних статистичних органах циркулює інформація, яка може вплинути на національну безпеку України. Відповідно, Закон України «Про державну статистику» від 17 вересня 1992 р. № 2614-XII регулює правові відносини в галузі державної статистики, визначає права і функції органів державної статистики, організаційні засади здійснення державної статистичної діяльності з метою отримання всебічної та об'єктивної статистичної інформації щодо економічної,

соціальної, демографічної та екологічної ситуації в Україні та її регіонах і забезпечення нею держави та суспільства.

У цьому Законі наведені такі визначення:

Адміністративні дані – дані, отримані на підставі спостережень, проведених органами державної влади (за винятком органів державної статистики), органами місцевого самоврядування та іншими юридичними особами відповідно до законодавства та з метою виконання адміністративних обов'язків та завдань, віднесених до їхньої компетенції.

Державна статистика – централізована система збирання, обробленання, аналізу, поширення, збереження, захисту та використання статистичної інформації.

Конфіденційна інформація – статистична інформація, що належить до інформації з обмеженим доступом і знаходиться у володінні, користуванні або розпорядженні окремого респондента та поширюється виключно за його згодою відповідно до погоджених з ним умов.

Статистична інформація (дані) – офіційна державна інформація, яка характеризує масові явища та процеси, що відбуваються в економічній, соціальній та інших сферах життя України та її регіонів.

Упорядкування статистичної інформації стосовно державної таємниці здійснюється відповідно до наказу Міністерства статистики України «Про затвердження форм державної статистичної звітності з питань державної таємниці» від 4 жовтня 1996 р. № 290.

Важливе значення в системі інформації держави відіграє науково-технічна інформація. Основи державної політики в галузі науково-технічної інформації, порядку її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу країни визначаються Законом України «Про науково-технічну інформацію», який виділяє такі поняття:

Науково-технічна інформація – це документовані або публічно оголошувані відомості про вітчизняні та зарубіжні досягнення науки, техніки і виробництва,

одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності.

Науково-інформаційна діяльність – це сукупність дій, спрямованих на задоволення потреб громадян, юридичних осіб і держави в науково-технічній інформації, що полягає в її збиранні, аналітично-синтетичній обробці, фіксації, зберіганні, пошуку і поширенні.

Інформаційні ресурси науково-технічної інформації – це систематизоване зібрання науково-технічної літератури і документації (книги, брошури, періодичні видання, патентована документація, нормативно-технічна документація, промислові каталоги, конструкторська документація, звітна науково-технічна документація з науково-дослідних і дослідно-конструкторських робіт, депоновані рукописи, переклади науково-технічної літератури і документації), зафіксовані на паперових чи інших носіях.

Довідково-інформаційний фонд – це сукупність упорядкованих первинних документів і довідково-пошукового апарату, призначених для задоволення інформаційних потреб.

Інформаційні ресурси спільного користування – це сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових, науково-технічних бібліотек, а також комерційних центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їхнє спільне використання.

Інформаційний ринок – це система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг.

У зв’язку з розвитком сучасних телекомунікаційних мереж і збільшенням циркуляції інформації в автоматизованих системах постало питання юридичного оформлення поширення та використання її через ці засоби, що закріплено в Законі України «Про захист інформації в інформаційно-телекомунікаційних системах», що регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах за умови до-

тримання права власності громадян та юридичних осіб на інформацію та права доступу до неї, права власника інформації на її захист, а також встановленого чинним законодавством обмеження на доступ до інформації. Доповненням цього нормативно-правового акта є Закон України «Про Національну програму інформатизації», який визначає, що інформаційний суверенітет держави – це здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави.

Питання, пов'язані з охороною державної таємниці, знаходять відображення і в інших законах.

Закон України «Про оперативно-розшукову діяльність» від 18 лютого 1992 р. № 2135-XII визначає таку підставу для проведення оперативно-розшукової діяльності, як запити повноважних державних органів, установ та організацій про перевірку осіб у зв'язку з їх допуском до державної таємниці.

Кримінальний кодекс України визначає склад злочинів, предметом яких є державна таємниця. Так, кримінально-правові норми, спрямовані на захист державної таємниці, містяться у розд. I «Злочини проти основ національної безпеки України», до якого включені ст. 111 «Державна зрада» та ст. 114 «Шпигунство», а також у розд. XIV «Злочини у сфері охорони державної таємниці, недоторканності кордонів, забезпечення призову та мобілізації», до якого входять ст. 328 «Розголошення державної таємниці» і ст. 329 «Втрата документів, що містять державну таємницю».

Кодекс України про адміністративні правопорушення (далі – КУпАП) передбачає адміністративну відповідальність за порушення законодавства про державну таємницю (ст. 212-2) у таких випадках:

1) недодержання встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;

2) засекречування інформації:

– про стан довкілля, про якість харчових продуктів і предметів побуту;

– про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися та загрожують безпеці громадян;

– про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти та культури населення;

– про факти порушень прав і свобод людини і громадянина; про незаконні дії органів державної влади, органів місцевого самоврядування та їх посадових осіб;

– іншої інформації, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена;

3) безпідставне засекречування інформації;

4) надання грифа секретності матеріальним носіям конфіденційної або іншої таємної інформації, яка не становить державної таємниці, або ненадання грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставне скасування чи зниження грифа секретності матеріальних носіїв секретної інформації;

5) порушення встановленого законодавством порядку надання допуску та доступу до державної таємниці;

6) невжиття заходів щодо забезпечення охорони державної таємниці та незабезпечення контролю за охороною державної таємниці;

7) провадження діяльності, пов'язаної з державною таємницею, без отримання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщення державних замовлень на виконання робіт, доведення мобілізаційних завдань, пов'язаних із державною таємницею, в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;

8) недодержання вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства та проведення роботи з ними;

9) невиконання норм і вимог криптографічного та технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення її конфіденційності, цілісності і доступності.

Кримінальний процесуальний кодекс України (далі – КПК) відносить зазначені вище злочини до підслідності Служби безпеки України.

Згідно з ч. 3 ст. 178 КПК України, виїмка документів, що становлять державну таємницю, проводиться тільки за вмотивованою постановою судді і в порядку, погодженому з керівництвом відповідної установи. Суб'єкти, які мають право бути наділені повноваженнями звертатися до суду щодо проведення виїмки документів, що становлять державну таємницю (орган дізнання, слідчий, прокурор), повинні мати допуск до секретної інформації.

Необхідно зазначити, що положення щодо захисту державної таємниці обов'язкові для виконання на території України і за її межами всіма органами представницької, виконавчої і судової влади, місцевого самоврядування, підприємствами, установами і організаціями, незалежно від їх організаційно-правової форми власності, посадовими особами, громадянами держави, які взяли на себе зобов'язання або зобов'язані за своїм статусом виконувати вимоги законодавства України стосовно державної таємниці.

РОЗДІЛ 3 ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В УКРАЇНІ

3.1. Службова інформація з обмеженим доступом

3.1.1. Поняття і сутність службової інформації

Для визначення поняття службової інформації (інформації для службового користування) необхідно визначити, які саме види діяльності слід вважати службою.

Закон України «Про державну службу» від 16 грудня 1993 р. № 3723-XII регулює суспільні відносини, які охоплюють діяльність держави щодо створення правових, організаційних, економічних та соціальних умов реалізації громадянами України права на державну службу; визначає основні організаційно-правові засади інституту державної служби в Україні та закріплює основи правового статусу державних службовців.

Відповідно до ст. 1 цього Закону України, *державна служба* в Україні – це професійна діяльність осіб, які займають посади в державних органах та їх апараті щодо практичного виконання завдань і функцій держави та одержують заробітну плату за рахунок державних коштів. Ці особи є державними службовцями і мають відповідні службові повноваження.

Уперше поняття «посадова особа» вводиться після проголошення незалежності України, коли виникла необхідність у формуванні інституту державної служби. *Посадовими особами* відповідно до цього Закону (ст. 2) вважаються керівники та заступники керівників державних органів та їх апарату, інші державні службовці, на яких законами або іншими нормативними актами покладено здійснення організаційно-розпорядчих та консультативно-дорадчих функцій. *Посада* – це визначена структурою і штатним розписом первинна структурна одиниця державного органу та його апарату, на яку покладено встановлене нормативними актами коло службових повноважень.

Правовий статус Президента України, Голови Верховної Ради України та його заступників, голів постійних комісій Верховної Ради України та їх заступників, народних депутатів України, Прем'єр-міністра України, членів Кабінету

Міністрів України, Голови та членів Конституційного Суду України, Голови та суддів Верховного Суду України, Голови та суддів вищих спеціалізованих судів України, Генерального прокурора України та його заступників регулюється Конституцією та спеціальними законами України.

Іншим видом служби є муніципальна служба. Законом України «Про службу в органах місцевого самоврядування» від 7 червня 2001 р. № 2493-III визначається, що *служба в органах місцевого самоврядування* – це професійна, на постійній основі діяльність громадян України, які займають посади в органах місцевого самоврядування, що спрямована на реалізацію територіальною громадою свого права на місцеве самоврядування та окремих повноважень органів виконавчої влади, наданих законом.

Регулювання правового статусу державних службовців, які працюють в апараті органів прокуратури, судів, дипломатичної служби, митного контролю, служби безпеки, внутрішніх справ та ін., здійснюється відповідно до Закону України «Про службу в органах місцевого самоврядування», якщо інше не передбачено законами України.

3.1.2. Законодавче забезпечення захисту конфіденційної інформації в Україні

Відповідно до ст. 9 Закону України «Про доступ до публічної інформації», до службової інформації може належати така інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони напряму пов'язані з розробкою діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф «Для службового користування».

Перелік відомостей, що становлять службову інформацію, який складається органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень, не може бути обмеженим у доступі.

Вимоги щодо захисту службової інформації визначені в ст. 10 Закону України «Про державну службу» і ст. 8 Закону України «Про службу в органах місцевого самоврядування» як збереження державної таємниці, інформації про громадян, що стала їм відома під час виконання обов'язків державної служби, а також іншої інформації, яка згідно з законодавством не підлягає розголошенню.

Закон України «Про Дисциплінарний статут митної служби України» від 6 вересня 2005 р. № 2805-IV вказує, що кожна посадова особа митної служби зобов'язана зберігати державну таємницю, конфіденційну, а також іншу охоронювану законом інформацію, що є власністю держави, фізичних та юридичних осіб.

У разі одержання доручення, яке суперечить чинному законодавству, державний службовець зобов'язаний невідкладно в письмовій формі доповісти про це посадовій особі, яка дала доручення, а в разі наполягання на його виконанні – повідомити вищу за посадою особу.

Відповідно до наказу Головного управління державної служби України «Про затвердження Загальних правил поведінки державного службовця» від 23 жовтня 2000 р. № 58 державному службовцю забороняється розголошувати довірену йому державну таємницю, іншу інформацію з обмеженим доступом, установлену законами України «Про інформацію» та «Про державну таємницю», у тому числі й після залишення ним державної служби, а також використовувати таку інформацію для власного інтересу або інтересу інших осіб шляхом порад чи рекомендацій. У той же час державний службовець не повинен приховувати від громадян факти та обставини, що становлять загрозу для життя, здоров'я і безпеки людей, крім випадків заборони розголошення відомостей, що становлять державну таємницю, вичерпний перелік яких визначений законом, а також завдавати шкоди державній інформаційній політиці, суб'єктам ін-

формаційних відносин шляхом ухилення чи утримання від вжиття заходів щодо охорони державної таємниці та іншої інформації з обмеженим доступом.

Специфічною вимогою є заборона використовувати інформацію з обмеженим доступом, що стала відомою державному службовцю у зв'язку з виконанням службових обов'язків, для власного інтересу. Причому необхідно зазначити, що ця вимога більшою мірою має етичний, ніж правовий характер, оскільки використання службової інформації для власного інтересу може відбуватися без її розголошення. А для застосування правових обмежень необхідно встановити причинно-наслідковий зв'язок між відомою суб'єкту службовою інформацією і його діями.

Для забезпечення виконання державними службовцями такого обмеження використовується низка обмежувально-профілактичних заходів: вимога ст. 5 Закону України «Про державну службу», згідно з якою державні службовці не повинні допускати дій і вчинків, які можуть зашкодити інтересам державної служби чи негативно вплинути на репутацію державного службовця, обов'язкове декларування доходів державного службовця (а в деяких випадках і членів його сім'ї) при вступі на державну службу та щорічно, обмеження, пов'язані з проходженням державної служби – як загальні (ст. 16), так і спеціальні (заборони займатися підприємницькою діяльністю), що встановлюються іншими законодавчими актами щодо окремих категорій державних службовців.

Основним нормативно-правовим актом, на основі якого здійснюється регулювання питань службової інформації, є Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави від 27 листопада 1998 р. № 1893. Згідно з цією Інструкцією переліки конфіденційної інформації, що є власністю держави і яким надається гриф обмеження доступу «Для службового користування», розробляються і вводяться в дію міністерствами, іншими центральними органами виконавчої влади, обласними, Київською міською державною адміністрацією, у яких утворюються або у володінні, користуванні чи розпорядженні яких перебувають ці відомості.

Цією Інструкцією визначаються основні правила поводження з носіями конфіденційної інформації, що становить службову інформацію, а саме:

– приймання і облік документів;

– розмноження і розсилання (відправлення) документів;

– формування виконаних документів у справи;

– використання документів; зняття грифа «Для службового користування»;

– особливе поводження з мобілізаційними документами;

– охорона конфіденційної інформації, що є власністю держави, під час прийому іноземних делегацій та окремих іноземців;

– відбір документів для зберігання і знищення;

– забезпечення збереження документів та перевірка їх наявності;

– облік, зберігання і використання печаток, штампів і бланків.

Оброблення, зберігання, а також друкування документів з грифом «Для службового користування» та конфіденційної інформації, що є власністю держави, з використанням автоматизованих систем дозволяється тільки за наявності виданого в установленому порядку Департаментом спеціальних телекомунікаційних систем та захисту інформації СБУ атестата відповідності комплексної системи захисту інформації в цій автоматизованій системі вимогам щодо захисту інформації.

Допускається, що в разі потреби на державних підприємствах, в установах і організаціях з урахуванням особливостей їхньої діяльності розробляються та за погодженням з міністерством, іншим центральним органом виконавчої влади, до сфери управління якого вони належать, вводяться в дію переліки конкретних видів документів у відповідній сфері діяльності.

Наприклад, наказом Міністерства економіки та з питань європейської інтеграції України «Про заходи щодо захисту конфіденційної і відкритої інформації, що циркулює в автоматизованій системі Міністерства» від 23 квітня 2002 р. № 121 з метою дотримання норм захисту конфіденційної і відкритої інформації, що циркулює в автоматизованій системі міністерства, затверджується нормати-

ний документ Комплексної системи захисту інформації в автоматизованій системі міністерства – Інструкція користувача автоматизованої системи.

Ця Інструкція регламентує роботу співробітників міністерства в частині захисту конфіденційної (для службового користування) та іншої інформації, що є власністю держави, під час користування автоматизованою системою, окремою локальною підмережею міністерства, що приєднана до мережі Інтернет та електронної пошти.

Інструкція розроблена на підставі таких документів:

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;

– Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, затверджена Постановою Кабінету Міністрів України;

– Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, у Міністерстві економіки України, затверджена наказом міністерства «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави у Міністерстві економіки України» від 18 травня 1999 р. № 67-ДСК;

– НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджені наказом Держспецзв'язку «Про затвердження і введення в дію нормативних документів» від 28 квітня 1999 р. № 22;

– НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу, затверджена наказом Держспецзв'язку від 28 квітня 1999 р. № 22;

– НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджені наказом Держспецзв'язку від 28 квітня 1999 р. № 22.

В окремих випадках за погодженням з управлінням інформаційних технологій дозволяється для виходу до глобальної комп'ютерної мережі користуватися індивідуальними факс-модемами, приєднаними до розеток міської телефонної мережі. Якщо через факс-модем здійснюється вихід до Інтернету, то, крім дотримання цієї Інструкції, необхідно дотримуватися вимог чинних нормативних документів щодо визначення провайдера.

Для захисту інформації, що є власністю держави, користувачу забороняється обробляти або зберігати на комп'ютері, що входить до автоматизованої системи, такі види інформації:

– з грифом «Для службового користування»;

– внутрішні організаційно-розпорядчі документи (накази, доручення, службові записки, протоколи засідань, акти тощо);

– документи щодо кадрової політики міністерства;

– документи бухгалтерського обліку і звітності, інші фінансові документи щодо господарської діяльності міністерства, документи, у яких віддзеркалена матеріальна база міністерства;

– юридичні документи щодо господарської діяльності міністерства;

– документи, що містять конфіденційну інформацію, яка належить контрагентам міністерства;

– документи щодо майбутніх переговорів з іноземними представниками;

– тези виступів керівництва міністерства;

– інші матеріали, безконтрольне розповсюдження яких за межами міністерства не є доцільним.

На комп'ютерах, котрі не входять до автоматизованої системи, зазначені вище види інформації дозволяється обробляти і зберігати без обмежень. При обробленні конфіденційної інформації з грифом «Для службового користування» необхідно користуватися Інструкцією про порядок обліку, зберігання і ви-

користання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, у Міністерстві економіки України. Додатково до вимог цієї Інструкції рекомендовано конфіденційну інформацію зберігати в окремій комп'ютерній «папці» (розділі), доступ до якої з боку інших користувачів локальної мережі програмно заборонено.

Для запобігання несанкціонованого доступу інших співробітників міністерства до комп'ютерів автоматизованої системи, що може призвести до оброблення на них недозволеної інформації, користувач для входу до операційної системи має використовувати персональні паролі.

Положення Інструкції не поширюються на роботи, які пов'язані з обробленням інформації, що становить державну таємницю, а також інформації, що має криптографічний захист.

Запобігання розголошенню відомостей, що містяться в документах з грифом «Для службового користування», та випадкам втрат таких документів покладається на режимно-секретні підрозділи організацій.

Служба безпеки здійснює контроль за обігом документів, які містять конфіденційну інформацію, що є власністю держави.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» визначає порядок доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її власника в порядку, встановленому законом. Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Власник системи, у якій обробляється інформація, котра є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Останнім часом в Україні для забезпечення прозорості діяльності органів державної влади та виключення можливостей необґрунтованого обмеження права громадян на інформацію зроблено певні кроки. Указом Президента України «Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади» від 1 серпня 2002 р. № 683/2002 Кабінету Міністрів України доручається підготувати та внести в установленому порядку пропозиції щодо вдосконалення діяльності в інформаційній сфері та проекти відповідних нормативно-правових актів, у яких, зокрема, передбачити вичерпний перелік видів інформації, вільне збирання, зберігання, використання і поширення якої в будь-який спосіб може бути обмежено в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров’я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя та вдосконалення порядку здійснення контролю за наданням такої інформації.

У сучасному конституційному законодавстві вживають два поняття *«посадова особа»* і *«службова особа»*. Найбільш поширене вживання цих понять відмічається в таких сферах права, як кримінальне та адміністративне право, і, відповідно, у зазначених галузях законодавства.

В адміністративному праві посадовими особами вважаються лише державні службовці державних органів та їхнього апарату, оскільки вчені розглядають правовий статус посадової особи як учасника управлінських відносин.

У кримінальному праві застосовується широке розуміння поняття «посадова особа», де посадова особа є суб'єктом, протиправні дії якого мають суспільну небезпеку.

Крім поняття «посадова особа», в українському законодавстві існує термін «службова особа»[45], який використовується в КК України, що спричинило певні проблеми в практиці реалізації законодавства.

Гостро постала проблема співвідношення понять посадової особи і службової особи після прийняття Закону України «Про державну податкову службу» (ст. 25) та Конституції України (статті 40, 56), де ці поняття вживаються одночасно, однак немає їх чіткого розмежування.

У зв'язку з цим Верховною Радою України було прийнято Закон України «Про внесення змін і доповнень до деяких законодавчих актів України щодо відповідальності посадових осіб» від 11 липня 1995 р. № 282/95-ВР, у якому зазначено, що в КПК України і КУпАП слова «службова особа» у всіх відмінках заміняються словами «посадова особа» у відповідних відмінках.

Відповідно до п. 3 Постанови Пленуму Верховного Суду України «Про судову практику у справах про перевищення влади або службових повноважень» від 26 грудня 2003 р. № 15, при вирішенні питання про те, чи є особа службовою, належить керуватися правилами, що викладені в примітках 1 і 2 до ст. 364 КК України.

Зазначена примітка до ст. 364 до службових осіб відносить дві категорії осіб:

– особи, які здійснюють функції представників влади;

– особи, які виконують організаційно-розпорядчі[46] чи адміністративно-господарські[47] обов'язки або виконують такі обов'язки за спеціальним повнова-

[45] Особа є службовою не тільки тоді, коли вона здійснює відповідні функції чи виконує обов'язки постійно, а й тоді, коли вона робить це тимчасово або за спеціальним повноваженням, за умови, що зазначені функції чи обов'язки покладені на неї правомочним органом або правомочною службовою особою.

женням в установах, організаціях та на підприємствах як державної, так і недержавної форми власності.

Діяльність та поведінка службових осіб повинні відповідати вимогам моральних принципів суспільства, а тому мають здійснюватися на засадах законності, неприпустимості порушення меж компетенції при виконанні своїх службових обов'язків. Гарантією виконання зазначених вимог службовою особою є визнання власного обов'язку збереження честі і гідності, зміцнення власної репутації, підвищення авторитету державної служби.

3.2. Професійна таємниця

3.2.1. Поняття і сутність професійної таємниці

Існують певні загальні *критерії*[48]*, за якими інформація може бути віднесена до професійної таємниці*:

– інформація довірена або стала відомою особі виключно через виконання нею своїх професійних обов'язків;

– особа, якій довірено інформацію, не перебуває на державній або муніципальній службі (в іншому випадку інформація вважається службовою таємницею);

– заборону на поширення довіреної або такої, що стала відомою, інформації, яка може зашкодити правам або законним інтересам довірителя, встановлено законом;

– інформація не належить до відомостей, що становлять державну або комерційну таємницю.

Сукупність правових норм, що регулюють професійну діяльність, утворює окремий правовий інститут або галузь законодавства. Належність до подібного виду професійної діяльності обумовлює наявність у її суб'єкта специфічних прав та обов'язків.

---

[46] Організаційно-розпорядчі обов'язки – це обов'язки зі здійснення керівництва галуззю промисловості, трудовим колективом, ділянкою роботи, виробничою діяльністю окремих працівників на підприємствах, в установах чи організаціях, незалежно від форми власності.

[47] Адміністративно-господарські обов'язки – це обов'язки з управління або розпорядження державним, колективним чи приватним майном (установлення порядку його зберігання, перероблення, реалізації, забезпечення контролю за цими операціями тощо).

[48] Бачило И. Л. Информационное право / И. Л. Бачило, В. Н. Лопатин, М. А. Федотов ; под ред. акад. РАН Б. Н. Топорнина. – СПб. : Юрид. центр Пресс, 2001. – С. 538.

Особливістю правового регулювання професійних таємниць уважається те, що відповідні правила поведінки своїм виникненням зобов'язані не загальнолюдським моральним нормам, а нормам корпоративної моралі (професійної етики) і виникли в процесі здійснення того чи іншого виду діяльності.

3.2.2. Законодавче обмеження доступу до інформації в інтересах правосуддя та судочинства

Згідно зі ст. 10 Конвенції про захист прав людини і основних свобод 1950 р., передбачається встановлення законодавчого обмеження доступу до інформації, яке необхідне для підтримання авторитету і безсторонності правосуддя.

В Основних принципах незалежності судових органів, схвалених резолюціями № 40/32 та № 40/146 Генеральної Асамблеї від 29 листопада та 13 грудня 1985 р., підкреслюється, що незалежність судових органів гарантується державою і закріплюється в конституції або законах країни. Правосуддя вимагає, щоб кожен мав право на справедливий і публічний розгляд у компетентному, незалежному та об'єктивному суді відповідно до принципів, проголошених в Загальній декларації прав людини (ст. 10), Міжнародному пакті про громадянські й політичні права (ст. 14) та в інших документах Організації Об'єднаних Націй.

Згідно з цими принципами (п. 15) *судді зобов'язані зберігати професійну таємницю щодо своєї роботи та конфіденційної інформації*, отриманої в ході виконання ними своїх обов'язків, за винятком відкритих судових розглядів, і їх не можна примушувати давати свідчення з таких питань.

Керівні принципи, що стосуються ролі осіб, які здійснюють судове переслідування, прийняті восьмим Конгресом ООН 27 серпня – 7 вересня 1990 р. з попередження злочинності і поводження з правопорушниками, зазначають, що судді зберігають професійну таємницю, якщо тільки виконання їх обов'язків або з міркувань правосуддя не потребують іншого. Це є забезпеченням незалежності і виключенням впливу на судові органи при прийнятті ними рішень. Такий вид конфіденційної інформації розглядається як професійна таємниця судді.

Згідно з нормами ст. 127 Конституції України, правосуддя здійснюють професійні судді та у визначених законом випадках народні засідателі і присяжні, відповідно, подібний обов'язок поширюється не лише на осіб, які є професійними суддями.

В українському законодавстві існують процесуальні норми, якими регулюється питання конфіденційності інформації з метою неупередженості судочинства.

Згідно зі ст. 20 КПК України, розгляд справ у всіх судах відкритий, за винятком випадків, коли це суперечить інтересам охорони державної таємниці або іншої захищеної законом таємниці. Згідно із ЗВДТ, відомості про зміст кримінальних справ, розголошення яких може завдати шкоди національній безпеці України, мають гриф «Таємно» зі строком засекречення до 5 років.

Крім того, *закритий судовий розгляд допускається за мотивованою ухвалою суду*:

– у справах про злочини осіб, які не досягли шістнадцятирічного віку;

– у справах про статеві злочини;

– в інших справах з метою запобігання розголошенню відомостей про інтимні сторони життя осіб, які беруть участь у справі;

– в інших справах, коли цього потребують інтереси безпеки осіб, взятих під захист.

Відповідно до ст. 322 КПК України, яка встановлює «таємницю наради суддів», вирок постановляється в окремому приміщенні – нарадчій кімнаті. Під час наради і постановлення вироку в нарадчій кімнаті можуть бути лише судді, які входять до складу суду в даній справі. Присутність у нарадчій кімнаті запасних суддів або секретаря судового засідання та інших осіб не допускається. Важливою є вимога, згідно з якою судді не мають права розголошувати міркування, що висловлювалися в нарадчій кімнаті. З настанням нічного часу суд має право перервати нараду для відпочинку.

Аналогічні вимоги містяться у ст. 196 Цивільного процесуального кодексу України:

– під час ухвалення судового рішення ніхто не має права перебувати в нарадчій кімнаті, крім складу суду, який розглядає справу;

– під час перебування в нарадчій кімнаті суддя не має права розглядати інші судові справи;

– судді не мають права розголошувати хід обговорення та ухвалення рішення.

У ст. 6 ЦПК України зазначається, що закритий судовий розгляд допускається, якщо:

– відкритий розгляд може привести до розголошення державної або іншої таємниці, яка охороняється законом, а також за клопотанням осіб, які беруть участь у справі, з метою забезпечення таємниці усиновлення, запобігання розголошенню відомостей про інтимні чи інші особисті сторони життя осіб, які беруть участь у справі, або відомостей, що принижують їх честь і гідність;

– особисті папери, листи, записи телефонних розмов, телеграми та інші види кореспонденції можуть бути оголошені в судовому засіданні тільки за згодою осіб, визначених ЦК України. Це правило застосовується при дослідженні звуко- і відеозаписів такого самого характеру.

Розгляд справи в закритому судовому засіданні проводиться з додержанням усіх правил цивільного судочинства. Про розгляд справи в закритому судовому засіданні суд зобов'язаний постановити мотивовану ухвалу в нарадчій кімнаті, яка оголошується негайно. Рішення суду оголошується прилюдно, крім випадків, коли розгляд проводився в закритому судовому засіданні. У справах про усиновлення дозволяється не оголошувати прилюдно рішення суду.

Наприклад, розгляд судом справ про розкриття банками інформації, яка містить банківську таємницю, щодо юридичних та фізичних осіб розглядається в п'ятиденний строк з дня надходження заяви в закритому судовому засіданні з повідомленням заявника, особи, щодо якої вимагається розкриття банківської таємниці, та банку, а у випадках, коли справа розглядається з метою охорони державних інтересів та національної безпеки, – з повідомленням тільки заявника.

Розгляд справ у господарських судах відкритий, за винятком випадків, коли це суперечить вимогам щодо охорони державної, комерційної або банківської таємниці, або коли сторони чи одна зі сторін обґрунтовано вимагають конфіденційного розгляду справи і подають відповідне клопотання до початку розгляду справи по суті (ст. 4-4 Господарського процесуального кодексу України).

На відміну від норм КПК України та ЦПК України, у господарському процесі таємниці наради суддів не встановлено. Рішення викладається в письмовій формі та підписується всіма суддями, які брали участь у засіданні. У разі розгляду справи трьома суддями суддя, не згодний з рішенням, зобов'язаний викласти в письмовій формі свою окрему думку, що приєднується до справи. А це суперечить принципам міжнародно-правових актів.

Відповідно до ст. 7 Закону України «Про доступ до судових рішень» від 22 грудня 2005 р. № 3262-IV, у текстах судових рішень, що відкриті для загального доступу через оприлюднення на офіційному веб-порталі судової влади або офіційне опублікування, не можуть бути розголошені відомості, що дають можливість ідентифікувати фізичну особу. Такі відомості замінюються літерними або цифровими позначеннями.

До відомостей, зазначених у ч. 1 цієї статті, належать:

– імена (ім'я, по батькові, прізвище) фізичних осіб;

– адреси місця проживання або перебування фізичних осіб, номери телефонів чи інших засобів зв'язку, адреси електронної пошти, ідентифікаційні номери (коди);

– реєстраційні номери транспортних засобів;

– інша інформація, що дає можливість ідентифікувати фізичну особу.

До відомостей, зазначених у ч. 1–2 цієї статті, не належать:

– прізвища та ініціали суддів, які ухвалили судове рішення;

– імена посадових чи службових осіб, які, виконуючи свої повноваження, беруть участь у цивільній, господарській, адміністративній чи кримінальній справах, справах про адміністративні правопорушення (проступки).

У текстах судових рішень, відкритих для загального доступу відповідно до цього Закону, не можуть бути розголошені відомості, для забезпечення нерозголошення яких було прийнято рішення про розгляд справи в закритому судовому засіданні.

Інформація, внесена до Єдиного державного реєстру судових рішень[49] (ст. 8), повинна мати захист від її викрадення, перекручення чи знищення, не допускається вилучення судових рішень із Реєстру, не допускається внесення будь-яких змін до судових рішень, які внесені до Реєстру, крім випадків, що пов'язані з необхідністю виправлення помилки, допущеної під час внесення судового рішення до Реєстру чи ведення Реєстру, у разі виправлення судового рішення відповідно до процесуального закону його текст у Реєстрі не змінюється.

До Реєстру додатково вноситься судове рішення, яким внесено зміни до відповідного судового рішення.

На відміну від кримінального законодавства, цивільне і господарське трохи інакше тлумачать принцип гласності судочинства, надаючи учасникам процесу широких прав щодо відходу від названого принципу з метою захисту особистої або конфіденційної інформації.

У таких випадках до залу засідань допускаються лише особи, які беруть участь у справі, а також у разі необхідності свідки, експерти та перекладачі. Окреме положення стосується того, що не допускаються громадяни молодші 16 років, які не беруть участі у справі або не є свідками.

Ситуація з іншим типом конфіденційної інформації – таємницею слідства – відрізняється від описаної вище.

Нормами ст. 52-1 КПК України встановлено вимогу щодо нерозголошення відомостей про особу, щодо якої здійснюються заходи безпеки.

Нерозголошення відомостей про особу, взяту під захист, може забезпечуватися шляхом обмеження відомостей про неї в матеріалах перевірки (заявах,

[49] Законом України «Про доступ до судових рішень» регулюються відносини щодо забезпечення доступу до судових рішень (рішень, судових наказів, постанов, вироків, ухвал), ухвалених судами загальної юрисдикції, та ведення Єдиного державного реєстру судових рішень. Забезпечується постійне внесення до Єдиного державного реєстру судових рішень електронних копій судових рішень Верховного Суду України, вищих спеціалізованих судів, апеляційних та місцевих адміністративних судів, апеляційних та місцевих господарських судів, апеляційних загальних судів, а також внесення судових рішень місцевих загальних судів до 1 січня наступного року.

поясненнях тощо), а також протоколах слідчих дій та судових засідань. Орган дізнання, слідчий, прокурор, суд (суддя), прийнявши рішення про застосування заходів безпеки, виносить мотивовану постанову, ухвалу про заміну прізвища, імені, по батькові особи, взятої під захист, на псевдонім. Надалі в процесуальних документах зазначається лише псевдонім (ст. 52-3 КПК України).

У випадку застосування подібних заходів безпеки заборонено розголошувати особисту інформацію, за допомогою якої можна ідентифікувати особу, щодо якої застосовано заходи безпеки. Стаття 52-3 КПК України до такої інформації відносить:

– справжні прізвище, ім'я, по батькові;

– рік, місяць і місце народження;

– сімейний стан;

– місце роботи;

– рід занять або посада;

– місце проживання;

– інші анкетні дані, що містять інформацію про особу, яка перебуває під захистом.

Зазначені дані вказуються лише в постанові (ухвалі) про заміну анкетних даних. Ця постанова (ухвала) до матеріалів справи не долучається, а зберігається окремо в органі, у провадженні якого перебуває кримінальна справа. У разі заміни прізвища особи, взятої під захист, на псевдонім з матеріалів справи вилучаються протоколи слідчих дій та інші документи, у яких зазначено достовірні відомості про цю особу, і зберігаються окремо, а до матеріалів справи додаються копії цих документів із заміною справжнього прізвища на псевдонім.

Відомості про заходи безпеки та осіб, взятих під захист, є інформацією з обмеженим доступом. На документи, що містять таку інформацію, не поширюються норми щодо процесуальних прав захисника (ч. 2 ст. 48 КПК України), ознайомлення деяких учасників процесу з матеріалами справи (статті 217–219 КПК України) і забезпечення права на ознайомлення з матеріалами справи (ст. 255 КПК України).

В українському законодавстві відносно такої інформації існують деякі розбіжності: ст. 52-3 КПК України визначає цю інформацію як інформацію з обмеженим доступом; цю ж інформацію включено до Зводу відомостей, що становлять державну таємницю (згідно із ЗВДТ, відомості про осіб, які беруть участь у кримінальному судочинстві і взяті під захист згідно з чинним законодавством України, носять гриф «Цілком таємно» зі строком засекречення 10 років).

Статтею 121 КПК України встановлюється недопустимість розголошення даних досудового слідства. Передбачено, що дані досудового слідства можуть бути оприлюднені тільки з дозволу слідчого або прокурора і в тому обсягу, у якому вони визнають можливим.

У необхідних випадках слідчий попереджає свідків, потерпілого, цивільного позивача, цивільного відповідача, захисника, експерта, спеціаліста, перекладача, понятих, а також інших осіб, присутніх при провадженні слідчих дій, про обов'язок не розголошувати без його дозволу дані досудового слідства. Винні в розголошенні даних досудового слідства несуть кримінальну відповідальність за ст. 387 КК України.

У випадках, коли розголошення може завдати шкоди національній безпеці України, на дані досудового слідства відповідно до ЗВДТ поширюються вимоги Закону України «Про державну таємницю». Важливим питанням, яке може істотно вплинути на хід кримінального провадження, завдати шкоди правам, свободам і законним інтересам учасників кримінального судочинства, стати на заваді встановлення обставин, що підлягають доказуванню і мають значення для кримінального провадження є розголошення відомостей, одержаних під час досудового розслідування. Щоб запобігти цьому законом встановлена заборона розголошувати такі відомості, а в разі необхідності окремі відомості можна розголосити лише з дозволу слідчого або прокурора.

Нерозголошення відомостей (даних) досудового розслідування (дізнання і досудового слідства) є однією з умов, які сприяють успішному розкриттю злочину і викриттю винного.

Передчасне їх розголошення може негативно вплинути на хід досудового провадження у справі, дати можливість винному приховати або знищити сліди злочину, речі (предмети) і документи, що можуть бути джерелами доказів, сфальсифікувати докази, ухилитися від слідства і суду, погрожувати або завдати шкоди підозрюваному та іншим співучасникам, потерпілому, свідкам-очевидцям та іншим особам.

У процесі досудового розслідування слідчий особисто зобов'язаний дотримуватись таємниці досудового провадження і вимагати цього від інших суб'єктів. Поняття таємниці досудового розслідування (слідства) в законі не визначено.

Розголошення даних досудового розслідування допускається лише у визначеному обсязі, за умови, що розголошення не суперечить інтересам досудового розслідування і не пов'язане з порушенням прав і законних інтересів учасників кримінального судочинства, а розголошення відомостей про приватне життя учасників кримінального судочинства третім особам або засобам масової інформації можливе лише у виняткових випадках і лише за згодою (у письмовій формі і долучається до матеріалів справи) тієї особи, якої вони стосуються.

Відомості досудового розслідування, згідно з ч. 1 ст. 222 Кримінального процесуального кодексу України, можна оголосити лише з дозволу слідчого або прокурора, і в тому обсязі, в якому вони визнають можливим. При цьому слідчий, прокурор повинні обов'язково визначити, які відомості (дані) і у якому обсязі можна розголосити, з урахуванням можливого настання негативних наслідків, оскільки чинним законом межі розголошення відомостей не встановлені.

Прийняття рішення щодо розголошення окремих відомостей досудового розслідування є відповідальним кроком особи, що здійснює кримінальне провадження, оскільки не можна повністю виключити настання негативних наслідків такого рішення. Тому ми переконані, що таке рішення повинна приймати лише одна особа – слідчий. Згідно з ч. 5 ст. 40 КПК України слідчий є самостійним у своїй процесуальній діяльності але закон не визначає межі такої самостійності, тобто не встановлює чіткого переліку процесуальних рішень, які слід-

чий має право приймати самостійно і в разі настання негативних наслідків нести за це особисту відповідальність, передбачену законом.

У законі (ч. 2 ст. 36 КПК України) передбачено, що прокурор здійснює нагляд за додержанням законів у процесі досудового розслідування у формі процесуального керівництва. Отже, прокурор здійснює одночасно дві функції: нагляд за додержанням законності і керівництво досудовим розслідуванням, що здійснює слідчий. Враховуючи це, рішення слідчого про розголошення окремих відомостей, на наш погляд, має бути узгоджене з прокурором. З метою попередження розголошення відомостей (даних) досудового провадження важливе значення має поняття і структура механізму нерозголошення.

Слід мати на увазі, що згідно зі ст. 28 Закону України «Про інформацію» за режимом доступу до інформації, вона поділяється на відкриту та з обмеженим доступом. Інформація з обмеженим доступом за своїм правовим режимом у свою чергу поділяється на конфіденційну і таємну. Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов (ч. 2 ст. 30 Закону України). До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі (ч. 7 ст. 30 Закону України). Така інформація є державною таємницею, згідно «Зводу відомостей, що становлять державну таємницю» (далі – ЗВДТ). Отже, якщо дані досудового розслідування відносяться до категорії державної таємниці, то їх розголошення навіть з дозволу слідчого або прокурора буде незаконним. У цьому контексті йдеться про поширення з дозволу зазначених службових осіб лише обмеженої інформації, яка на період досудового розслідування відноситься до категорії конфіденційної.

Обмеження доступу до інформації здійснюється відповідно до Закону України «Про доступ до публічної інформації» при дотриманні сукупності таких вимог:

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

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Законом України «Про оперативно-розшукову діяльність» передбачено нерозголошення відомостей про особу, щодо якої здійснюють заходи безпеки. Ця інформація відповідно до пунктів 4.1.4. і 4.1.6. Зводу відомостей є державною таємницею. Коли згідно закону, стосовно свідка прийнято рішення про зміну його анкетних даних на псевдонім, а він бере участь у провадженні окремих слідчих дій за участю інших суб'єктів процесу, необхідно застосовувати відповідні заходи забезпечення його безпеки (наприклад, впізнання поза візуальним спостереженням того, кого впізнають; застосування засобів маскування тощо), а з метою нерозголошення відомостей про таких осіб від інших учасників слідчої дії в обов'язковому порядку необхідно відбирати письмові зобов'язання (розписку) про нерозголошення таких даних.

У разі розголошення відомостей про заходи безпеки, щодо особи, взятої під захист, службовою особою, якою прийнято рішення про ці заходи, особою, яка їх здійснює, або службовою особою, якій ці рішення стали відомі у зв'язку з її службовим становищем, а так само особою, взятою під захист, якщо ці дії спричинили шкоду здоров'ю особи, взятої під захист її смерть або інші тяжкі наслідки винні особи підлягають кримінальній відповідальності за ст. 381 Кримінального кодексу України (далі – КК). Законом не визначено вичерпного переліку наслідків розголошення відомостей щодо заходів безпеки.

В окремих випадках КПК України від 28.12.1960 р. (ст. 185 КПК України) зобов'язував слідчого вживати заходів щодо нерозголошення окремих даних, отриманих під час розслідування злочину. Зокрема, закон передбачав, що слід-

чий повинен вживати заходів до того, щоб не були розголошені виявлені під час обшуку або виїмки обставини особистого життя обшукуваного та інших осіб, які проживають або тимчасово перебувають у цьому приміщенні.

Згідно з частиною 2 ст. 121 КПК України у необхідних випадках слідчий, особа, яка провадить дізнання чи прокурор попереджають свідків, потерпілого, цивільного позивача, цивільного відповідача, захисника, експерта, спеціаліста, перекладача, понятих, а також інших осіб, які присутні під час провадження слідчих дій, про обов'язок не розголошувати без їхнього дозволу даних досудового слідства або дізнання. Винні в розголошенні даних досудового слідства або дізнання несуть кримінальну відповідальність за статтею 387 КК України.

Кримінальна відповідальність передбачена за розголошення без дозволу прокурора, слідчого або особи, яка провадила оперативно-розшукову діяльність, даних оперативно-розшукової діяльності або досудового розслідування особою, попередженою в установленому законом порядку про обов'язок не розголошувати такі дані (ч. 1 ст. 387 КК України).

Згідно з ч. 2 ст. 387 КК України, передбачена кримінальна відповідальність за розголошення даних оперативно-розшукової діяльності, досудового розслідування, вчинене суддею, прокурором, слідчим, працівником оперативно-розшукового органу незалежно від того, чи приймала ця особа безпосередню участь в оперативно-розшуковій діяльності, досудовому розслідуванні, якщо розголошені дані ганьблять людину, принижують її честь і гідність.

Закон не передбачає обов'язкової письмової форми попередження слідчим (прокурором; особою, яка провадить дізнання) осіб, які брали участь у провадженні слідчих дій або були присутніми при цьому, про обов'язок не розголошувати без його дозволу даних досудового слідства.

У процесуальній літературі сформульована думка, про те, що попередження про недопустимість розголошення і дозвіл на розголошення (якщо такий було надано) доцільно фіксувати в протоколі певної слідчої (розшукової) дії, результати якої слідчий, прокурор забороняє розголошувати, або в окремому протоколі чи іншому документі. Крім того, на нашу думку, у таких випадках

необхідно відбирати розписку від суб'єктів процесу, яких попереджено про недопустимість розголошення таких даних та кримінальну відповідальність згідно зі статтею 387 КК України.

Складені документи мають істотне юридичне значення під час вирішення питання щодо притягнення винної особи до кримінальної відповідальності у разі порушення визначеної законом заборони.

У випадках, коли розголошення може завдати шкоди національній безпеці України, на дані досудового слідства відповідно до ЗВДТ поширюються вимоги Закону України «Про державну таємницю».

3.2.3. Комерційна таємниця

Визнання права приватної власності, відмова держави від монополії у сфері управління економікою спричинили появу значної кількості суб'єктів підприємницької діяльності. Одночасно з новими економічними відносинами з'явилися нові економічні правопорушення – недобросовісна конкуренція. А тому постало питання захисту комерційної таємниці.

Питання захисту комерційної таємниці, по суті, не є питанням захисту інформаційної безпеки, оскільки сам по собі інститут комерційної таємниці ґрунтується не на прямих вказівках закону, а на праві власності на ті чи інші відомості. Доступ до цієї інформації означає набуття певних матеріальних благ.

Згідно з ч. 1 ст. 36 ГК України, «відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, що не є державною таємницею, розголошення яких може завдати шкоди інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею. Склад і обсяг відомостей, що становлять комерційну таємницю, спосіб їх захисту визначається суб'єктом господарювання відповідно до закону».

Режим доступу до комерційної інформації визначається правом власності на цю інформацію. Законодавством України встановлені обмеження щодо таких відомостей. По-перше, ця інформація не є власністю держави в особі органів державної влади, а належить фізичним та юридичним особам – суб'єктам підприємницької діяльності. По-друге, склад і обсяг відомостей, що не становлять

комерційну таємницю, визначається Постановою Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці» від 9 серпня 1993 р. № 611. Ці відомості використовуються при проведенні перевірок контролюючими органами, аудиторами для проведення аудиту, при підготовці звітності в різні фонди.

Комерційну таємницю не становлять:

– установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами;

– інформація за всіма встановленими формами державної звітності;

– дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;

– відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;

– документи про сплату податків і обов'язкових платежів;

– інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;

– документи про платоспроможність;

– відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю;

– відомості, що відповідно до чинного законодавства підлягають оголошенню.

Слід зауважити, що дані відомості не є відкритими і загальнодоступними. Однак передбачено, що підприємства зобов'язані подавати перелічені у відповідній Постанові Кабінету Міністрів відомості органам державної виконавчої влади, контролюючим і правоохоронним органам, іншим юридичним особам відповідно до чинного законодавства на їхню вимогу, що є гарантією забезпечення поінформованості державних органів та громадськості про важливі аспе-

кти їхньої діяльності, а це гарантує як виконання державою своїх контрольних та фіскальних функцій, так і забезпечення прав окремих осіб та інтересів суспільства, маючи значення для інформаційної безпеки в цілому.

Для здійснення прокурорського нагляду, відповідно до ст. 20 Закону України «Про прокуратуру» від 5 листопада 1991 р. № 1789-XII, підприємства, установи та організації повинні надавати прокурору свою документацію, у тому числі за його письмовим запитом, відомості, що складають комерційну таємницю, а у випадку необхідності прокурор має право затребувати передання для перевірки вказаних документів у прокуратуру.

Термін «комерційна таємниця» ототожнюють з терміном «конфіденційна інформація». Норми Закону України «Про інформацію» прямо вказують на право власності на конфіденційну інформацію як правову основу її захисту. Виходячи з положень ч. 1 ст. 30 Закону України «Про інформацію» (конфіденційна інформація знаходиться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб), ч. 1 ст. 162 ГК України (суб'єкт господарювання, що є володільцем технічної, організаційної або іншої комерційної інформації, має право на захист від незаконного використання цієї інформації третіми особами, за умов, що ця інформація має комерційну цінність у зв'язку з тим, що вона не відома третім особам, і до неї немає вільного доступу інших осіб на законних підставах, а володілець інформації вживає належних заходів до охорони її конфіденційності), інформація, що становить комерційну таємницю, може перебувати або в приватній, або в колективній власності, або в оперативному розпорядженні державних підприємств, установ та організацій.

Тільки власник може визначити перелік відомостей, що підлягають розголошенню, встановлювати випадки і осіб, через яких може здійснюватися таке розголошення, що вважається з точки зору права правомірним. Вимога нерозголошення комерційної таємниці має подвійну направленість: внутрішню і зовнішню. Внутрішня спрямована на працівників суб'єкта підприємницької діяльності, зовнішня – на службових осіб організацій та установ, які проводять перевірку підприємства.

Незаконні дії щодо комерційної таємниці спричинять руйнівний вплив на одну з найважливіших сфер суспільного життя – господарську, що загрожує нормальному існуванню суспільства, його позитивному розвитку. На цю небезпеку вказано в Резолюції Шостого конгресу ООН, а Сьомий конгрес ООН відніс економічні злочини до особливо небезпечних та висунув вимогу про посилення боротьби з ними.

Згідно з ч. 3 ст. 36 ГК України, «*розголошенням комерційної таємниці* є ознайомлення іншої особи без згоди особи, уповноваженої на те, з відомостями, що відповідно до закону становлять комерційну таємницю, особою, якій ці відомості були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків, якщо це завдало чи могло завдати шкоди суб'єкту господарювання».

Способами розголошення відомостей, що становлять комерційну таємницю, можуть бути:

– передання інформації конкурентам підприємця;

– ознайомлення з комерційною таємницею службових осіб державних організацій та органів без належних на те прав і підстав як із боку розголошувача, так і з боку державного службовця;

– розголошення відомостей, що складають комерційну інформацію, через засоби масової інформації;

– використання в особистих цілях – передання родичам, знайомим для заняття власною підприємницькою діяльністю;

– схилення до розголошення комерційної таємниці.

Мотиви розголошення можуть бути різноманітними й частину їх можна віднести до «вічних»: користь, помста, безвідповідальне ставлення до службових і трудових обов'язків. У певних умовах мотивами визнаються наміри, що є відносно стійкими утвореннями й формуються в стані холодного розуму і розрахунку. Обов'язковою ознакою порушення конкурентного законодавства у вигляді розголошення комерційної таємниці є наявність шкоди, завданої підприємцю таким розголошенням.

За вчинення дій, визначених законодавцем як неправомірне використання комерційної таємниці (ч. 5 ст. 36 ГК України), «неправомірне збирання, розголошення або використання відомостей, що є комерційною таємницею» (ч. 6 ст. 36 ГК України), винні особи несуть відповідальність у вигляді накладання Антимонопольним комітетом України штрафів, а також адміністративну, цивільну та кримінальну відповідальність у випадках, визначених законодавством.

Службовці державних установ і органів, які проводять перевірки підприємця, отримують доступ до комерційної таємниці на основі відповідних актів державних органів і установ. Інформацію стосовно комерційної таємниці підприємця вони отримують у рамках адміністративних правовідносин. Об'єм їхнього доступу до інформації обмежується в документах на перевірку.

За розголошення комерційної таємниці службовці державних органів і установ несуть відповідальність, встановлену законодавством України. Загальним підґрунтям такої відповідальності є ГК України.

Законом України «Про державну податкову службу в Україні» від 4 грудня 1990 р. № 509-XII передбачені зобов'язання щодо дотримання службовою особою державної податкової служби комерційної і службової таємниці. За невиконання або неналежне виконання своїх обов'язків посадові особи притягаються до дисциплінарної, адміністративної, кримінальної та матеріальної відповідальності згідно з чинним законодавством (ст. 13).

Адміністративна відповідальність за порушення, що пов'язані з комерційною таємницею, встановлюється за отримання, використання, розголошення комерційної таємниці (ст. 164-3 КУпАП).

Законом України «Про захист від недобросовісної конкуренції» від 7 червня 1996 р. № 236/96-ВР передбачена відповідальність:

– статтею 16 – за неправомірне збирання комерційної таємниці, яким уважається добування протиправним способом відомостей, що відповідно до законодавства України становлять комерційну таємницю, якщо це завдало чи могло завдати шкоди суб'єкту господарювання;

– статтею 17 – за розголошення комерційної таємниці, яким є ознайомлення іншої особи без згоди особи, уповноваженої на те, з відомостями, що відповідно до чинного законодавства України становлять комерційну таємницю, особою, якій ці відомості були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків, якщо це завдало чи могло завдати шкоди господарюючому суб'єкту господарювання;

– статтею 18 – за схилення до розголошення комерційної таємниці, яким є спонукання особи, якій були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків відомості, що відповідно до законодавства України становлять комерційну таємницю, до розкриття цих відомостей, якщо це завдало чи могло завдати шкоди господарюючому суб'єкту господарювання;

– статтею 19 – за неправомірне використанням комерційної таємниці, яким є впровадження у виробництво або врахування під час планування чи здійснення підприємницької діяльності без дозволу уповноваженої на те особи відомостей, що становлять відповідно до законодавства України комерційну таємницю.

Кримінальним кодексом України передбачена відповідальність за злочинні дії, що пов'язані з порушенням вимог охорони комерційної таємниці: незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231), розголошення комерційної або банківської таємниці (ст. 232).

Законодавство України, гарантуючи право підприємства на комерційну таємницю і її захист, певною мірою регулює і питання юридичної відповідальності за правопорушення в цій сфері.

За порушення законодавства про комерційну таємницю встановлені такі види відповідальності: кримінальна; цивільно-правова; адміністративна; дисциплінарна.

Суб'єктом незаконного використання відомостей, що містять комерційну таємницю, може бути особа, яка досягла 16-річного віку.

Порушувати кримінальні справи за фактами комерційного шпигунства або розголошення комерційної таємниці відповідно до ст. 4 Кримінально-процесуального кодексу України мають право суд, прокуратура на підставі заяви потерпілої сторони. Відповідно до ст. 49 КПК України потерпілою особою (юридичною або фізичною) визначається та, у відношенні до якої порушене право на комерційну таємницю і якій завдано значного матеріального збитку. Ця особа на підставі ст. 50 КПК України вважається і цивільним позивачем.

Розглядаючи питання про кримінальну відповідальність за порушення прав на комерційну таємницю, слід враховувати, що підприємство не може вимагати від державних органів гарантій на захист комерційної таємниці, якщо воно не набуло на це право згідно з встановленим законодавством України порядком.

Цивільно-правовою санкцією є відшкодування збитків, заподіяних внаслідок вчинення дій, визначених законодавством як неправомірне збирання, розголошення та використання комерційної таємниці, підлягають відшкодуванню за позовами заінтересованих осіб у порядку, визначеному Цивільним законодавством України (ст. 255 Господарського кодексу України, ст. 24 Закону України «Про захист від недобросовісної конкуренції»).

Підприємства постійно стикаються з різного роду ревізіями та перевірками окремих аспектів їх господарської та іншої діяльності представниками податкових, аудиторських, контроль-ревізійних, правоохоронних та інших органів, які мають право доступу до інформації, що охороняється. У зв'язку з цим слід зазначити, що ЦК України передбачає відповідальність за шкоду, заподіяну незаконними діями державних і громадських організацій, а також посадових осіб при виконанні ними службових обов'язків в галузі адміністративного управління, і відшкодовується вона на загальних підставах.

Органи державної влади зобов'язані охороняти від недобросовісного комерційного використання інформацію, яка надана їм з метою отримання встановленого законом дозволу на діяльність, пов'язану з фармацевтичними, сільськогосподарськими, хімічними продуктами, що містять нові хімічні сполуки.

Органи влади зобов'язані охороняти комерційну таємницю також в інших випадках, передбачених законом (ст. 507 ЦК України).

Порушення прав на комерційну таємницю передбачено і регулюється двома нормативно-правовими актами: Кодексом про адміністративні правопорушення і Законом України « Про захист від недобросовісної конкуренції». Ст. 1643 Кодексу про адміністративні правопорушення встановлює, що отримання, використання, розголошення комерційної таємниці, а також конфіденційної інформації з метою заподіяння шкоди діловій репутації або майну іншого підприємця становить адміністративне правопорушення і тягне за собою стягнення у вигляді накладання штрафу.

Закон України «Про захист від недобросовісної конкуренції» передбачає адміністративну відповідальність за неправомірне збирання комерційної таємниці (ст. 16), розголошення комерційної таємниці (ст. 17), схилення до розголошення комерційної таємниці (ст. 18), неправомірне використання комерційної таємниці (ст. 19). За вказані правопорушення настає адміністративна відповідальність у вигляді штрафів, які накладаються Антимонопольним комітетом України.

Суб'єктами цих порушень є як юридичні, так і фізичні особи.

Відповідно до Кодексу законів про працю України стосовно штатних співробітників підприємства, що припустили порушення встановлених на підприємстві режиму, порядку і правил збереження комерційної таємниці, можуть застосовуватись такі види стягнень: догана; звільнення; переведення на іншу роботу, не пов'язану з комерційною таємницею; позбавлення премій, передбачених системою оплати праці; зміна часу надання чергової відпустки.

Підстави застосування зазначених дисциплінарних стягнень відповідно до ст. 147 КЗпП України повинні бути чітко передбачені «Положенням про комерційну таємницю підприємства і правил її збереження).

Основною умовою забезпечення збереження комерційної таємниці є персональна відповідальність осіб, яким надано доступ до комерційної таємниці.

Важливо розуміти, що в ринковій економіці інформація є цінним товаром і підпорядковується законам товарно-грошових відносин. Неправомірне заволодіння чужими інформаційними ресурсами з метою їх використання є найбільш небезпечною формою недобросовісної конкуренції. Таким чином, основним питанням проблеми захисту інформації в процесі реалізації комерційної діяльності можна вважати питання визначення змісту відомостей, які є складовими комерційної таємниці, і утворення правового механізму захисту прав власника інформації з врахуванням видів комерційної діяльності.

3.2.4. Банківська таємниця

З моменту проголошення незалежності України її банківська система перебуває в процесі розбудови. Протягом останніх років відбулися істотні зрушення в становленні і розвитку банківського законодавства нашої держави. Етапним моментом стало прийняття Закону України «Про банки і банківську діяльність» від 7 грудня 2000 р. № 2121-III, який у цілому відповідає міжнародним стандартам у сфері банківського регулювання, у тому числі рекомендаціям Базельського комітету з банківського нагляду та директивам Європейського Союзу з питань координації діяльності кредитних установ.

Банк – це юридична особа, яка має виключне право на підставі ліцензії Національного банку України здійснювати в сукупності такі операції: залучення у вклади грошових коштів фізичних і юридичних осіб та розміщення зазначених коштів від свого імені, на власних умовах та на власний ризик, відкриття і ведення банківських рахунків фізичних та юридичних осіб.

Банківська система України складається з Національного банку України та інших банків, що створені і діють на території України відповідно до положень згаданого вище Закону України. Національний банк України здійснює регулювання та банківський нагляд відповідно до положень Конституції України, законів України «Про банки і банківську діяльність», «Про Національний банк України» від 20 травня 1999 р. № 679-XIV, інших законодавчих актів та нормативно-правових актів Національного банку України.

Відповідно до Закону України «Про банки і банківську діяльність» одним з основних пріоритетів регулювання діяльності банків як специфічних господарських утворень, які оперують чужими коштами, є захист прав вкладників та інформації, розголошення якої може завдати шкоди клієнту банку.

У листі Національного банку України від 19 квітня 2001 р. № 18-112/1467-2599 зазначено, що, відповідно до ст. 30 Закону України «Про інформацію», конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюється за їх бажанням відповідно до передбачених ними умов. Юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною за власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Згідно з положеннями ст. 1076 ЦК України та ст. 60 Закону України «Про банки і банківську діяльність», будь-яка інформація, що стосується клієнта, якою банк володіє на законних підставах, є *банківською таємницею* (за винятком, якщо така інформація складає державну таємницю).

Забезпечення банківської таємниці з позиції інформаційного права відповідно до впровадження новітніх інформаційно-комунікаційних технологій здійснюється згідно із Директивою 2015/849 Європейського Парламенту та Ради від 20 травня 2015 року про запобігання використанню фінансової системи для цілей відмивання грошей або фінансування тероризму, що вносить зміни до Регламенту № 648/2012 Європейського Парламенту і Ради, а також скасовує Директиву 2005/60/ЄС Європейського Парламенту і Ради та Директиву Комісії 2006/70/ЄС і Регламенту Комісії 2015/703 від 30 квітня 2015 року, що запроваджує мережевий кодекс правил функціональної сумісності та обміну даними.[50]

[50] Реферативний огляд європейського права (інформаційно-аналітичний дайджест квіт. – черв. 2015 р.) / За заг. ред. В. О. Зайчука. – К.: Ін-т законодавства Верховної Ради України, 2015. – 64 с.

Відповідно до Закону України «Про банки та банківську діяльність» від 7 грудня 2000 р. № 2121-III (у редакції від 06.01.2018 р.) *банківська таємниця* (bank secrecy) – інформація щодо діяльності та фінансового стану клієнта, яка відомою банку в процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту. До банківської таємниці належать відомості та інформація:

– про банківські рахунки клієнтів, зокрема кореспондентські рахунки банків у Національному банку України;

– про операції, проведені на користь чи за дорученням клієнта, та здійснені ним угоди;

– про фінансово-економічний стан клієнтів;

– про системи охорони банку та клієнтів;

– про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності;

– стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;

– щодо звітності банку, за винятком тієї, що підлягає опублікуванню; про коди банків для захисту інформації.

Національні Правила зберігання, захисту, використання та розкриття банківської таємниці повною мірою відповідає стандартам Базельського комітету банківського нагляду.

Зважаючи на норми ч. 1 ст. 60 Закону України, відповідно до яких банківською таємницею є та інформація, розголошення якої може завдати шкоди клієнту банку, до конфіденційної інформації, якою володіють банки, належить будь-яка інформація, неправомірне розголошення якої може завдати шкоди безпосередньо банку. Згідно зі ст. 30 Закону України «Про інформацію», банки самостійно визначають перелік такої інформації. Тому умовою нерозголошення ін-

формації, що становить банківську таємницю, у цьому випадку є віднесення банком останньої до конфіденційної інформації.

Інформація про банки чи клієнтів, що збирається під час проведення банківського нагляду, становить банківську таємницю. Водночас існує перелік інформації, що підлягає обов'язковому опублікуванню. Він встановлюється Національним банком України та додатково самим банком на його розсуд.

Національний банк України видає нормативно-правові акти з питань зберігання, захисту, використання та розкриття інформації, що становить банківську таємницю, та надає роз'яснення щодо застосування таких актів.

Відповідно до ст. 57 Закону України «Про Національний банк України», для здійснення своїх функцій Національний банк має право безоплатно одержувати від банків, банківських об'єднань та юридичних осіб, які отримали ліцензію Національного банку на здійснення окремих банківських операцій, а також від осіб, стосовно яких Національний банк здійснює наглядову діяльність відповідно до Закону України «Про банки і банківську діяльність», інформацію про їх діяльність та пояснення стосовно отриманої інформації і проведених операцій.

Для підготовки банківської та фінансової статистики, аналізу економічної ситуації Національний банк має право безоплатно отримувати необхідну інформацію від органів державної влади і органів місцевого самоврядування та суб'єктів господарювання усіх форм власності.

Отримана інформація не підлягає розголошенню, за винятком випадків, передбачених законодавством України.

Згідно зі ст. 66, службовцям Національного банку забороняється розголошувати інформацію, що становить державну таємницю, банківську таємницю або іншу конфіденційну інформацію, яка стала відома їм у зв'язку з виконанням службових обов'язків, і в разі припинення роботи в Національному банку, крім випадків, передбачених законодавством України.

Закон України «Про банки і банківську діяльність» покладає на банки обв'язки, з одного боку, забезпечити збереження таємниці такої інформації, а з іншого – розкривати таку інформацію лише в передбачених законом випадках.

Схожі положення містяться в Директиві Європейського парламенту та Ради «Щодо започаткування діяльності кредитних установ та її ведення» від 20 березня 2000 р. № 2000/12/ЄС. Так, у ст. 30 («Обмін інформацією та професійна таємниця») цього акта вказується, що держави-члени повинні забезпечити, щоб усі особи, які працюють або працювали на компетентні органи, так само, як і аудитори або експерти, які діють від імені компетентних органів, зберігали професійну таємницю. Це означає, що ніяка конфіденційна інформація, яку вони можуть отримувати під час виконання своїх обов'язків, не повинна розкриватися будь-якій особі або органу, за винятком інформації у вигляді резюме або в узагальненій формі таким чином, щоб не можна було визначити окремі установи. Така заборона не поширюється на випадки, передбачені кримінальним законодавством. Незважаючи на це, якщо кредитна установа була проголошена банкрутом або примусово ліквідується, конфіденційна інформація, що не стосується третіх осіб, які намагаються врятувати цю кредитну установу, може бути розголошена в суді під час цивільних або арбітражних процесів.

Відповідно до ст. 61 Закону України «Про банки і банківську діяльність», *банки зобов'язані забезпечити збереження банківської таємниці* шляхом:

1) обмеження кола осіб, що мають доступ до інформації, яка становить банківську таємницю;

2) організації спеціального діловодства з документами, що містять банківську таємницю;

3) застосування технічних засобів для запобігання несанкціонованому доступу до електронних та інших носіїв інформації;

4) застосування застережень щодо збереження банківської таємниці та відповідальності за її розголошення в договорах та угодах між банком і клієнтом.

Службовці банку при вступі на посаду підписують зобов'язання щодо збереження банківської таємниці. Керівники та службовці банків зобов'язані не

розголошувати та не використовувати з вигодою для себе чи для третіх осіб конфіденційну інформацію, яка стала відома їм при виконанні своїх службових обов'язків.

Приватні особи та організації, які при виконанні своїх функцій або наданні послуг банку безпосередньо чи опосередковано отримали конфіденційну інформацію, зобов'язані не розголошувати цю інформацію і не використовувати її на свою користь чи на користь третіх осіб.

У разі заподіяння банку чи його клієнту збитків шляхом витоку інформації про банки та їх клієнтів з органів, які уповноважені здійснювати банківський нагляд, збитки відшкодовуються винними органами.

Відповідно до п. 1 ст. 1076 ЦК України, відомості, що складають банківську таємницю, можуть бути надані банком органам державної влади та їх посадовим особам виключно у випадках та в порядку, встановлених законом про банки і банківську діяльність. Відповідно до ст. 62 Закону України «Про банки і банківську таємницю», інформація щодо юридичних та фізичних осіб, яка містить банківську таємницю, розкривається банками:

1) на письмовий запит або з письмового дозволу власника такої інформації;

2) на письмову вимогу суду або за рішенням суду;

3) органам прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України, Антимонопольного комітету України – на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу;

4) органам державної податкової служби України на їх письмову вимогу з питань оподаткування або валютного контролю стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу;

5) центральному органу виконавчої влади із спеціальним статусом з питань фінансового моніторингу на його запит щодо фінансових операцій,

пов’язаних з фінансовими операціями, що стали об’єктом фінансового моніторингу (аналізу) згідно із законодавством щодо запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму, а також учасників зазначених операцій;

6) органам державної виконавчої служби на їх письмову вимогу з питань виконання рішень судів стосовно стану рахунків конкретної юридичної особи або фізичної особи – суб’єкта підприємницької діяльності.

Вимога відповідного державного органу, у тому числі й суду, на отримання інформації, яка містить банківську таємницю, повинна:

– бути викладена на бланку державного органу встановленої форми;

– бути надана за підписом керівника державного органу (чи його заступника), скріпленого гербовою печаткою;

– містити передбачені цим Законом підстави для отримання цієї інформації;

– містити посилання на норми закону, відповідно до яких державний орган має право на отримання такої інформації.

Довідки за рахунками (вкладами) у разі смерті їх власників надаються банком особам, зазначеним власником рахунку (вкладу) в заповідальному розпорядженні банку, державним нотаріальним конторам або приватним нотаріусам, іноземним консульським установам у справах спадщини за рахунками (вкладами) померлих власників рахунків (вкладів).

Банку забороняється надавати інформацію про клієнтів іншого банку, навіть якщо їх імена зазначені в документах, угодах та операціях клієнта. У зв’язку з цим банки повинні надавати інформацію про рух коштів на рахунку клієнта без зазначення відправника цих коштів та їх одержувача (які є як клієнтами іншого банку, так і клієнтами запитуваного банку) (див. додаток).

Банк має право надавати інформацію, що становить банківську таємницю, іншим банкам та Національному банку України в обсягах, необхідних при наданні кредитів, банківських гарантій.

Банк має право розкривати інформацію, що містить банківську таємницю, особі (у тому числі яка уповноважена діяти від імені держави), на користь якої відчужуються активи та зобов'язання банку при виконанні заходів, передбачених програмою фінансового оздоровлення банку, або під час здійснення процедури ліквідації. Національний банк України (тимчасовий адміністратор) має право надавати Міністерству фінансів України інформацію, яка містить банківську таємницю, щодо банків, участь у капіталізації яких бере держава.

Обмеження стосовно отримання інформації, що містить банківську таємницю, передбачені ст. 62, не поширюються на службовців Національного банку України або уповноважених ними осіб, які в межах повноважень, наданих Законом України «Про Національний банк України», здійснюють функції банківського нагляду або валютного контролю.

Національний банк України відповідно до міжнародного договору України або за принципом взаємності має право надавати інформацію, отриману при здійсненні нагляду за діяльністю банків, органу банківського нагляду іншої держави, а також отримувати від органу банківського нагляду іншої держави таку інформацію. Надана (отримана) інформація може бути використана виключно з метою банківського нагляду або запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом, чи фінансуванню тероризму.

Положення ч. 2 та 4 ст. 62 не поширюються на випадки надання спеціально уповноваженому органу виконавчої влади з питань фінансового моніторингу інформації про фінансові операції у випадках, передбачених законом.

Особи, винні в порушенні порядку розкриття та використання банківської таємниці, несуть відповідальність згідно із законами України.

Законодавством не передбачено здійснення виконавчого провадження щодо судових рішень про розкриття банками інформації, яка містить банківську таємницю. Водночас нормами нової редакції ЦПК України передбачено, що рішення суду щодо розкриття банком інформації, яка містить банківську таємницю, підлягає негайному виконанню. Оскарження такого рішення не зупиняє його виконання.

Доступ до банківської таємниці мають працівники Національного банку при виконанні ними своїх службових обов'язків.

Органи державної податкової служби, прокуратури, Служби безпеки України, Міністерства внутрішніх справ мають право отримати будь-яку інформацію, віднесену законом до банківської таємниці, з дозволу власника цієї інформації та за рішенням суду. Крім того, ці органи мають право отримати на письмову вимогу лише інформацію стосовно операцій за рахунками юридичних осіб та фізичних осіб – суб'єктів підприємницької діяльності за конкретний проміжок часу. Інші державні органи мають право отримати таку інформацію лише з дозволу власника цієї інформації та за рішенням суду.

Під час здійснення оперативно-розшукових заходів, а також провадження у кримінальних справах (особливо з господарських злочинів) виникає необхідність з метою збирання доказів одержати від установ банків інформацію про документи, що пов'язані з проведенням фінансово-господарських операцій певною юридичною або фізичною особою – клієнтом банку, тобто інформації, яка становить банківську таємницю. Законом України «Про банки і банківську діяльність» обмежено перелік випадків, у яких надається така інформація, заборонено вимагати від банків, їхніх керівників і службовців, приватних осіб деякі відомості, що належать до банківської таємниці.

Додатково обов'язок працівників банків зберігати банківську таємницю закріплено Законом України «Про платіжні системи та переказ коштів в Україні» від 5 квітня 2001 р. № 2346-III, згідно з п. 39.4 ст. 39 якого працівники суб'єктів переказу повинні виконувати вимоги щодо захисту інформації при здійсненні переказів, зберігати банківську таємницю та підтримувати конфіденційність інформації, що використовується в системі захисту цієї інформації.

Інститут банківської таємниці є дуже важливим чинником забезпечення прав і свобод людини, включаючи право на заняття підприємницькою діяльністю, не забороненою законом, право на невтручання в приватне життя тощо. Крім того, ступінь забезпеченості банківської таємниці є фактором, що обумовлює привабливість країни для іноземного капіталу, а також для вирішення ак-

туальної для України проблеми зменшення тіньового сектора економіки та повернення вивезених капіталів в Україну.

Однак банківське законодавство України не може вважатися сформованим у повному обсязі – відповідати сучасним вимогам економічного розвитку. Нагальною потребою в контексті поглиблення економічних реформ залишається подальше вдосконалення банківського законодавства України в напрямку його гармонізації з банківським законодавством розвинених країн світу.

Угода про асоціацію між Україною та Європейським Союзом передбачає адаптацію національного законодавства щодо забезпечення банківської таємниці до вимог ЄС. Законодавчі аспекти забезпечення банківської таємниці з позиції інформаційного права відповідно до впровадження новітніх інформаційно-комунікаційних технологій згідно із Директивою (Євросоюз) 2015/849 Європейського Парламенту та Ради від 20 травня 2015 року про запобігання використанню фінансової системи для цілей відмивання грошей або фінансування тероризму, що вносить зміни до Регламенту (Євросоюз) № 648/2012 Європейського Парламенту і Ради, а також скасовує Директиву 2005/60/ЄС Європейського Парламенту і Ради та Директиву Комісії 2006/70/ЄС і Регламенту Комісії (Євросоюз) 2015/703 від 30 квітня 2015 р., що запроваджує мережевий кодекс правил функціональної сумісності та обміну даними.

У березні 2015 р. Європейська Комісія розробила Проект заходів, спрямованих на досягнення прозорості у податкових питаннях (Transparency Package). Основні пропозиції: автоматичний обмін інформацією щодо податкових погоджень (rulings), виданих державами-членами ЄС; публічне розкриття міжнародними бізнес-групами деяких відомостей податкової звітності; перегляд підходів щодо визначення «шкідливих податкових режимів», які порушують конкуренцію між державами ЄС; підготовка статистичних відомостей щодо податкових злочинів та інших зловживань у податковій сфері для розроблення ефективних заходів протидії.

Міжнародний обмін інформацією передбачає: обмін за запитом (стандарт Exchange of Information on request (EOIR), який сьогодні залишається основним

інструментом для України; спонтанний обмін; автоматичний обмін (стандарт Automatic Exchange of Information (AEOI).

Автоматичний обмін передбачає: збирання інформації; модель обміну; співвідношення з іншими формами обміну (стандарт (Model Competent Authority, Agreement Common Reporting Standard (Common standard on reporting, due diligence and exchange of information); стандарт AEOI[51].

На міжнародному рівні Україна повинна ратифікувати Конвенцію про адміністративну допомогу (EU Directive on administrative cooperation in the field of taxation), підписати міжвідомчі угоди, досягти взаємної згоди з партнерами про обмін, узгодити форми обміну з державами, які погодились на обмін. На національному рівні необхідно імплементувати стандарт AEOI, врегулювати регулярне оновлення внутрішніх процедур відповідно до вимог стандарту AEOI, забезпечити дотримання вимог конфіденційності та захисту персональних даних, унормувати автоматизацію та технологічне забезпечення збирання інформації та обміну.

Країни Європейського союзу домовилися про обмін інформацією про банківських клієнтів та їх доходів за підсумками саміту 19-20 березня 2014 р., фактично відмовившись від банківської таємниці на території ЄС. Раніше протягом більш ніж п’яти років проти цього заходу наполегливо виступали Люксембург і Австрія, але й вони – одними з останніх – проголосували за обмін інформацією про будь-які види доходів іноземних громадян в 28 країнах Євросоюзу. Таким чином, ЄС посилює боротьбу проти податкових махінацій. Щороку країни ЄС, за даними Єврокомісії, втрачають трильйон євро через відведення доходів від оподаткування. «Такий крок неминучий і необхідний для того, щоб країни-члени ЄС могли вживати більш рішучих заходів проти податкових махі-

[51] Останні тенденції у сфері міжнародного оподаткування. Обмін податковою інформацією та прозорість офшорних структур. 23 червня 2015 року. Building better working world EY. p.18-22.[Електронний ресурс]. – Режим доступу: [http://www.ey.com/Publication/ vwLUAssets/EYinternational- tax-trends-23-jun-2015/$FILE/EY-international-tax-trends-23-jun-2015.pdf].

націй та ухилення від сплати податків», – заявив президент Європейської ради Херман ван Ромпей.[52]

3.2.5. Адвокатська таємниця

Формування права праслов'янського етносу відбувалося в тих же соціально-економічних умовах, що й формування римського права, і, відповідно, загальновизнані норми і правила поведінки суспільної людини мають не внутрішньодержавний, а загальнодержавний характер.

Інститут захисту та писемне право розвивалися в Київській Русі (IX–XIII ст.) в особливих історичних умовах общинного співжиття, тобто захист, обвинувачення, покарання ставали функціями общини. Суд як соціальний інститут з'явився пізніше, а функції представників визначилися на певному рівні відповідного правового побуту, тобто звичаєвого права. Роль захисників виконували рідні та приятелі сторін: послухи та видоки[53].

Процесуальна змагальність мала відкритий характер, тобто таємниці захисту не існувало. Якщо якісь факти приховувалися, то такі дії вважалися умисними, а сама таємниця розглядалася як нерозкритість чи неможливість виявити обставини справи, тобто ще не була сформована як правова необхідність. Формування держави призводить до визнання рівності громадян перед загальновизнаною нормою і, відповідно, до формування представництва. Право ставало формою організації суспільного життя, тобто державною справою. Представництво ставало вимогою часу. На рівні представництва як процесуально визначеної дії йдеться про таємницю як правову категорію. Особиста участь сторін та їх змагальність базувалися на особистому інтересі. Тобто таємниця теж залишалася їх особистою справою і визначалася в її тривіальному розумінні, тоді як представництво закладало інформаційне обмеження і певне ставлення до інформації. Представництво закладало правовий прецедент інформаційної відповідальності, формуючи як права і свободи сторін, так і права і свободи представників. На

[52] ЄС ліквідував банківську таємницю для іноземних громадян. [Електронний ресурс]. – Режим доступу: https://www.epravda.com.ua/news/2014/03/21/430321/

[53] Сутяжні справи вирішувалися громадою в цілому; по суті, усі ставали свідками безпосередньої події чи свідками порядного життя обвинуваченого. Перших називали «видоками», а других – «послухами».

цьому етапі правовий захист формується через представництво і таємниця як правова категорія стає ознакою формування нового правового побуту.

У кінці XVI ст. найбільш суттєвим і систематизованим законом, за яким жила держава періоду Литовсько-Руської доби, стала третя редакція Литовського статуту, основним джерелом якого були Руська Правда та магдебурзьке право. Литовський статут (редакції 1529, 1566, 1588 рр.) мав особливе значення для розвитку права в Україні, зокрема адвокатури. Третій Литовський статут детально встановлював порядок судового захисту (57–61 артиклі дев'ятого розділу) і визначав поняття «адвокатська таємниця».

Наступний період розвитку права в Україні пов'язаний із появою кодексу «Прав, за якими судиться малоросійський народ», у якому вперше вживаються терміни «адвокат», «повірений».

Адвокатура як самостійний правовий інститут запроваджена в Україні після проведення на початку 60-х рр. XIX ст. судової реформи. Правову регламентацію інститут адвокатури дістав за судовими статутами від 20 листопада 1864 р. За судовими статутами (ст. 403) присяжний повірений не повинен був розголошувати таємниці свого довірителя не тільки під час ведення його справи, а й у випадку усунення від неї і навіть після закінчення її.

У Радянській Україні з 2 жовтня 1922 р. діяло Положення про адвокатуру, у якому йшлося про колегії оборонців. 20 жовтня 1929 р. набрав чинності Статут про колективні форми роботи колегії оборонців у зв'язку із скасуванням приватної практики, діяльність якої визначалася як професійна.

Роль єдиного незалежного професійного правозахисного інституту, який покликаний захищати права та свободи, представляти законні інтереси особи в державних владних структурах на закріплених Законом України «Про адвокатуру і адвокатську діяльність» принципах верховенства закону, незалежності, демократизму, гуманізму та конфіденційності, реалізується адвокатурою в складній системі правовідносин.

Адвокатура України – недержавний самоврядний інститут, що забезпечує здійснення захисту, представництва та надання інших видів правової допомоги

на професійній основі, а також самостійно вирішує питання організації і діяльності адвокатури в порядку, встановленому цим Законом.

Згідно зі ст. 59 Конституції України, адвокатура виконує важливу функцію щодо забезпечення права на захист від обвинувачення та надання правової допомоги при вирішенні справ у судах та інших державних органах.

Відповідно до ст. 129 Конституції України, однією з головних засад судочинства є рівність усіх учасників судового процесу перед законом і судом та забезпечення обвинуваченому права на захист.

Адвокат – фізична особа, яка здійснює адвокатську діяльність на підставах та в порядку, що передбачені Законом України «Про адвокатуру і адвокатську діяльність».

Адвокатська діяльність – незалежна професійна діяльність адвоката щодо здійснення захисту, представництва та надання інших видів правової допомоги клієнту.

Захист – вид адвокатської діяльності, що полягає в забезпеченні захисту прав, свобод і законних інтересів підозрюваного, обвинуваченого, підсудного, засудженого, виправданого, особи, стосовно якої передбачається застосування примусових заходів медичного чи виховного характеру або вирішується питання про їх застосування у кримінальному провадженні, особи, стосовно якої розглядається питання про видачу іноземній державі (екстрадицію), а також особи, яка притягається до адміністративної відповідальності під час розгляду справи про адміністративне правопорушення.

У ст. 44 КПК України зазначається, що захисником є особа, яка в порядку, встановленому законом, уповноважена здійснювати захист прав і законних інтересів підозрюваного, обвинуваченого, підсудного, засудженого, виправданого та надання їм необхідної юридичної допомоги при провадженні у кримінальній справі.

Як захисники допускаються особи, які мають свідоцтво про право на заняття адвокатською діяльністю в Україні, та інші фахівці в галузі права, які за законом мають право на надання правової допомоги особисто чи за дорученням

юридичної особи. У випадках і в порядку, передбачених КПК України, як захисники допускаються близькі родичі обвинуваченого, підсудного, засудженого, виправданого, його опікуни або піклувальники.

Повноваження захисника на участь у справі стверджується:

1) адвоката – ордером відповідного адвокатського об'єднання;

2) адвоката, який не є членом адвокатського об'єднання, – угодою, інших фахівців у галузі права, які за законом мають право на надання правової допомоги особисто чи за дорученням юридичної особи або дорученням юридичної особи – угодою або дорученням юридичної особи;

3) близьких родичів, опікунів або піклувальників – заявою обвинуваченого, підсудного, засудженого, виправданого про їх допуск до участі у справі як захисників.

Захисник допускається до участі у справі на будь-якій стадії процесу. Про допуск захисника до участі у справі особа, яка провадить дізнання, слідчий, прокурор, суддя виносять постанову, а суд – ухвалу.

Адвокат при здійсненні своєї професійної діяльності виступає носієм обов'язків, іноді суперечливих, по відношенню до: клієнтів; судів та інших державних органів; адвокатури в цілому та окремих адвокатів; суспільства в цілому.

Під час здійснення адвокатської діяльності адвокат зобов'язаний: дотримуватися присяги адвоката України та правил адвокатської етики; на вимогу клієнта надати звіт про виконання договору про надання правової допомоги; невідкладно повідомляти клієнта про виникнення конфлікту інтересів; підвищувати свій професійний рівень; виконувати рішення органів адвокатського самоврядування; виконувати інші обов'язки, передбачені законодавством та договором про надання правової допомоги.

Під час здійснення адвокатської діяльності адвокат має право вчиняти будь-які дії, не заборонені законом, правилами адвокатської етики та договором про надання правової допомоги, необхідні для належного виконання договору про надання правової допомоги (ст.20), зокрема:

1) звертатися з адвокатськими запитами, у тому числі щодо отримання копій документів, до органів державної влади, органів місцевого самоврядування, їх посадових і службових осіб, підприємств, установ, організацій, громадських об'єднань, а також до фізичних осіб (за згодою таких фізичних осіб);

2) представляти і захищати права, свободи та інтереси фізичних осіб, права та інтереси юридичних осіб у суді, органах державної влади та органах місцевого самоврядування, на підприємствах, в установах, організаціях незалежно від форми власності, громадських об'єднаннях, перед громадянами, посадовими і службовими особами, до повноважень яких належить вирішення відповідних питань в Україні та за її межами;

3) ознайомлюватися на підприємствах, в установах і організаціях з необхідними для адвокатської діяльності документами та матеріалами, крім тих, що містять інформацію з обмеженим доступом;

4) складати заяви, скарги, клопотання, інші правові документи та подавати їх у встановленому законом порядку;

5) доповідати клопотання та скарги на прийомі в посадових і службових осіб та відповідно до закону одержувати від них письмові мотивовані відповіді на ці клопотання і скарги;

6) бути присутнім під час розгляду своїх клопотань і скарг на засіданнях колегіальних органів та давати пояснення щодо суті клопотань і скарг;

7) збирати відомості про факти, що можуть бути використані як докази, в установленому законом порядку запитувати, отримувати і вилучати речі, документи, їх копії, ознайомлюватися з ними та опитувати осіб за їх згодою;

8) застосовувати технічні засоби, у тому числі для копіювання матеріалів справи, в якій адвокат здійснює захист, представництво або надає інші види правової допомоги, фіксувати процесуальні дії, в яких він бере участь, а також хід судового засідання в порядку, передбаченому законом;

9) посвідчувати копії документів у справах, які він веде, крім випадків, якщо законом установлено інший обов'язковий спосіб посвідчення копій документів;

10) одержувати письмові висновки фахівців, експертів з питань, що потребують спеціальних знань;

11) користуватися іншими правами, передбаченими цим Законом та іншими законами.

Наведені права надані тільки адвокату, у зв'язку з чим особа, яка не користується його допомогою, ці засоби захисту застосувати не може.

Забезпечення права на захист від обвинувачення та надання правової допомоги під час вирішення справ у судах та інших державних органах реалізуються адвокатами в складній системі правовідносин із різними суб'єктами. Система критеріїв правильності вибору того чи іншого варіанта поведінки в ситуаціях зіткнення, суперечності різних обов'язків і прав повинна бути єдиною для всіх адвокатів і передбачуваною.

Адвокат іноземної держави здійснює адвокатську діяльність на території України відповідно до цього Закону, якщо інше не передбачено міжнародним договором, згода на обов'язковість якого надана Верховною Радою України.

У *Загальному кодексі правил для адвокатів країн ЄС*, прийнятому делегацією дванадцяти країн-учасниць на пленарному засіданні у Страсбурзі 1 жовтня 1988 р., підкреслено роль деонтологічних правил для забезпечення виконання адвокатурою її важливої ролі в суспільстві. У преамбулі до цих правил зазначено, що адвокат у демократичному суспільстві при виконанні своїх професійних обов'язків вступає в різноманітні відносини, котрі покладають на нього відповідні обов'язки перед клієнтами, судом та іншими органами влади, адвокатською професією, її окремими представниками, суспільством.

Правила, якими керується будь-яке об'єднання адвокатів, походять від існуючих у ньому традицій. Вони також співвідносяться з умовами і характером завдань, що виконуються членами даної організації в межах судових і адміністративних процедур, із державним законодавством.

У ст. 2.3. Загального кодексу правил для адвокатів зазначається, що:

– особливість професії адвоката полягає в тому, що він одержує від клієнта відомості, які той не буде повідомляти іншій особі, а також іншу інформа-

цію, яку йому належить зберігати в таємниці. Довіра до адвоката може виникнути лише за умови обов'язкового додержання ним принципу конфіденційності. Таким чином, конфіденційність є першорядним і фундаментальним правом та обов'язком адвоката;

– адвокат зобов'язаний однаковою мірою зберігати в таємниці як відомості, одержані ним від клієнта, так і інформацію про клієнта, надану йому в процесі надання послуг клієнту;

– на обов'язок додержання конфіденційності не поширюється дія строку давності;

– адвокат зобов'язаний вимагати додержання конфіденційності від помічників і від будь-яких інших осіб, які беруть участь у наданні послуг клієнту.

У ст. 14 Основних принципів, які стосуються юристів, що прийняті VIII Конгресом ООН 27 серпня – 7 вересня 1990 р., зазначено, що адвокат, захищаючи права своїх клієнтів при здійсненні правосуддя, повинен сприяти захисту прав людини і основних свобод, визнаних національним і міжнародним правом, діяти вільно і наполегливо відповідно до закону й визнаних професійних стандартів та етичних норм.

Адвокатська таємниця не може розглядатися у відриві від соціально-економічних, політичних, духовних норм сучасного життя суспільства. Встановлена законодавством адвокатська таємниця, яку адвокат зобов'язаний зберігати, є однією з гарантій сумлінного виконання адвокатом своїх професійних обов'язків та забезпечення прав і законних інтересів його клієнта. Адвокат може виступати в якості представника потерпілого, цивільного позивача та цивільного відповідача.

Згідно Закону України «Про адвокатуру і адвокатську діяльність», предметом адвокатської таємниці є питання, з яких громадянин або юридична особа зверталися до адвоката, суть консультацій, порад, роз'яснень та інших відомостей, одержаних адвокатом при здійсненні своїх професійних обов'язків.

Адвокату забороняється: використовувати свої права всупереч правам, свободам та законним інтересам клієнта; без згоди клієнта розголошувати відомості, що становлять адвокатську таємницю, використовувати їх у своїх інте-

ресах або інтересах третіх осіб; займати у справі позицію всупереч волі клієнта, крім випадків, якщо адвокат впевнений у самообмові клієнта; відмовлятися від надання правової допомоги, крім випадків, установлених законом. (ст. 21).

Адвокатською таємницею є будь-яка інформація, що стала відома адвокату, помічнику адвоката, стажисту адвоката, особі, яка перебуває у трудових відносинах з адвокатом, про клієнта, а також питання, з яких клієнт (особа, якій відмовлено в укладенні договору про надання правової допомоги з передбачених цим Законом підстав) звертався до адвоката, адвокатського бюро, адвокатського об'єднання, зміст порад, консультацій, роз'яснень адвоката, складені ним документи, інформація, що зберігається на електронних носіях, та інші документи і відомості, одержані адвокатом під час здійснення адвокатської діяльності (ст. 22).

Інформація або документи можуть втратити статус адвокатської таємниці за письмовою заявою клієнта (особи, якій відмовлено в укладенні договору про надання правової допомоги з передбачених цим Законом підстав). При цьому інформація або документи, що отримані від третіх осіб і містять відомості про них, можуть поширюватися з урахуванням вимог законодавства з питань захисту персональних даних.

Обов'язок зберігати адвокатську таємницю поширюється на адвоката, його помічника, стажиста та осіб, які перебувають у трудових відносинах з адвокатом, адвокатським бюро, адвокатським об'єднанням, а також на особу, стосовно якої припинено або зупинено право на заняття адвокатською діяльністю. Адвокат, адвокатське бюро, адвокатське об'єднання зобов'язані забезпечити умови, що унеможливлюють доступ сторонніх осіб до адвокатської таємниці або її розголошення.

У разі пред'явлення клієнтом вимог до адвоката у зв'язку з адвокатською діяльністю адвокат звільняється від обов'язку збереження адвокатської таємниці в межах, необхідних для захисту його прав та інтересів. У такому випадку суд, орган, що здійснює дисциплінарне провадження стосовно адвоката, інші органи чи посадові особи, які розглядають вимоги клієнта до адвоката або яким

стало відомо про пред'явлення таких вимог, зобов'язані вжити заходів для унеможливлення доступу сторонніх осіб до адвокатської таємниці та її розголошення.

Особи, винні в доступі сторонніх осіб до адвокатської таємниці або її розголошенні, несуть відповідальність згідно із законом.

Забороняється вимагати від адвоката, його помічника, стажиста, особи, яка перебуває у трудових відносинах з адвокатом, адвокатським бюро, адвокатським об'єднанням, а також від особи, стосовно якої припинено або зупинено право на заняття адвокатською діяльністю, надання відомостей, що є адвокатською таємницею. З цих питань зазначені особи не можуть бути допитані, крім випадків, якщо особа, яка довірила відповідні відомості, звільнила цих осіб від обов'язку зберігати таємницю в порядку, передбаченому законом (ст. 23).

Забороняється залучати адвоката до конфіденційного співробітництва під час проведення оперативно-розшукових заходів чи слідчих дій, якщо таке співробітництво буде пов'язане або може призвести до розкриття адвокатської таємниці (ст. 23). З метою забезпечення дотримання вимог Закону України «Про адвокатуру і адвокатську діяльність» щодо адвокатської таємниці під час проведення зазначених процесуальних дій представнику ради адвокатів регіону надається право ставити запитання, подавати свої зауваження та заперечення щодо порядку проведення процесуальних дій, що зазначаються у протоколі.

Відмова в наданні інформації на адвокатський запит, несвоєчасне або неповне надання інформації, надання інформації, що не відповідає дійсності, тягнуть за собою відповідальність, встановлену законом, крім випадків відмови в наданні інформації з обмеженим доступом.

Адвокат забезпечує захист персональних даних про фізичну особу, якими він володіє, відповідно до законодавства з питань захисту персональних даних.

Адвокату забороняється укладати договір про надання правової допомоги і він зобов'язаний відмовитися від виконання договору, укладеного адвокатом, адвокатським бюро або адвокатським об'єднанням, у разі, якщо виконання договору про надання правової допомоги може призвести до розголошення адво-

катської таємниці У разі відмови від укладення договору про надання правової допомоги адвокат зобов'язаний зберігати адвокатську таємницю про відомості, що стали йому відомі від особи, яка звернулася з пропозицією укладення такого договору (ст. 28).

Дані попереднього слідства, які стали відомі адвокату у зв'язку з виконанням ним своїх професійних обов'язків, можуть бути розголошені тільки з дозволу слідчого або прокурора.

Адвокати, винні в розголошенні відомостей попереднього слідства, несуть відповідальність згідно з чинним законодавством.

Адвокату, помічнику адвоката, посадовим особам адвокатських об'єднань забороняється розголошувати відомості, що становлять предмет адвокатської таємниці, і використовувати їх у своїх інтересах або в інтересах третіх осіб.

Важливість функціонального навантаження адвокатури вимагає від адвокатів слідування високим етичним стандартам поведінки; водночас специфіка, комплексний характер обов'язків, що лежать на адвокатурі, обумовлюють необхідність збалансування служіння адвоката інтересам окремого клієнта та інтересам суспільства в цілому.

Виходячи з наведених міркувань були вироблені Правила адвокатської етики, метою яких є уніфіковане закріплення традицій і досвіду української адвокатури у сфері тлумачення норм адвокатської етики, а також загальновизнаних деонтологічних норм і правил, прийнятих у міжнародному адвокатському співтоваристві.

Закон України «Про адвокатуру і адвокатську діяльність» передбачає дотримання правил адвокатської етики як одного із основних обов'язків адвоката, котрі він бере на себе, складаючи Присягу адвоката України. У ст. 9 Правил адвокатської етики, що схвалені Вищою кваліфікаційною комісією адвокатури при Кабінеті Міністрів України 1 жовтня 1999 р., вказано:

1. Дотримання принципу конфіденційності є необхідною і щонайважливішою передумовою довірчих відносин між адвокатом і клієнтом, без яких є неможливим належне надання правової допомоги. Тому збереження конфіден-

ційності будь-якої інформації, отриманої адвокатом від клієнта, а також про клієнта (зокрема щодо його особи) або інших осіб у процесі здійснення адвокатської діяльності, є правом адвоката у відносинах з усіма суб'єктами права, які можуть вимагати розголошення такої інформації, та обов'язком щодо клієнта і тих осіб, кого ця інформація стосується.

2. Дія принципу конфіденційності не обмежена в часі.

3. Конфіденційність певної інформації, що охороняється правилами цієї статті, може бути відмінена тільки особою, зацікавленою в її дотриманні (або спадкоємцями такої фізичної особи чи правонаступниками юридичної особи), у письмовій або іншій зафіксованій формі.

4. Адвокат не відповідає за порушення цього принципу у випадках допиту його у встановленому законом порядку як свідка стосовно обставин, які виходять за межі предмета адвокатської таємниці, визначеного чинним законодавством, хоча й охоплюється предметом конфіденційності інформації, передбаченим цими Правилами.

5. За всіх інших обставин при визначенні обсягу відомостей, на котрі поширюється обов'язок збереження конфіденційності, адвокат повинен виходити з норм цих Правил.

6. Розголошення відомостей, що складають адвокатську таємницю, заборонено за будь-яких обставин, включаючи незаконні спроби органів дізнання, попереднього слідства і суду допитати адвоката про обставини, що складають адвокатську таємницю.

7. Адвокат (адвокатське об'єднання) зобов'язаний забезпечити розуміння і дотримання принципу конфіденційності його помічниками та членами технічного персоналу.

8. Адвокат (адвокатське об'єднання) зобов'язаний забезпечити такі умови зберігання документів, переданих йому клієнтом, адвокатських досьє та інших матеріалів, що знаходяться в його розпорядженні і містять конфіденційну інформацію, котрі розумно виключають доступ до них сторонніх осіб.

Інтереси клієнта захищає ст. 23 Правил адвокатської етики, оскільки запроваджує дотримання принципу неприпустимості представництва клієнтів із суперечливими інтересами.

Функції захисту адвокатської таємниці закладені в змісті таких статей Правил адвокатської етики:

– стаття 23 – адвокат не має права прийняти доручення, якщо інтереси клієнта об'єктивно суперечать інтересам іншого клієнта, з яким адвокат (адвокатське об'єднання) зв'язаний угодою про надання правової допомоги, або якщо є розумні підстави вважати, що передбачуваний розвиток інтересів нового і попереднього клієнта призведе до виникнення суперечності інтересів;

– стаття 25 – адвокат не повинен приймати доручення, виконання якого може потягнути розголошення відомостей, конфіденційність котрих охороняється Правилами адвокатської етики, крім випадків, коли на це буде отримано письмову згоду особи, зацікавленої в збереженні конфіденційності, за умови, що її інтересам при цьому об'єктивно не буде завдано шкоди;

– стаття 26 – правила, викладені в статтях 23 і 25, у частині, що стосується адвокатських об'єднань, поширюються на членів адвокатських об'єднань, діяльність яких здійснюється в одному приміщенні, які користуються технічними послугами одного й того самого технічного персоналу та користуються спільною офісною технікою, а також перебувають при здійсненні професійної діяльності у відносинах регулярного спілкування, пов'язаного з технічними особливостями організації роботи об'єднання; жоден з адвокатів – членів адвокатського об'єднання не може прийняти доручення клієнта, якщо іншому адвокату – члену цього адвокатського об'єднання це забороняється згідно з правилами, передбаченими статтями 23, 25 Правил адвокатської етики;

– стаття 57 – адвокат не має права при здійсненні професійної діяльності в суді будь-яким чином безпосередньо або опосередковано порушувати конфіденційність інформації, яка відноситься до предмета адвокатської таємниці, або є конфіденційною згідно з Правилами адвокатської етики;

– стаття 71 – адвокат не може використовувати у своїй громадській, науковій або публіцистичній діяльності інформацію, конфіденційність якої охороняється цими Правилами, без згоди на це осіб, зацікавлених у нерозголошенні такої інформації.

Володіння таємницею впливає на вибір позиції адвоката в цивільних справах. Він може відмовитися від захисту інтересів свого довірителя, якщо повідомлені йому факти впливають на можливість підтримання позиції клієнта. Але вже беручи участь у справі, адвокат зобов'язаний представляти інтереси довірителя, використовуючи всі передбачені законом засоби і способи для встановлення обставин, що є підставою вимог і заперечень клієнта. Володіючи таємницею, адвокат має сприяти створенню необхідних умов для правильного вирішення справи судом, тобто його позиція не повинна бути протиставлена здійсненню правосуддя.

Якщо закон забороняє надання правової допомоги особам із протилежними інтересами, які беруть участь в одній справі, то моральні норми не допускають можливості участі адвоката як процесуального противника і щодо колишніх довірителів, незалежно від тривалості часу з моменту виконання доручення та його характеру.

Уважається недопустимим повідомлення тих чи інших фактів своїм колегам при обговоренні спірних чи сумнівних моментів справи. Розгляд спірної ситуації з відома чи за згодою клієнта може бути прийнятним лише в інтересах справи, що вимагає від адвоката вдумливості, такту та обачливості.

Особливо уважно необхідно ставитися до запиту матеріалів щодо свого довірителя, коли це стосується даних особистого порядку, у такому разі має бути отримана згода клієнта.

Адвокат не має права робити запити з метою отримання матеріалів щодо протилежної сторони, якщо вони за своїм змістом ганьблять цю особу (відомості про захворювання, факти інтимного життя, які процесуальний противник намагається приховати з тих чи інших міркувань).

Гарантією правового забезпечення адвокатської таємниці є право підозрюваного, обвинуваченого, поряд з іншими правами, на побачення віч-на-віч із захисником до першого допиту, заборона допиту захисника як свідка, заборона знайомитися з матеріалами, що складають адвокатське досьє, заборона щодо розголошення даних досудового слідства.

У той час коли інші види конфіденційної інформації можуть бути отримані державними органами відповідно до певних процедур, нормами ст. 10 Закону України «Про адвокатуру і адвокатську діяльність» «забороняється будь-яке втручання в адвокатську діяльність, вимагання від адвоката, його помічника, посадових осіб і технічних працівників адвокатських об'єднань відомостей, що становлять адвокатську таємницю». З цих питань адвокати не можуть бути допитані як свідки.

Документи, пов'язані з виконанням адвокатом доручення, не підлягають оглядові, розголошенню чи вилученню без його згоди. Законом забороняється прослуховування телефонних розмов адвокатів у зв'язку з оперативно-розшуковою діяльністю без санкції Генерального прокурора України, його заступників.

Дисциплінарним проступком адвоката є (ст. 34): порушення вимог несумісності; порушення присяги адвоката України; порушення правил адвокатської етики; розголошення адвокатської таємниці або вчинення дій, що призвели до її розголошення; невиконання або неналежне виконання своїх професійних обов'язків; невиконання рішень органів адвокатського самоврядування; порушення інших обов'язків адвоката, передбачених законом.

За порушення вимог Закону України «Про адвокатуру і адвокатську діяльність», інших актів законодавства України, що регулюють діяльність адвокатури, Присяги адвоката України рішенням дисциплінарної палати кваліфікаційно-дисциплінарної комісії до адвоката можуть бути застосовані дисциплінарні стягнення. Накладення на адвоката дисциплінарного стягнення у вигляді позбавлення права на заняття адвокатською діяльністю може застосовуватися виклю-

чно у разі розголошення адвокатом відомостей, що становлять адвокатську таємницю, використання їх у своїх інтересах або в інтересах третіх осіб (с. 32).

Адвокати, винні в розголошенні конфіденційних відомостей, що становлять адвокатську таємницю, несуть дисциплінарну відповідальність, а в разі розголошення ними без дозволу слідчого або прокурора даних попереднього слідства – і кримінальну відповідальність (ст. 387 КК України).

Отже, конфіденційність інформації, що становить адвокатську таємницю, має найбільші серед інформації з обмеженим доступом правові гарантії.

3.2.6. Нотаріальна таємниця

У правовій системі нотаріат відіграє значну роль як орган безспірної цивільної юрисдикції та превентивного правосуддя. Латинський вислів «consensus facit ius», що означає «згода творить право» підкреслює важливість нотаріальної діяльності, в межах якої згода сторін формулюється та оформлюється в нотаріальних актах, що мають доказову силу та публічне визнання.

Принципи організації та діяльності сучасного нотаріату вперше формалізовані Н. Бонапартом у Законі «Про принципи організації нотаріату» від 16 березня 1803 р.[54]

Міжнародний союз латинського нотаріату (МСЛН) утворився в 1948 р. у Буенос-Айресі під час зустрічей представників національних організацій, цей орган поєднує нотаріальні організації латинського нотаріату. На сьогоднішній день у МСЛН входять більше 60 країн: (ФРН, Італія, Франція, Швейцарія, Іспанія й т.д.). МСЛН має своєю метою сприяти поширенню у світі законодавства країн-членів союзу, а також знайомству з його інститутами.

Особливості побудови нотаріатів у різних країнах обґрунтовуються належністю останніх до відповідної правової сім'ї. Згідно з традиційним поділом правових систем світу на англосаксонську та континентальну можна вести мову про нотаріат латинського типу.

[54] 16 березня 1803 р. за календарем Французької революції, відповідно, становить 25 вантоза XI р., у зв'язку з чим цей закон одержав назву «Закон Вантоза». Закон передбачав процедуру призначення нотаріуса органами юстиції, обмеження державою загальної кількості нотаріусів та їх незмінність і незамінність. Посада нотаріуса була визнана несумісною з іншими посадами. Нотаріальні документи, за виготовлення яких нотаріуси справляли тариф, одержали статус суспільної довіри.

Економічні зрушення в Україні, сучасні соціальні відносини, потреба економіки в налагоджених юридичних процедурах, покликаних забезпечувати стабільність та адаптованість економічних і правових відносин до сучасних світових тенденцій у галузі правового їх оформлення, потребують наявності сучасного ефективного дієвого нотаріату.

Український нотаріат зазнає впливу тенденцій нотаріату латинського типу.

Відповідно до положень ст. 1 Закону України «Про нотаріат» від 2 вересня 1993 р. № 3425-XII, *нотаріат в Україні* – це система органів і посадових осіб, на які покладено обов'язок посвідчувати права, а також факти, що мають юридичне значення, та вчиняти інші нотаріальні дії, передбачені цим Законом, з метою надання їм юридичної вірогідності.

Правовою основою діяльності нотаріату є Конституція України, указаний вище Закон, інші законодавчі акти України.[55]

У зв'язку з підвищенням значущості нотаріату особливі вимоги ставляться не тільки до нотаріальної діяльності, а й до особи нотаріуса. У своїй діяльності нотаріуси реалізують основні завдання нотаріату та належать до органів, що виконують нотаріальні функції. Відносини між нотаріусом та заінтересованими особами мають довірчий характер, а тому передбачають збереження конфіден-

[55] Значним джерелом в регулюванні нотаріальної діяльності є Укази президента України, а саме «Про впорядкування справляння плати за вчинення нотаріальних дій», від 10 липня 1998 р., «Про врегулювання діяльності нотаріату в Україні» від 23 серпня 1998 р. та ін. Джерелом нотаріального процесуального права є постанови, декрети та розпорядження Кабінету Міністрів України: Положення «Про Вищу кваліфікаційну комісію нотаріату» від 22 лютого 1994 р., Постанова Кабінету Міністрів України «Про порядок посвідчення заповітів і доручень, прирівнюваних до нотаріально посвідчених» від 15 червня 1994 р. № 419, Постанова Кабінету Міністрів України «Про затвердження Тимчасового порядку державної реєстрації правочинів» від 26 травня 2004 р. № 671, Постановление Кабинета Министров Украины «Перечень документов, по которым взыскание задолженности производится в бесспорном порядке на основании исполнительных надписей нотариусов» от 29 июня 1999 г. № 1172.

Для регулювання діяльності нотаріальних органів мають накази Міністерства юстиції України, якими затверджені інструкції: «О порядке совершения нотариальных действий должностными лицами исполнительных комитетов сельских, поселковых, городских советов народных депутатов Украины» от 25 августа 1994 г. № 22/5, «Про порядок вчинення нотаріальних дій нотаріусами України» від 03.03.2004 р. № 20/5, « Про ведення Державного реєстру правочинів» від 18.08.2004 р. № 86/5, «Про порядок передачі нотаріальних документів на тимчасове зберігання до державного нотаріального архіву» від 09.07.2002 р. № 63/5 тощо.

Питання вчинення нотаріальних дій за кордоном визначаються Консульським статутом України, консульськими конвенціями, та різними міжнародними угодами, що уклала Україна з іншими державами. Порядок вчинення нотаріальних дій консульськими установами України регулюється законом України «Про нотаріат». Консульським статутом України від 2 квітня 1994 р., спільним наказом Міністерства юстиції та Міністерства закордонних справ України від 27 грудня 2004 р., яким затверджено Положення «Про порядок здійснення нотаріальних дій дипломатичних представництвах і консульських установах України», іншими нормативними актами.

ційності інформації про майновий та немайновий стан осіб, що звертаються за вчиненням нотаріальних дій. Професійна діяльність нотаріуса забезпечує превентивний правовий захист і унеможливлює порушення в майбутньому прав та інтересів суб'єктів права й виникнення спорів у судах. Отже, нотаріат як інститут позасудового превентивного захисту своєю діяльністю має сприяти досягненню завдань правосуддя, запобігаючи виникненню судових спорів шляхом попередження порушення цивільних прав та інтересів, забезпечення їх належної реалізації. Адже, за відомим латинським висловом «melior est iustitia vere praeveniens quam se vere puniens», кращим є правосуддя, що істинно попереджає, ніж те, що суворо карає.

Вчинення нотаріальних дій в Україні покладається на нотаріусів, які працюють у державних нотаріальних конторах, державних нотаріальних архівах (державні нотаріуси) або займаються приватною нотаріальною діяльністю (приватні нотаріуси).

Документи, оформлені державними і приватними нотаріусами, мають однакову юридичну силу.

Особа, якій уперше надається право займатися нотаріальною діяльністю, у головних управліннях юстиції в областях, місті Києві в урочистій обстановці приносить присягу такого змісту: «Урочисто присягаю виконувати обов'язки нотаріуса чесно і сумлінно, згідно з законом і совістю, поважати права і законні інтереси громадян і організацій, зберігати професійну таємницю, скрізь і завжди берегти чистоту високого звання нотаріуса».

Відповідно до ст. 5 Закону України «Про нотаріат», нотаріус зобов'язаний:

– здійснювати свої професійні обов'язки відповідно до цього Закону і принесеної присяги;

– сприяти громадянам, підприємствам, установам і організаціям у здійсненні їх прав та захисті законних інтересів, роз'яснювати права і обов'язки, попереджати про наслідки вчинюваних нотаріальних дій для того, щоб юридична необізнаність не могла бути використана їм на шкоду;

– зберігати в таємниці відомості, одержані ним у зв'язку з вчиненням нотаріальних дій;

– відмовити у вчиненні нотаріальної дії в разі її невідповідності законодавству України або міжнародним договорам;

– вести нотаріальне діловодство та архів нотаріуса відповідно до встановлених правил;

– дбайливо ставитися до документів нотаріального діловодства та архіву нотаріуса, не допускати їх пошкодження чи знищення;

– надавати документи, інформацію і пояснення на вимогу Міністерства юстиції України, Головного управління юстиції Міністерства юстиції України в Автономній Республіці Крим, головних управлінь юстиції в областях, містах Києві та Севастополі при здійсненні ними повноважень щодо контролю за організацією діяльності та виконанням нотаріусами правил нотаріального діловодства;

– постійно підвищувати свій професійний рівень, а у випадках, передбачених п. 3 ч. 1 ст. 29-1 цього Закону, проходити підвищення кваліфікації;

– виконувати інші обов'язки, передбачені законом.

Нотаріальна таємниця – сукупність відомостей, отриманих під час вчинення нотаріальної дії або звернення до нотаріуса заінтересованої особи, у тому числі про особу, її майно, особисті майнові та немайнові права і обов'язки тощо.

У ст. 8 Закону України «Про нотаріат» передбачений обов'язок зберігати нотаріальну таємницю для:

– нотаріуса та інших посадових осіб, які вчиняють нотаріальні дії, а також стажиста нотаріуса (навіть якщо їх діяльність обмежується наданням правової допомоги чи ознайомленням з документами і нотаріальна дія або дія, яка прирівнюється до нотаріальної, не вчинялась);

– осіб, яким про вчинені нотаріальні дії стало відомо у зв'язку з виконанням ними службових обов'язків чи іншої роботи, на осіб, залучених для вчинення нотаріальних дій у якості свідків, та на інших осіб, яким стали відомі відомості, що становлять предмет нотаріальної таємниці.

Слід також зауважити, що нотаріус не має права давати свідчення в якості свідка щодо відомостей, які становлять нотаріальну таємницю, крім випадків, коли цього вимагають особи, за дорученням яких або щодо яких вчинялися нотаріальні дії.

Законом передбачено низку гарантій збереження нотаріальної таємниці. Однак є випадки, коли відомості, що належать до нотаріальної таємниці, можуть бути розголошені. Стаття 8 вказаного вище Закону визначає вичерпний перелік таких випадків:

1) довідки про вчинені нотаріальні дії та копії документів, що зберігаються у нотаріуса, видаються нотаріусом виключно фізичним та юридичним особам, за дорученням яких або щодо яких вчинялися нотаріальні дії. У разі смерті особи чи визнання її померлою такі довідки видаються спадкоємцям померлого. У разі визнання особи безвісно відсутньою опікун, призначений для охорони майна безвісно відсутнього, має право отримувати довідки про вчинені нотаріальні дії, якщо це необхідно для збереження майна, над яким встановлена опіка;

2) довідки про вчинені нотаріальні дії та інші документи надаються нотаріусом протягом десяти робочих днів на обґрунтовану письмову вимогу суду, прокуратури, органів дізнання і досудового слідства у зв'язку з цивільними, господарськими, адміністративними або кримінальними справами, справами про адміністративні правопорушення, що знаходяться в провадженні цих органів, з обов'язковим зазначенням номера справи та прикладенням гербової печатки відповідного органу;

3) довідки про суму нотаріально посвідчених договорів, які необхідні виключно для встановлення додержання законодавства з питань оподаткування, надаються нотаріусом протягом 10 робочих днів на обґрунтовану письмову вимогу органів державної податкової служби. Довідки про наявність складеного заповіту та витяги із спадкового реєстру за виключенням заповідача видаються тільки після смерті заповідача;

4) на вимогу Міністерства юстиції України, Головного управління юстиції Міністерства юстиції України в Автономній Республіці Крим, головних управлінь

юстиції в областях, містах Києві та Севастополі з метою регулювання організації нотаріальної діяльності нотаріуси видають підписані ними копії документів та витяги з них, а також пояснення нотаріусів у строк, встановлений цими органами.

Відповідно до ст. 129 Конституції України судді при здійсненні правосуддя незалежні і підкоряються лише закону. Нотаріус у результаті здійснення своєї професійної діяльності може стати учасником судового процесу. При цьому він не «застрахований» від участі в жодному з існуючих в Україні судових проваджень: цивільному, адміністративному чи кримінальному. Законність як одна з основних засад судочинства в Україні, захищає професійну діяльність нотаріуса шляхом уведення в законодавство поняття «нотаріальна таємниця».

До осіб, яким про вчинені нотаріальні дії стало відомо у зв'язку з виконанням ними службових обов'язків, можна віднести співробітників Міністерства юстиції України, головних управлінь юстиції в областях, місті Києві, які діють з метою регулювання організації нотаріальної діяльності. На їх вимогу нотаріуси зобов'язані видавати підписані ними копії документів та витяги з них, а також пояснення нотаріусів у строк, встановлений цими органами. Співробітники вказаних органів влади зобов'язані дотримуватися нотаріальної таємниці.

Захисний режим нотаріальної таємниці полягає в тому, що не лише нотаріуси та їх помічники не просто мають право, а й зобов'язані відмовитися від виконання правомірних вимог інших суб'єктів правовідносин, але також й інші особи, які в силу тих чи інших обставин отримали доступ до відомостей, що становлять нотаріальну таємницю, також стають її носієм і зобов'язані охороняти її. Проте слід зазначити, що Закон містить певні обмеження режиму нотаріальної таємниці, таким чином позбавляючи її абсолютного характеру. Наприклад, та ж сама ст. 8 Закону зобов'язує нотаріуса протягом десяти робочих днів надати довідку про вчинені нотаріальні дії на письмову вимогу суду, прокуратури, органів, що здійснюють оперативно-розшукову діяльність, органів досудового розслідування у зв'язку з кримінальним провадженням, цивільними, господарськими, адміністративними справами, справами про адміністративні

правопорушення, що знаходяться в провадженні цих органів. Однак нотаріус зобов'язаний задовольнити таку письмову вимогу за умови, якщо вона обґрунтована. Тобто законодавець надав нотаріусу право оцінювати, обґрунтованою є вимога вказаних органів чи ні. Зрозуміло, що реалізувавши це право, тобто оцінивши обґрунтованість вимоги, нотаріус має й інше право, похідне від вищезазначеного, а саме: право відмовити у наданні відповідної довідки про вчинені нотаріальні дії та інших документів, якщо вважатиме, що письмова вимога є необґрунтованою. Вважати категоричним та безумовним обов'язок нотаріуса видати довідку на вимогу вказаних органів можна лише проігнорувавши наявність у цій нормі права слова «обґрунтована».

Особи, винні в порушенні нотаріальної таємниці, несуть відповідальність у порядку, встановленому законом.

Будь-яке втручання в діяльність нотаріуса, зокрема з метою перешкоджання виконанню ним своїх обов'язків або спонукання до вчинення ним неправомірних дій, у тому числі вимагання від нього, його стажиста, інших працівників, які знаходяться у трудових відносинах з нотаріусом, відомостей, що становлять нотаріальну таємницю, забороняється і тягне за собою відповідальність відповідно до законодавства. Разом з тим, забезпечити збереження таємниці вчинення нотаріальних дій, якщо в одному приміщенні державної нотаріальної контори ведуть прийом кілька нотаріусів одночасно.

3.2.7. Лікарська таємниця

3.2.7.1. Історичні витоки формування лікарської таємниці

Яскравим і давнім прикладом професійної таємниці вважається лікарська таємниця, корені якої сягають ще Стародавньої Греції. Ця таємниця закріплена в клятві Гіппократа на межі V–IV ст. до н. е.: «Щоб при лікуванні – а також і без лікування – я не побачив чи не почув стосовно людського життя з того, що не слід будь-коли розголошувати, я промовчу про те, вважаючи подібні речі таємницею».

Женевська декларація, що прийнята 2-ю Генеральною асамблеєю Всесвітньої медичної асамблеї у вересні 1948 р., з поправками, внесеними 22-ю Всес-

вітньою медичною асамблеєю в серпні 1968 р., 35-ю Всесвітньою медичною асамблеєю у вересні 1983 р., 46-ю Генеральною асамблеєю Всесвітньої медичної асамблеї у вересні 1994 р., в урочистій клятві лікарів вимагає зберігати довірені таємниці й після смерті пацієнта.

У жовтні 1981 р. на 34-й Всесвітній медичній асамблеї незалежна професійна організація лікарів світу Всесвітня медична асоціація прийняла документ про мінімальний міжнародний стандарт прав пацієнтів – Лісабонську декларацію про права пацієнтів, згідно з яким пацієнт має право на: вільний вибір лікаря, погодитися чи відмовитися від лікування після отримання адекватної інформації, очікувати, що його лікар буде поважати конфіденційний характер медичних і приватних відомостей стосовно нього.

Декларація щодо незалежності та професійної свободи лікаря, котра прийнята 38-ю Всесвітньою медичною асамблеєю в жовтні 1986 р., зазначає, що лікарі повинні мати професійну свободу надавати допомогу своїм пацієнтам без зовнішніх впливів, повинні охоронятися й захищатися професійні призначення лікаря, а також його свобода при прийнятті клінічних або етичних рішень під час лікування і надання допомоги пацієнтам.

Біоетичні принципи знайшли втілення в схваленому на І Національному конгресі з біоетики (Київ, 2001) проекті «Етичного кодексу українського лікаря». Подальше обговорення принципів біоетики відбулося на Міжнародному симпозіуму з біоетики (Київ, 2002). У цьому контексті варто згадати, що етику в галузі науки і технологій ЮНЕСКО зробила одним з пріоритетів своєї стратегії на 2002-2007 роки. У етичному кодексі українського лікаря розглянути питання конфіденційності – нерозголошення лікарем професійної та приватної інформації без дозволу пацієнта.

Текст клятви лікаря затверджений Указом Президента України від 15 червня 1992 р. № 349.

В Україні на законодавчому рівні лікарську таємницю закріплено в Законі України «Основи законодавства України про охорону здоров'я» від 19 листопада 1992 р. № 2801-XII. У ст. 40 цього Закону зазначається, що меди-

чні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина, не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків. Обов'язок зберігати лікарську таємницю закріплений і ст. 78 даного Закону, у якій вказано, що медичні і фармацевтичні працівники мають дотримуватися «вимог професійної етики і деонтології, зберігати лікарську таємницю».

При використанні інформації, що становить лікарську таємницю, у навчальному процесі, науково-дослідній роботі, у тому числі у випадках її публікації в спеціальній літературі, повинна бути забезпечена анонімність пацієнта.

Випускники медичних спеціальностей вищих медичних навчальних закладів приносять Присягу лікаря України (ст. 76 Закону України «Основи законодавства України про охорону здоров'я»).

Відповідно до ст. 39 цього Закону, медичний працівник зобов'язаний надати пацієнтові в доступній формі інформацію про стан його здоров'я, мету проведення запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, у тому числі наявність ризику для життя і здоров'я. Пацієнт, який досяг повноліття, має право на отримання достовірної і повної інформації про стан свого здоров'я, у тому числі на ознайомлення з відповідними медичними документами, що стосуються його здоров'я. Забороняється вимагати та подавати за місцем роботи або навчання інформації про діагноз та методи лікування пацієнта.

Таким чином, предмет лікарської таємниці складають:

- стан здоров'я пацієнта;
- хвороби і діагноз;
- огляд і його результати;
- методи лікування;
- інтимна і сімейна сторони життя пацієнта;
- інші відомості, отримані при медичному обстеженні.

Конфіденційність особистої інформації про людину гарантує ст. 32 Конституції України і ст. 286 Цивільного кодексу України, яка гарантує кожному право на право на таємницю про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також відомості, одержані при медичному обстеженні. Згідно зі ст. 7 Закону України «Про захист персональних даних» до обробки персональних даних про здоров'я людини пред'являються особливі вимоги. Персональні дані такого характеру можуть бути предметом збору та обробки тільки, якщо це необхідно з метою охорони здоров'я, встановлення медичного діагнозу, для забезпечення опіки або лікування або надання медичних послуг за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я, на якого покладено обов'язки щодо забезпечення захисту персональних даних і на якого поширюється законодавство про лікарську таємницю.

Гарантією збереження лікарської таємниці є те, що лікарі та інші медичні працівники не можуть бути допитані як свідки ні в цивільному, ні в кримінальному процесі щодо відомостей, що становлять лікарську таємницю (п.2 ст.51 ЦПК України та п.4 ч.2 ст. 65 КПК України).

Якщо інформація про хворобу пацієнта може погіршити стан його здоров'я або погіршити стан здоров'я фізичних осіб, визначених частиною другою цієї статті, зашкодити процесові лікування, медичні працівники мають право надати неповну інформацію про стан здоров'я пацієнта, обмежити можливість їх ознайомлення з окремими медичними документами.

3.2.7.2. Правовий порядок розголошення лікарської таємниці

Відповідно до частини другої статті 39 Закону України «Основи законодавства України про охорону здоров'я» батьки (усиновлювачі), опікун, піклувальник мають право на отримання інформації про стан здоров'я дитини (до 18 років) або підопічного (недієздатної особи).

Тимчасовий доступ до документів, що містять лікарську таємницю, може надати слідчий суддя або суд в рамках розслідування кримінальної справи, як-

що при цьому буде встановлено, що інших способів отримання необхідної слідству інформації немає (ч.6 ст. 163 КПК України).

Також *лікарська таємниця може бути розголошена без згоди пацієнта у таких випадках*:

– розкриття медичним працівником відомостей про позитивний ВІЛ-статус особи партнеру (партнерам) дозволяється, якщо людина, що живе з ВІЛ, звернеться до медичного працівника з відповідним письмово підтвердженим проханням або ж людина, що живе з ВІЛ, померла, втратила свідомість або існує ймовірність того, що вона не отямиться і не відновить свою здатність надавати усвідомлену інформовану згоду.

– допускається передача відомостей про стан психічного здоров'я особи та надання їй психіатричної допомоги без згоди особи або без згоди її законного представника для організації надання особі, яка страждає важким психічним розладом, психіатричної допомоги; проведення досудового розслідування або судового розгляду за письмовим запитом слідчого, прокурора і суду.

– відомості про лікування в наркологічному закладі можуть бути розголошені правоохоронним органам у разі притягнення такої особи до кримінальної або адміністративної відповідальності.

У ст. 80 Закону України «Основи законодавства України про охорону здоров'я» вказується, що особи, винні в порушенні законодавства про охорону здоров'я, несуть цивільну, адміністративну або кримінальну відповідальність згідно із законодавством.

За незаконне розголошення лікарської таємниці встановлена кримінальна відповідальність (ст. 145 КК України). Так, умисне розголошення лікарської таємниці особою, якій вона стала відома у зв'язку з виконанням професійних чи службових обов'язків, якщо таке діяння спричинило тяжкі наслідки, – карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до двохсот сорока годин, або позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, або виправними роботами на строк до двох років.

Згідно зі ст. 132 КК України розголошення службовою особою лікувального закладу, допоміжним працівником, який самочинно здобув інформацію, або медичним працівником відомостей про проведення медичного огляду особи на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби, що є небезпечною для життя людини, або захворювання синдром набутого імунодефіциту (СНІД) та його результатів, що стали їм відомі у зв'язку з виконанням службових або професійних обов'язків, – карається штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до двохсот сорока годин, або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

3.2.7.3. Етичні принципи психіатричної допомоги

У Гавайській декларації II, яка схвалена Генеральною асамблеєю Всесвітньої медичної асамблеї 10 липня 1983 р., вказується, що метою психіатрії є лікування психічних хвороб і покращення психічного стану. Застосовуючи свої можливості, у відповідності з отриманими науковими знаннями і прийнятими етичними принципами психіатр повинен служити вищим інтересам пацієнта, а також турбуватися про загальне благо і справедливе розміщення ресурсів охорони здоров'я. Досягнення цих цілей вимагає безперервних досліджень і постійного навчання медичного персоналу, пацієнтів і громадськості.

Психіатр прагне до таких відносин із пацієнтом, які ґрунтуються на взаємній згоді. В оптимальному варіанті це вимагає конфіденційності, співпраці і взаємної довіри. З деякими пацієнтами встановлення таких взаємних відносин може бути неможливим. У такому разі контакт встановлюється з родичами або іншими людьми, близькими пацієнту. Якщо взаємовідносини встановлені не в терапевтичних цілях, а в цілях судової психіатрії чи інших, їх природа мусить бути в подробицях пояснена зацікавленим особам.

Що б не було сказано пацієнту або не було записано протягом обстеження чи лікування, це повинно бути конфіденційно, якщо тільки пацієнт не звіль-

нив психіатра від такого зобов'язання або розкриття інформації є необхідним для попередження спричинення серйозної шкоди пацієнту чи іншим особам. У цьому випадку пацієнт повинен бути поінформований про порушення конфіденційності.

У Резолюції «Захист осіб з психічними захворюваннями та поліпшення психіатричної допомоги» № 46/119, котра прийнята Генеральною Асамблею ООН 18 лютого 1992 р., принцип 6 стосовно конфіденційності встановлює, що повинно поважатися право на конфіденційність інформації щодо всіх осіб, до яких застосовуються дані принципи.

Слід зазначити, що співзвучні вимоги містяться і в Законі України «Про психіатричну допомогу» від 22 лютого 2000 р. № 1489-III. Зокрема, ст. 6 «Конфіденційність відомостей про стан психічного здоров'я особи та надання психіатричної допомоги» цього Закону передбачає, що медичні працівники, інші фахівці, які беруть участь у наданні психіатричної допомоги, та особи, яким у зв'язку з навчанням або виконанням професійних, службових, громадських чи інших обов'язків стало відомо про наявність у особи психічного розладу, про факти звернення за психіатричною допомогою та лікування в психіатричному закладі чи перебування в психоневрологічних закладах для соціального захисту або спеціального навчання, а також інші відомості про стан психічного здоров'я особи, її приватне життя, не можуть розголошувати ці відомості, крім випадків, передбачених ч. 3, 4, 5 цієї статті.

Право на одержання і використання конфіденційних відомостей про стан психічного здоров'я особи та надання їй психіатричної допомоги має сама особа чи її законний представник.

За усвідомленою згодою особи або її законного представника відомості про стан психічного здоров'я цієї особи та надання їй психіатричної допомоги можуть передаватися іншим особам лише в інтересах особи, яка страждає на психічний розлад, для проведення обстеження та лікування чи захисту її прав і законних інтересів, для здійснення наукових досліджень, публікацій у науковій літературі, використання в навчальному процесі.

Допускається передача відомостей про стан психічного здоров'я особи та надання їй психіатричної допомоги без згоди особи або без згоди її законного представника для:

1) організації надання особі, яка страждає на тяжкий психічний розлад, психіатричної допомоги;

2) провадження дізнання, попереднього слідства або судового розгляду за письмовим запитом особи, яка проводить дізнання, слідчого, прокурора та суду.

У листку непрацездатності, що видається особі, яка страждає на психічний розлад, діагноз психічного розладу вписується за згодою цієї особи, а в разі її незгоди – лише причина непрацездатності (захворювання, травма або інша причина).

Забороняється без згоди особи або без згоди її законного представника та лікаря-психіатра, який надає психіатричну допомогу, публічно демонструвати особу, яка страждає на психічний розлад, фотографувати її чи робити кінозйомку, відеозапис, звукозапис та прослуховувати співбесіди особи з медичними працівниками чи іншими фахівцями при наданні їй психіатричної допомоги.

Забороняється вимагати відомості про стан психічного здоров'я особи та про надання їй психіатричної допомоги, за винятком випадків, передбачених цим Законом та іншими законами.

Документи, що містять відомості про стан психічного здоров'я особи та надання їй психіатричної допомоги, повинні зберігатися з додержанням умов, що гарантують конфіденційність цих відомостей. Вилучення оригіналів цих документів та їх копіювання може здійснюватися лише у випадках, встановлених законом.

Щодо інформації про стан психічного здоров'я особи та надання психіатричної допомоги, згідно ст. 26 Закону України «Про психіатричну допомогу» лікар-психіатр зобов'язаний пояснити особі, якій надається психіатрична допомога, з урахуванням її психічного стану, у доступній формі інформацію про стан її психічного здоров'я, прогноз можливого розвитку захворювання, про застосу-

вання методів діагностики та лікування, альтернативні методи лікування, можливий ризик та побічні ефекти, умови, порядок і тривалість надання психіатричної допомоги, її права та передбачені цим Законом можливі обмеження цих прав при наданні психіатричної допомоги. Право на одержання зазначеної інформації щодо неповнолітнього віком до 15 років та особи, визнаної у встановленому законом порядку недієздатною, мають їх законні представники.

Особа при наданні їй психіатричної допомоги або її законний представник має право на ознайомлення з історією хвороби та іншими документами, а також на отримання в письмовому вигляді будь-яких рішень щодо надання їй психіатричної допомоги.

У випадках, коли повна інформація про стан психічного здоров'я особи може завдати шкоди її здоров'ю або призвести до безпосередньої небезпеки для інших осіб, лікар-психіатр або комісія лікарів-психіатрів можуть таку інформацію обмежити. У цьому разі лікар-психіатр або комісія лікарів-психіатрів інформує законного представника особи, враховуючи особисті інтереси особи, якій надається психіатрична допомога. Про надану інформацію або її обмеження робиться запис у медичній документації.

Особи, винні у порушенні законодавства про психіатричну допомогу, несуть відповідальність згідно з законами України (ст. 33 Закону України «Про психіатричну допомогу»).

Охорона здоров'я є пріоритетним напрямом діяльності суспільства і держави, одним із головних чинників виживання та розвитку народу України. Державні, громадські або інші органи, підприємства, установи, організації, посадові особи та громадяни зобов'язані забезпечити пріоритетність охорони здоров'я у власній діяльності, не завдавати шкоди здоров'ю населення і окремих осіб, у межах своєї компетенції надавати допомогу хворим, інвалідам та потерпілим від нещасних випадків, сприяти працівникам органів і закладів охорони здоров'я в їх діяльності, а також виконувати інші обов'язки, передбачені законодавством про охорону здоров'я.

Лікар зобов'язаний цінувати довір'я хворого і виправдати його та зберегти у таємниці всі відомості, отримані від нього. Цей принцип не лише можна, але і необхідно порушити, якщо збереження таємниці призведе до заподіяння шкоди як хворому, його родичам, так і суспільству загалом.

3.3. Охорона інтелектуальної власності

3.3.1. Історіографія формування правової охорони інтелектуальної власності

Історично передумови формування інституту монопольних прав на розповсюдження творчих результатів склалися наприкінці XV ст. у Європі.

Підставою для надання привілею були різні причини: винайдення нового способу вироблення певних виробів, розвиток виробництва, війська, зброї, пошук та добування корисних копалин, удосконалення певної системи, заміна привізних товарів власними, будь-яка новизна, що приносила певну вигоду, прибуток особі, яка видає привілей, чи її державі.

Венеціанська Республіка у 1474 р. першою прийняла положення про привілеї «Парте Венеціана». Разом із наданням привілеїв почали складатися їх правові засади. Основними з них були: корисність, новизна для держави, виключне право (монополія) на його використання особи, яка його створила, покарання порушника наданого привілею.

Початком стало відоме відкриття Й. Гутенбергом способу друкування книг на друкарських станках, що зробило процес тиражування книг менш трудомістким, більш швидким і знизило ціни на книги. Згодом це призвело до зіткнення інтересів книговидавців, які намагалися друкувати одні й ті самі популярні твори. За таких обставин королівськими законами почали вводитися так звані привілеї, що надавали окремим книговидавцям монопольне право на друк певних творів, забороняючи іншим друкувати той самий твір. Система привілеїв проіснувала до початку XVIII ст. і була гарантією економічних інтересів книговидавців. Саме королівські привілеї вважаються попередниками сучасного авторського права, оскільки вони опосередковано захищали права автора, бо для

отримання монопольного права на друк слід було документально підтвердити наявність згоди автора на це.

Першим законодавчим актом у галузі авторського права, котрий був спрямований на захист прав автора, уважається Статут королеви Анни, прийнятий в Англії в 1709 р., за яким автор отримав монопольне право видавати та перевидавати свій твір протягом 14 років (строк правової охорони).

В умовах буржуазних революцій під впливом ідей природних прав поширюються поняття літературної та промислової власності, яка подібно праву власності на матеріальні цінності розуміється як природне право людини на продукт своєї праці і можливість вільно розпоряджатися результатами творчої діяльності на свій розсуд. Наприкінці XVIII – на початку XIX ст. право літературної та промислової власності закріпилося в національних законах багатьох країн Західної Європи (Франції, Німеччини, Данії та ін.).

Норми, що охороняють творчий результат, постійно змінюються і ускладнюються під впливом науково-технічного прогресу, який безперервно породжує нові форми відтворення та розповсюдження інтелектуального продукту. Значну роль у процесі законотворення охорони інтелектуальної власності відіграють міжнародні конвенції, які закладають засади розвитку національних правових систем у сфері охорони інтелектуальної власності. Найдавнішими і найвідомішими серед них є Паризька конвенція про охорону промислової власності, яка підписана 20 березня 1883 р., включаючи будь-яку з її переглянутих редакцій, та Бернська конвенція про охорону літературних і художніх творів, прийнята 9 вересня 1886 р., включаючи будь-яку з її переглянутих редакцій.

У Росії перший нормативний акт про привілеї був прийнятий у 1723 р. під назвою «Правила выдачи привилегии на заведение фабрик». Цим актом певною мірою було упорядковано видання привілеїв. 17 червня 1812 р. був прийнятий Закон Росії «О привилегиях на разные изобретения и открытия в художествах и ремеслах». Цим законом передбачалася видача привілеїв на власні винаходи і ті, що завозилися із-за кордону, строком на три, п'ять і десять років. Строк дії привілеїв за цим законом становив від 3,5 до 10 років. Привілеї надавав без пе-

ревірки суті винаходу міністр внутрішніх справ після розгляду питання Державою радою.

Основним нормативно-правовим актом, який регулював відносини у сфері авторських прав у Російській імперії, був Закон «Про авторське право від 20 березня 1911 р.», норми якого базувалися на традиції ставлення до інституту авторського права як до різновиду права власності: права авторів оголошувалися літературною власністю, яка могла повністю відчужуватися на увесь строк охорони авторських прав насамперед видавцями, що могли купувати права по відношенню до всіх творів.

У Законі «Про авторське право від 20 березня 1911 р.» вперше на законодавчому рівні були класифіковані об'єкти, які охороняються авторським правом відповідно до галузей творчої діяльності. Згідно зі ст. 1, до них належали:

– літературні твори: як письмові, так й усні (промови, лекції, реферати, доповіді, повідомлення, проповіді тощо);

– музичні твори, у тому числі й музичні імпровізації;

– художні твори (живопис, гравірування та інші види графічного мистецтва);

– фотографії[56] та подібні їм твори.

Ст. 2 Закону «Про авторське право від 20 березня 1911 р.» встановлювала виключність права автора у можливості використання власного твору.

Для адаптації російського законодавства до європейського[57] у ст. 4 Закону «Про авторське право від 20 березня 1911 р.» вказувалося, що авторське право визнавалося і щодо неопублікованих творів та творів опублікованих за кордоном за усіма авторами та їх правонаступниками, незалежно від їх підданства, визначалося поняття співавторства (ст. 5), розрізняючи подільне і неподільне співавторство (ст. 15), окреслено коло спадкоємців, до яких може перейти

[56] Новацією стало включення фотографічних творів в одному нормативному акті з іншими об'єктами авторського права.

[57] У Російській імперії до початку XX ст. авторське право на твір у особи виникало з моменту його опублікування. Твори видані за кордоном правову охорону не отримували.

авторське право (ст. 6) та встановлені строки охорони авторських прав (ст. 11, 12).

Згідно зі ст.17 Закону «Про авторське право від 20 березня 1911 р.» протягом п'ятдесяти років поширювалася охорона на анонімні твори, або твори під псевдонімом. Відповідно до ст.18 відлік строку охорони авторських прав починався з 1 січня року смерті автора.

Вагомим поступом у розвитку інституту авторського права в Російській імперії є визнання двоякості юридичної природи авторського права, що полягає у комплексі особистих немайнових і майнових прав.

З прийняттям Закону «Про авторське право від 20 березня 1911 р.» вперше на законодавчому рівні було визнано право на авторське ім'я, яке визначало використання твору під своїм власним іменем, під псевдонімом або анонімно; закріплювалося право автора на недоторканність твору, що полягало у недопущенні без згоди автора або його спадкоємців видавати або використовувати твір з будь-якими змінами (ст. 20). Під час використання твору або його частин необхідно було вказувати ім'я автора та джерело запозичення (ст. 19).

Закон «Про авторське право від 20 березня 1911 р.» установлював, що закони і урядові розпорядження, постанови законодавчих установ, суспільних зібрань і матеріали, на яких ці закони, розпорядження і постанови ґрунтуються, а також рішення судових установ (ст. 37) не належать до об'єктів авторського права.

Нововведенням, що було закріплено в Законі «Про авторське право від 20 березня 1911 р.», було право перекладу. Воно існувало за умови вказівки на титульному листі або у передмові про збереження за автором цього права. Виключне право перекладу зберігалося за автором протягом 10 років з моменту публікації оригіналу за умови друку протягом 5 років з цього ж моменту перекладу (ч. 2 ст. 33). Права автора по використанню твору розширилося: вперше було вказано, що переробка оповідального твору у драматичну форму або навпаки допускається лише зі згоди автора або його спадкоємців (ст. 31).

Що стосується художніх творів, то виникнення авторського права на них у попередньому законодавстві залежало від реєстрації цих творів. Згідно із Законом «Про авторське право від 20 березня 1911 р.» художнику належали всі права на його твір. Купівля твору у художника не переносила на покупця твору авторського права на сам твір, якщо це не обумовлювалося у договорі. Авторське право художнику на твір не було абсолютним. Ст. 52 встановлювалося, що право виставляти, відтворювати і розповсюджувати портрети і бюсти, створені художником, належить особам, з яких написаний портрет або бюст та їх спадкоємцям.

Що стосується захисту авторських прав композиторів, то ст. 42 Закону 1911 р. гарантувала виключні права перекладати свої твори на один чи декілька голосів, інші тони, окремі інструменти чи на оркестр. Крім того, автори отримали право перекладу власних творів на механічні інструменти (фонографи, грамофони). Однак це право обмежувалося у тому, що композитор, який почав видавати грамофонні платівки, зобов'язаний був видавати дозволи всім бажаючим. Якщо композитор не міг дійти добровільної згоди з особою, що хотіла отримати ліцензію то така ліцензія надавалася судом у примусовому порядку. У законі вказувалося, що публічне виконання музичних творів без згоди композитора допускалося, якщо воно здійснювалося: не з метою отримання матеріальної вигоди; під час народних гулянь; для збору коштів на благодійництво і виконавці не отримували винагороди. Такі музичні твори, як романси, ораторії, симфонії не могли виконуватися публічно без згоди композитора за умови, що він на кожному екземплярі твору застеріг це своє право (ст. 48).

Новацією стало включення фотографічних творів в одному нормативному акті з іншими об'єктами авторського права. Для них закон створював певні формальності, які не застосовувалися до інших форм художньої творчості: фотографія не могла бути анонімною, на ній повинні були вказуватися ім'я, прізвище, адреса фотографа та рік видання. Авторські права фотографів захищалися тільки в творах зроблених фотографічним, механічним або хімічним способом.

Строк охорони фотографічних творів тривав 10 років, а особливо цінні збірники фотографічних творів, що мали культурну та історичну цінність 25 років.

Таким чином, Закон «Про авторське право від 20 березня 1911 р.» був істотним кроком вперед у процесі розвитку законодавства у сфері авторського права в Російській імперії та спробою адаптації його до світових стандартів та положень Бернської конвенції.

3.3.2. Сучасний стан правової охорони інтелектуальної власності

Всесвітня конвенція про авторське право була розроблена і прийнята на спеціальній конференції, що відбулася під егідою ЮНЕСКО 6 вересня 1952 р. у Женеві. Головна мета Конвенції – створення універсального режиму для охорони і захисту авторських прав на літературні, наукові і художні твори на міжнародному рівні. Маються на увазі такі різновиди творів, як письмові, музичні, драматичні і кінематографічні, твори живопису, графіки та скульптури. У Конвенції досить чітко регламентується порядок публікації творів, оформлення авторства, конкретні гарантії матеріальних і нематеріальних прав авторів.

Будь-яка договірна держава, за внутрішнім законодавством якої неодмінною умовою охорони авторського права є дотримання формальностей, як-от: депонування примірників, реєстрація, застереження про збереження авторського права, нотаріальні посвідчення, сплата зборів, виготовлення або випуск у світ примірників твору на території цієї держави, – має вважати ці вимоги виконаними щодо тих творів, які охороняються на підставі цієї Конвенції і які вперше випущені у світ поза територією цієї держави і автори яких не є її громадянами, якщо, починаючи з першого випуску у світ цих творів, усі їхні примірники, випущені з дозволу автора або будь-якого іншого власника його прав, носитимуть знак © із зазначенням імені володаря авторського права і року першого випуску у світ; цей знак, ім’я і рік випуску мають бути розташовані таким чином і на такому місці, які б ясно показували, що авторське право зберігається. У Конвенції передбачається також, що період охорони авторського права не може бути коротшим за життя автора і 25 років після його смерті.

Конвенція про заснування Всесвітньої організації інтелектуальної власності підписана в Стокгольмі 14 липня 1967 р. та змінена 2 жовтня 1979 р. Цілями організації є сприяння охороні інтелектуальної власності в усьому світі шляхом співробітництва держав і у відповідних випадках через взаємодію з будь-якою іншою міжнародною організацією.

Всесвітня організація інтелектуальної власності (ВОІВ) сприяє охороні інтелектуальної власності в усьому світі, гармонізації певних норм міжнародного права у сфері інтелектуальної власності та адміністративного управління окремими глобальними договорами, становленню і підтримці законності прав промислової власності.

Інтелектуальна власність включає права, які стосуються:

– літературних, художніх і наукових творів;

– виконавчої діяльності артистів, звукозапису;

– радіо- і телевізійних передач;

– винаходів у всіх галузях людської діяльності;

– наукових відкриттів;

– промислових зразків, знаків обслуговування, фірмових найменувань і комерційних позначень;

– захисту проти недобросовісної конкуренції;

– а також усі інші права, що відносяться до інтелектуальної діяльності в промисловій, науковій, літературній і художній сфері.

Закони України «Про приєднання України до Бернської конвенції про охорону літературних і художніх творів (Паризького акта від 24 липня 1971 року, зміненого 2 жовтня 1979 року)» від 31 травня 1995 р. № 189/95-ВР і «Про приєднання України до Договору Всесвітньої організації інтелектуальної власності про авторське право» від 20 вересня 2001 р. № 2733-III є правовою підставою для продовження охорони прав українських авторів, сприяють розширенню співробітництва України із зарубіжними країнами в цій сфері.

Протягом останнього десятиліття з розвитком подій у галузі економіки, техніки і права посилився інтерес міжнародних організацій до інтелектуальної власності.

Інтелектуальна власність стала невід'ємною частиною системи багатосторонньої торгівлі, що відображено в Угоді про торговельні аспекти прав інтелектуальної власності (Угода ТРІПС), підписаній 15 квітня 1994 р. Цілями цієї Угоди є охорона і реалізація прав інтелектуальної власності. Дана Угода повинна сприяти технічному прогресу та переданню і розповсюдженню технології для взаємної вигоди виробників і користувачів технологічних знань, сприяючи соціально-економічному добробуту, і для досягнення балансу прав і обов'язків. У даному документі термін «інтелектуальна власність» поширюється на всі категорії інтелектуальної власності: товарні знаки, географічні назви, промислові зразки, патенти, топології (топографії) інтегральних мікросхем, охорону закритої інформації.

Принципи Угоди визначають, що при формуванні або вдосконаленні своїх національних законів і правил члени можуть здійснювати заходи, необхідні для захисту здоров'я та харчування населення, а також спонукати суспільний інтерес у секторах, життєво важливих для їх соціально-економічного та технологічного розвитку, за умови, що такі заходи відповідають положенням цієї Угоди.

У розд. 7 «Захист нерозголошуваної інформації» зазначається, що в процесі забезпечення ефективного захисту проти недобросовісної конкуренції, як передбачено в ст. 10-bis Паризької конвенції (1967 р.), члени повинні надавати захист нерозголошуваної інформації. Фізичні і юридичні особи повинні мати можливість перешкоджати тому, щоб інформація, яка законно знаходиться під їх контролем, розголошувалась, збиралась або використовувалась іншими особами без їхньої згоди у такий спосіб, який суперечить чесній комерційній практиці, якщо така інформація:

– є секретною у тому розумінні, що вона як єдине ціле або у точній сукупності та поєднанні її компонентів не є загальновідомою або доступною для осіб у тих колах, що звичайно мають справу з інформацією, про яку йдеться;

– має комерційну цінність через те, що вона є секретною;

– зберігається у секреті внаслідок вжиття за відповідних обставин певних заходів особою, яка законно здійснює контроль за цією інформацією.

Для цього положення вислів «спосіб, який суперечить чесній комерційній практиці» означає принаймні таку практику, як порушення контракту, порушення довіри та спонукання до порушення довіри, і включає придбання інформації, що не підлягає розкриттю, третіми особами, які знали або не могли не знати, що з цим придбанням пов'язана така практика.

Договір Всесвітньої організації інтелектуальної власності про авторське право, прийнятий Дипломатичною конференцією 20 грудня 1996 р., передбачає, що охорона авторських прав поширюється на форму вираження, а не на ідеї, процеси, методи діяльності або математичні концепції як такі.

Інформація про управління правами означає інформацію, яка ідентифікує твір, автора твору, володаря будь-якого права на твір або інформацію про умови використання твору, а також будь-які цифри або коди, у яких подана така інформація, якщо будь-яка з цих складових інформації додана до примірника твору або фігурує у зв'язку із розповсюдженням твору серед широкої публіки.

Управління охороною прав на об'єкти інтелектуальної власності є важливим напрямом публічного управління, оскільки від результативності його здійснення залежать:

– рівень забезпечення прав фізичних осіб, які мають у своєму користуванні, володінні або розпорядженні об'єкти інтелектуальної власності;

– рівень економічного зростання держави;

– престиж країни у світі.

У загальному розумінні метод управління становить правовий засіб досягнення поставленої мети, розв'язань завдань, що виникли. По суті, методи – це способи впливу, звернені до поведінки суб'єктів соціального життя. Вирішення

завдань щодо охорони прав на об’єкти інтелектуальної власності здійснюється суб’єктами управління через використання методів управлінського впливу.

Для методів управління у сфері охорони прав на об’єкти інтелектуальної власності характерним є:

– використання суб’єктами управління в зазначеній сфері для вирішення завдань, що стоять перед ними;

– забезпечення режиму законності у володінні, користуванні, розпорядженні правами на об’єкти інтелектуальної власності;

– запобігання, припинення порушень режиму володіння, користування, розпорядження правами на об’єкти інтелектуальної власності;

– притягнення осіб, котрі скоїли правопорушення, пов’язані з порушенням встановленого режиму володіння, користування або розпорядження правами на об’єкти інтелектуальної власності, до юридичної відповідальності;

– застосування повсякденно та вибірково залежно від необхідності вирішення того або іншого завдання;

– вираження у взаємодії суб’єкта управління з об’єктом управління;

– найбільш повне та всебічне встановлення меж владних повноважень суб’єктів управління.

Зобов’язання стосовно інформації про управління правами передбачають відповідні ефективні засоби юридичної відповідальності по відношенню до будь-якої особи, яка свідомо чинить недозволене поширення, імпортування для розповсюдження, передання в ефір або розповсюдження серед широкої публіки творів або примірників творів, знаючи, що має місце недозволене усунення або зміна будь-якої електронної інформації про управління правами.

Відповідно до ст. 14 Договору Всесвітньої організації інтелектуальної власності про авторське право, прийнятого Дипломатичною конференцією 20 грудня 1996 р., визначено, що договірні сторони передбачають наявність у їх законах заходів щодо забезпечення прав, які дозволяють ефективно протидіяти будь-яким актам порушення прав, передбачених цим Договором, включаючи

термінові заходи для запобігання порушень та заходи як стримуючий засіб від подальших порушень.

У 2001 р. міжнародні відносини у сфері інтелектуальної власності зазнали змін, котрі дають змогу винахідникам і авторам усього світу користуватися більш надійною охороною, більш широкими і ефективними засобами захисту своїх творів на сьогоднішньому глобальному ринку, який, у свою чергу, характеризується високим суперництвом.

Об'єктами охорони промислової власності є патенти на винаходи, корисні моделі, промислові зразки, товарні знаки, знаки обслуговування, фірмові найменування та вказівки про походження чи найменування місця походження, а також припинення недобросовісної конкуренції.

Договір про патентне право, прийнятий 15 січня 2002 р., спрощує формальності й раціоналізує процедури по відношенню до національних і регіональних патентних заявок[58], а також положення та інструкції цього Договору застосовуються до виданих національних і регіональних патентів на винаходи та до національних і регіональних додаткових патентів, які є чинними для будь-якої договірної сторони (ст. 3), спрощує вимоги до дати подання заявки, визначає стандартний набір формальних вимог, передбачених Договором про патентне право, передбачає стандартні бланки, спрощені процедури у відомостях, засоби для попередження випадкової втрати прав і основні принципи електронного подання заявок. Таким чином, користувачі патентної системи можуть спиратися на спрощені процедури подання національних заявок і підтримку в силі патентів у всіх державах-учасницях. Для гармонізації патентного права, що виходить за рамки формальних вимог, Постійний комітет Всесвітньої організації інтелектуальної власності з патентного права прийняв рішення про початок роботи над гармонізацією матеріальних норм патентного права. Комітет сконцентрував увагу на питаннях, що безпосередньо пов'язані з виданням патентів, на питаннях патентоспроможності, включаючи визначення рівня визначеності, новизни, винахідни-

[58] Конвенція про уніфікацію деяких положень патентного права (ETS № 47) від 27 листоп. 1963 р., Європейська конвенція про міжнародну патентну класифікацію від 19 груд. 1954 р.

цького рівня (неочевидності і промислового застосування), корисності, складання і тлумачення пунктів формули з вимогами достатнього розкриття[59].

Більш довгостроковою метою розвитку міжнародної патентної системи є забезпечення механізмів і програм, за допомогою яких винахідники матимуть доступ до національних, регіональних і ефективних міжнародних систем правової охорони, які дозволили б отримувати, підтримувати і захищати свої патенти, котрі:

– являються простими, недорогими, своєчасними і надійними, тобто такими, що відповідають вимогам надання ефективної охорони;

– сприяють використанню запатентованої технології у формі впровадження у виробництво, створення стимулів для інвестицій, міжнародного ліцензування чи комерційних угод або інших способів передання технологій.

3.3.3. Законодавче забезпечення регулювання правовідносин у сфері інтелектуальної власності в Україні

Необхідність створення в Україні ефективної системи охорони прав інтелектуальної власності викликана вимогою часу: незалежною країна не може бути без економічного розвитку, а розвинута незалежна економічна структура держави неможлива без політики захисту права інтелектуальної власності.

Проголошений Україною курс на інтеграцію до Європейського Союзу і вступ до Світової організації торгівлі актуалізують потребу забезпечення захисту прав на об’єкти авторських і суміжних прав та об’єкти промислової власності на рівні, який існує в економічно розвинених країнах.

Правовідносини у сфері інтелектуальної власності регулюються нормами Конституції України, Цивільного, Кримінального, Митного, Господарського кодексів України, Кодексу України про адміністративні правопорушення, спеціальними законами і підзаконними нормативними актами. Зокрема, ч. 4 ст. 13 Конституції України передбачено, що держава забезпечує захист прав усіх суб’єктів права власності і господарювання, соціальну спрямованість економіки. Усі суб’єкти права власності рівні перед законом. Частиною 1 ст. 41 Конститу-

[59] Про приєднання України до Договору про патентне право : закон України від 22 листоп. 2002 р. № 245-IV / Відомості Верховної Ради України. – 2003. – № 3. – Ст. 20.

ції України передбачено право кожного володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності. Згідно з ч. 1 ст. 54 Конституції України, громадянам гарантується свобода літературної, художньої, наукової творчості та захист інтелектуальної власності, їхніх авторських прав, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності. Відповідно до ч. 2 цієї статті, кожний громадянин має право на результати своєї інтелектуальної, творчої діяльності; ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом.

26 квітня 1970 р. Україна (УРСР) приєдналася до Всесвітньої організації інтелектуальної власності і в нинішній час є учасницею Міжнародного (Паризького) союзу з охорони промислової власності та Міжнародного (Бернського) союзу з охорони літературних і художніх творів.

Україна прийняла ряд спеціальних законів у сфері інтелектуальної власності: «Про авторське право і суміжні права», «Про охорону прав на сорти рослин» від 21 квітня 1993 р. № 3116-XII; три закони від 15 грудня 1993 р.: «Про охорону прав на винаходи і корисні моделі» № 3687-XII, «Про охорону прав на промислові зразки» № 3688-XII, «Про охорону прав на знаки для товарів і послуг» № 3689-XII; а також закони «Про охорону прав на топографії інтегральних мікросхем» від 5 листопада 1997 р. № 621/97-ВР, «Про видавничу справу» від 5 червня 1997 р. № 318/97-ВР, «Про розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних» від 23 березня 2000 р. № 1587-III.

Найважливішими міжнародними договорами, що діють у рамках ВОІВ, є:

– Паризька конвенція про охорону промислової власності від 20 березня 1883 р. (у редакції від 2 жовтня 1979 р.), якою передбачено дії щодо захисту прав на винаходи, корисні моделі, промислові зразки, знаки для товарів і послуг, фірмові найменування, зазначення походження товарів; для України набула чинності 25 грудня 1991 р.;

– Всесвітня конвенція про авторське право від 6 вересня 1952 р., ратифікована Україною 23 грудня 1993 р., набрала чинності 3 листопада 1995 р.;

– Бернська конвенція про охорону літературних і художніх творів від 9 вересня 1886 р., якою передбачено правову охорону авторських прав на кожний літературний, науковий чи художній твір, незалежно від форми його вираження. Україна 31 травня 1995 р. приєдналася до Паризького акта від 24 липня 1971 р. (зі змінами від 2 жовтня 1979 р.), який практично є новою редакцією Бернської конвенції;

– Міжнародна (Римська) конвенція про охорону інтересів виконавців, виробників фонограм і організацій мовлення від 26 жовтня 1961 р., якою передбачено охорону прав виконавців (акторів, співаків, музикантів, танцюристів або інших осіб, які виконують роль, співають, читають, декламують, виконують або будь-яким іншим способом беруть участь у виконанні творів літератури чи мистецтва), виробників фонограм і організацій мовлення; дата приєднання України – 20 вересня 2001 р.;

– Конвенція (Женевська) про охорону інтересів виробників фонограм від незаконного відтворення їхніх фонограм від 29 жовтня 1971 р., якою передбачено охорону інтересів авторів, артистів, виконавців і виробників фонограм від незаконного відтворення та поширення фонограм; дата приєднання України – 15 червня 1999 р.

Країни – учасниці підписаних конвенцій погодилися прийняти на себе зобов’язання здійснити всі передбачені цими міжнародними документами заходи, проте з урахуванням положень чинного національного законодавства.

Захист прав інтелектуальної власності здійснюється також у рамках антимонопольного законодавства України. Згідно з нормами Закону України «Про захист від недобросовісної конкуренції» Антимонопольний комітет України, який має розгалужену систему регіональних представництв, здійснює захист прав інтелектуальної власності в адміністративному порядку.

Спеціальним законодавством у сфері інтелектуальної власності передбачена можливість оскарження рішень щодо набуття прав на об’єкти інтелектуаль-

ної власності до Апеляційної палати Державного департаменту інтелектуальної власності.

З метою досягнення в Україні захисту прав інтелектуальної власності на рівні міжнародних стандартів протягом останнього часу було прийнято низку нормативно-правових актів, зокрема:

– у 2003 р. Верховною Радою України прийнято Цивільний кодекс України, що містить окрему книгу «Право інтелектуальної власності», у якій зосереджені загальні норми щодо набуття, здійснення та захисту прав інтелектуальної власності в Україні;

– набув чинності Закон України «Про внесення змін до деяких законодавчих актів України щодо правової охорони інтелектуальної власності», яким законодавство України у сфері інтелектуальної власності приведено в повну відповідність до норм Угоди ТРІПС, яка є основною угодою Світової організації торгівлі. Даним Законом значно посилена відповідальність за порушення прав інтелектуальної власності, передбачено положення стосовно запобіжних заходів, які ще до пред'явлення позовної заяви можуть бути вжиті за ухвалою суду (ст. 50 Угоди ТРІПС);

– для вирішення проблеми піратства у сфері авторського права і суміжних прав у 2002 р. прийнято Закон України «Про особливості державного регулювання діяльності суб'єктів господарювання, пов'язаної з виробництвом, експортом, імпортом дисків для лазерних систем зчитування» від 17 січня 2002 р. № 2953-III, прийнято низку постанов Кабінету Міністрів України, спрямованих на запровадження дієвих механізмів щодо недопущення виробництва та розповсюдження контрафактної продукції;

– у липні 2002 р. Верховною Радою України прийнято новий Митний кодекс України, який містить розділ щодо контролю за переміщенням через митний кордон України товарів, що містять об'єкти інтелектуальної власності. Положення зазначеного Кодексу відповідають міжнародним нормам, зокрема положенням Угоди про торговельні аспекти прав інтелектуальної власності (Угода ТРІПС), яка є однією з найважливіших угод Світової організації торгівлі;

– в Україні зроблені перші кроки до законодавчого врегулювання використання об’єктів інтелектуальної власності в мережі Інтернет. Зокрема, Верховною Радою України прийнято Закон України «Про внесення змін до деяких законів України з питань інтелектуальної власності» від 4 липня 2002 р. № 34-IV, відповідно до якого внесено зміни до ряду законодавчих актів України щодо використання об’єктів інтелектуальної власності в мережі Інтернет.

У зв’язку із цим до КУпАП були внесені зміни: спочатку включено ст. 51-2, якою передбачено відповідальність за порушення права на об’єкт права інтелектуальної власності, а потім ст. 164-9, якою передбачено відповідальність за незаконне розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп’ютерних програм, баз даних. Право інтелектуальної власності – суб’єктне право, а це означає, що завдання адміністративного розслідування у справах за ст. 51-2 КУпАП необхідно виконувати в повному обсязі і вживати всіх заходів для встановлення суб’єкта права, повідомляти останнього про порушення його права та долучати відповідну інформацію до матеріалів справи.

У травні 2003 р. Міністерство освіти і науки України, Міністерство внутрішніх справ України, Служба безпеки України, Державна податкова адміністрація України, Генеральна прокуратура України, Мінкультури України, Держпідприємництво України та Держмитслужба України затвердили Програму скоординованих дій правоохоронних та контролюючих органів по боротьбі з незаконним виробництвом, розповсюдженням і реалізацією аудіо- і відеопродукції, компакт-дисків та інших об’єктів інтелектуальної власності. У Програмі визначено основні напрямки співробітництва зазначених органів щодо проведення єдиної політики в боротьбі з порушеннями прав інтелектуальної власності на всій території нашої держави.

Основними напрямками діяльності Координаційної ради є забезпечення легального використання об’єктів інтелектуальної власності; проведення єдиної політики з боротьби з порушеннями прав інтелектуальної власності; удосконалення нормативно-правової бази в зазначеній сфері. З метою реалізації Про-

грами Координаційною радою передбачено проведення заходів для забезпечення контролю за правомірним використанням об'єктів інтелектуальної власності, зокрема:

– створення мережі регіональних центрів із захисту прав інтелектуальної власності;

– проведення заходів, направлених на припинення розповсюдження контрафактної продукції;

– сприяння громадським організаціям, які захищають права інтелектуальної власності і ведуть боротьбу з піратством;

– проведення освітянських заходів на підприємствах та організаціях, впровадження програм з питань інтелектуальної власності в навчальних закладах.

З метою забезпечення контролю за дотриманням законодавства у сфері інтелектуальної власності та забезпечення механізмів його реалізації у складі Держдепартаменту створено підрозділ контролю за дотриманням законодавства у сфері інтелектуальної власності – підрозділ державних інспекторів та державне підприємство «Інтелзахист», яке забезпечує видачу контрольних марок та ведення Єдиного реєстру одержувачів контрольних марок[60].

У ст. 51 Закону України «Про авторське право і суміжні права» визначено: порядок захисту авторського права та/або суміжних прав: захист особистих немайнових і майнових прав суб'єктів авторського права і суміжних прав здійснюється в порядку, встановленому адміністративним, цивільним і кримінальним законодавством.

Закон України «Про внесення змін до Кримінального кодексу України щодо захисту прав інтелектуально власності» від 9 лютого 2006 р. № 3423-IV передбачив відповідні зміни ст. 176 «Порушення авторського права і суміжних

[60] Рішення Колегії Міністерства освіти та науки України «Про проблеми захисту прав інтелектуальної власності та шляхи їх вирішення» від 4 грудня 2003 р. № 12/2-16.
За порушення порядку розповсюдження, а саме: у разі продажу примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних без маркування контрольними марками або з маркуванням контрольними марками, що мають серію чи містять інформацію, які не відповідають носію цього примірника, або номер, який не відповідає даним Єдиного реєстру одержувачів контрольних марок, настає адміністративна відповідальність за ст. 164-9 КУпАП.

прав», ст. 177 «Порушення прав на винахід, корисну модель, промисловий зразок, топографію інтегральної мікросхеми, сорт рослин, раціоналізаторську пропозицію», ст. 229 «Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару».

Право на судовий захист суб'єктивних прав інтелектуальної власності гарантується ст. 432 ЦК України.

В Указі Президента України «Про заходи щодо охорони інтелектуальної власності в Україні» від 27 квітня 2001 р. № 285/2001 надано доручення Кабінету Міністрів України вивчити питання щодо створення спеціалізованого Патентного суду.

Питання спеціалізації суддів щодо розгляду справ, пов'язаних із захистом прав інтелектуальної власності, детально опрацьовувалось Держдепартаментом інтелектуальної власності спільно з Вищим господарським судом України. З огляду на специфіку зазначеної категорії справ запровадження такої спеціалізації визнано доцільним. Така спеціалізація надасть можливість забезпечити однакове застосування норм чинного законодавства у сфері інтелектуальної власності і буде направлена на забезпечення надійного захисту прав інтелектуальної власності в судовому порядку.

Першим важливим кроком у напрямку спеціалізації суддів, які розглядають справи, пов'язані із захистом прав інтелектуальної власності, можна вважати утворення колегії суддів Вищого господарського суду України з розгляду справ, пов'язаних із захистом прав інтелектуальної власності, згідно з наказом Вищого господарського суду України від 26 липня 2001 р. № 19. Такі ж колегії відповідно до зазначеного наказу утворено у складі господарських судів Автономної Республіки Крим, областей, міст Києва та Севастополя та апеляційних господарських судів.

У рекомендації Президії Вищого господарського суду України «Про деякі питання практики вирішення спорів, пов'язаних із захистом прав інтелектуальної власності» від 10 червня 2004 р. № 04-5/1107 зазначено, що, відповідно до ч. 2 ст. 154 ГК України, до відносин, пов'язаних із використанням у господарській

діяльності прав інтелектуальної власності, застосовуються положення ЦК України з урахуванням особливостей, передбачених ГК України та іншими законами.

З урахуванням викладених вимог Конституції України та ЦК України господарські суди мають застосовувати міжнародні договори у сфері інтелектуальної власності, згода на обов'язковість яких надана Верховною Радою України. Перелік таких договорів наведено в інформаційному листі Вищого господарського суду України «Про нормативно-правові акти, що регулюють питання, пов'язані з охороною прав на об'єкти інтелектуальної власності» від 8 жовтня 2003 р. № 01-8/1199.

На сьогодні в Україні створені належні законодавчі засади охорони та захисту прав авторів. З метою забезпечення конституційних прав громадян на захист інтелектуальної власності в системах Міністерства внутрішніх справ України та Служби безпеки України створені та діють спеціальні підрозділи з боротьби з порушеннями у сфері інтелектуальної власності, активізують свою роботу підрозділ державних інспекторів з питань інтелектуальної власності Держдепартаменту інтелектуальної власності та інші державні органи, які в межах своєї компетенції можуть здійснювати заходи, спрямовані на посилення захисту прав інтелектуальної власності.

Якщо міжнародним договором, учасником якого є Україна, встановлено інші правила охорони, ніж ті, котрі містяться в Законі України «Про авторське право і суміжні права», то застосовуються норми міжнародного договору.

У даний час в Україні здійсненні заходи, які пов'язані з утворенням Вищого спеціалізованого суду з питань інтелектуальної власності.

3.4. Персональні дані та захист права на невтручання в особисте життя

3.4.1. Правове забезпечення захисту прав суб'єктів персональних даних у світі

Більшість держав світу давно прийняли закони в галузі захисту прав суб'єктів[61] персональних даних і створили на їхній основі незалежні від уряду державні органи із захисту таких прав на чолі з омбудсменом. Ці органи колегіальні та мають зазвичай назву «Комісія із захисту даних», або *Data Protection Commission*. Уперше такий орган почав працювати в 1919 р. у Швеції.

Сполучені Штати Америки були першою державою, яка зайнялася проблемою захисту персональних даних. Початок було покладено у 1964–1965 рр. роботами комісії Конгресу США «ЕОМ і порушення секретності». У 1966 р. сенатор Дж. Маккарті запропонував Білль про ЕОМ і про права, котрий став основою для урядової пропозиції 1967 р., яка відома як Правила про секретність. Розділ Правил «Дані про особу» надав кожному громадянину право знати зміст файла, який його стосується, і ввів просту процедуру для виправлення можливих помилок. У 1974 р. у США було прийнято Закон «Про охорону особистих таємниць», котрий регламентував доступ до інформаційних матеріалів, що зберігаються в державних органах США.

У 1969 р. парламент Великої Британії прийняв Білль про нагляд за даними, встановлюючи контроль за зібраною інформацією.

У 1970 і 1971 рр. Канада і Австралія прийняли, відповідно, закони «Про секретність» і «Про порушення секретності», які використовували принципи захисту інформації, що застосовувались у США і Великій Британії.

Закон Швеції «Про дані» 1972 р. передбачає введення інспекції, на яку покладалися обов'язки з контролю персональних даних, що зберігаються в автоматизованих системах. Створення будь-якої картотеки персональних даних передбачає отримання дозволу інспекції, яка надає необхідні інструкції щодо усунення ризику порушення прав людини.

---

[61] Першим в історії правовим актом, котрий встановлював обов'язки держави із захисту прав людини, був прийнятий англійським парламентом у 1679 р. Закон «Про свободу людини», основою якого був принцип недоторканності особи.

У 1776 р. колоністи Північної Америки проголосували за Декларацію незалежності, а невдовзі – за Білль про права, який проголосив свободу слова, совісті, зібрань, недоторканність людини. У 1787 р. на основі цих документів була розроблена і прийнята Конституція США. 26 серпня 1789 р. Національними зборами – вищим законодавчим органом Франції – був прийнятий основний документ французької революції – Декларація прав людини і громадянина, у якій уперше були зафіксовані природні права людини: права людині надаються не владою, а належать їй від народження.

У 1978 р. Франція прийняла Закон «Про інформатику, картотеки, свободу».

У Великій Британії з 1984 р. Законом «Про захист даних» здійснюється захист персональних даних, що обробляються засобами ЕОМ.

На базі Закону Землі Гессен 1970 р. був розроблений і прийнятий базовий нормативний акт ФРН «Про подальший розвиток оброблення даних і захисту даних» від 20 грудня 1990 р., який регулює суспільні відносини, що виникають у процесі накопичення, перероблення і використання персоніфікованої інформації (персональних даних).

Міжнародне визнання важливості проблеми захисту персональних даних закріплено основними міжнародними правовими стандартами: Європейською конвенцією про захист осіб стосовно автоматизованого оброблення даних особистого характеру від 28 січня 1981 р. (набула чинності 1 жовтня 1985 р.), директивами Європейського парламенту і Ради: про захист фізичних осіб при обробленні персональних даних і про вільне переміщення таких даних від 24 жовтня 1995 р. № 95/46/ЄС, щодо оброблення персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі від 15 грудня 1997 р. № 97/66/ЄС.

Метою Європейської конвенції про захист осіб стосовно автоматизованого оброблення даних особистого характеру є забезпечення для кожної особи, незалежно від її національності або місця проживання, поважання її прав і основних свобод, і, зокрема, її права на недоторканність особистого життя, стосовно автоматизованого оброблення даних особистого характеру, що її стосуються. Сторони зобов’язуються застосовувати цю Конвенцію до файлів даних особистого характеру для автоматизованого оброблення та до автоматизованого оброблення даних особистого характеру в державному та приватному секторах. Для захисту даних особистого характеру, що зберігаються у файлах даних для автоматизованого оброблення, застосовуються відповідні заходи захисту, спрямовані на запобігання випадковому чи несанкціонованому знищенню

або випадковій втраті, а також на запобігання несанкціонованому доступу, зміненню або розповсюдженню.

Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованим оброблення персональних даних щодо органів нагляду та транскордонних потоків даних від 8 листопада 2001 р. виходячи із важливості обміну інформацією між народами та збільшенням обміну персональними даними через національні кордони гарантує ефективний захист прав людини та фундаментальних свобод, зокрема право на недоторканність особистого життя стосовно таких обмінів персональними даними. З цією метою орган нагляду має, зокрема, повноваження щодо розслідування та втручання, а також право брати участь у судовому розгляді або повідомляти компетентні судові органи про порушення умов внутрішньодержавного права, розглядає та приймає рішення щодо заяв будь-якої особи відносно захисту його/її прав і основних свобод відносно оброблення персональних даних у межах своєї компетенції.

Відходячи від положень ст. 2 «Транскордонні потоки персональних даних до користувачів, які не підпадають під юрисдикцію Сторони Конвенції» цього Протоколу, кожна Сторона може дозволити передання персональних даних, якщо внутрішньодержавне право забезпечує це у зв'язку зі:

– специфічними інтересами суб'єкта даних;

– перевагою законних інтересів, в особливості важливих, суспільних інтересів;

– якщо гарантії, що, зокрема, можуть походити з договірних положень, надаються контролером, відповідальним за передання, та визнаються достатніми компетентними органами відповідно до внутрішньодержавного права.

Відповідно до Директиви Європейського парламенту і Ради про захист фізичних осіб при обробленні персональних даних і про вільне переміщення таких даних від 24 жовтня 1995 р. № 95/46/ЄС захищаються основні права і свободи осіб і особливо їхнє право на невтручання в особисте життя при обробленні персональних даних.

Дана Директива Європейського парламенту і Ради застосовується при обробленні персональних даних за допомогою повного чи часткового використання автоматизованих засобів, а також при обробленні неавтоматичними засобами персональних даних, що є частиною картотеки чи призначені для внесення в картотеку. У ст. 2 цього документа визначається термінологія таких понять:

– *персональні дані* означають будь-яку інформацію, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити (*суб'єкт даних*); особою, яку можна встановити, є така, яка може бути встановленою прямо чи непрямо, зокрема, за допомогою ідентифікаційного коду або одного чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості;

– *оброблення персональних даних* означає будь-яку операцію чи сукупність операцій, здійснюваних з персональними даними (з допомогою чи без допомоги автоматизованих засобів), таких як збирання, реєстрація, організація, зберігання, адаптація чи зміна, пошук, консультація, використання, розкриття за допомогою передання, поширення чи іншого надання, упорядкування чи комбінування, блокування, стирання чи знищення;

– *картотека персональних даних* означає будь-який структурований масив персональних даних, що є доступним за визначеними критеріями, незалежно від того, чи є такий масив централізованим, децентралізованим або розподіленим на функціональних або географічних засадах;

– *контролер* означає фізичну чи юридичну особу, державний орган, агентство або будь-який інший орган, що окремо чи разом з іншими визначає цілі і засоби оброблення персональних даних; якщо цілі і засоби оброблення визначені законодавчими чи нормативними положеннями держави чи ЄС, контролер або особливі критерії його призначення можуть визначатися правом держави чи ЄС;

– *оператор оброблення даних* означає фізичну чи юридичну особу, державний орган, агентство чи будь-який інший орган, що обробляє персональні дані від контролера;

– *одержувач* означає фізичну чи юридичну особу, державний орган, агентство чи будь-який інший орган, якому надаються дані, незалежно від того, це третя особа чи ні; однак органи, що можуть одержувати дані в рамках окремого запиту, не розглядаються як одержувачі;

– *згода суб'єкта даних* означає будь-яке вільно виражене спеціальне і поінформоване зазначення його бажань, за допомогою якого суб'єкт даних дає згоду на оброблення персональних даних, що його стосуються.

Згідно зі ст. 4 цього документа, кожна держава застосовує до оброблення персональних даних національні положення, котрі вона приймає відповідно до даної Директиви, якщо:

– оброблення здійснюється в контексті діяльності установи контролера на території держави-члена; якщо ж один і той самий контролер заснований на території кількох держав-членів, він повинен вжити всіх необхідних заходів для забезпечення того, що кожна з цих установ дотримується зобов'язань, передбачених відповідним національним законодавством;

– контролер заснований не на території держава-члена, а в місці, де його національне законодавство застосовується відповідно до міжнародного публічного права;

– контролер не заснований на території ЄС, але з метою оброблення персональних даних використовує автоматизоване чи будь-яке інше устаткування, розташоване на території згаданої держави-члена, за умови, що таке устаткування не використовується винятково з метою транзиту через територію Євросоюзу.

Загальні правила законності оброблення персональних даних передбачаються ст. 6 цієї Директиви, а саме: персональні дані повинні:

– оброблятися чесно і законно;

– збиратися для встановлення чітких і законних цілей і надалі не оброблятися у спосіб, несумісний з цими цілями. Подальше оброблення даних в історичних, статистичних чи наукових цілях не розглядається як несумісне, якщо держави-члени забезпечують відповідні гарантії;

– бути достовірними, відповідними і не надлишковими відповідно цілей, заради яких вони збираються і/або надалі обробляються;

– бути точними і, якщо необхідно, обновлятися; слід вживати всіх розумних заходів, щоб гарантувати, що дані, які є неточними чи неповними, з урахуванням цілей, заради яких вони були зібрані чи заради яких вони надалі обробляються, стиралися чи виправлялися;

– зберігатися у формі, що дозволяє встановлювати особу суб'єктів даних не довше, ніж це необхідно для цілей, заради яких дані були зібрані чи заради яких вони надалі обробляються. Держави-члени встановлюють відповідні гарантії для персональних даних, що зберігаються протягом більш тривалих періодів з метою історичного, статистичного чи наукового використання.

Критерії законності оброблення даних (ст. 7) державами-членами полягають у тому, що персональні дані можуть оброблятися тільки за умови, якщо:

– суб'єкт даних недвозначно дав свою згоду;

– оброблення необхідне для виконання контракту, стороною якого є суб'єкт даних, чи для здійснення заходів на прохання суб'єкта даних до підписання контракту;

– оброблення даних необхідне для дотримання правового зобов'язання, яким зв'язаний контролер;

– оброблення даних необхідне для захисту життєво важливих інтересів суб'єкта даних;

– оброблення даних необхідне для виконання завдання, здійснюваного в суспільних інтересах, чи при виконанні офіційних повноважень, якими наділений контролер або третя сторона, якій надаються дані;

– оброблення необхідне в цілях законних інтересів, переслідуваних контролером, третьою стороною або сторонами, для яких надаються дані, крім випадків, коли над такими інтересами переважають інтереси основних прав і свобод суб'єкта даних.

У Директиві наголошується, що держави-члени забороняють оброблення персональних даних, що вказують на расове чи етнічне походження, політичні

погляди, релігійні чи філософські переконання, профспілкове членство, і оброблення даних, що стосуються здоров'я чи статевого життя людини.

Директива вказує, що у випадку, якщо дані не були отримані від суб'єкта даних, держави-члени передбачають, що контролер чи його представник під час реєстрації персональних даних чи, якщо передбачене розголошення даних третій особі, не пізніше того часу, коли дані вперше розголошуються, надати суб'єкту даних наступну інформацію, крім тих випадків, коли в нього вже є ця інформація:

– цілі оброблення;

– будь-яка інформація, як наприклад: категорії використання даних, одержувачі чи категорії одержувачів, існування права доступу і права на виправлення даних, які його стосуються тією мірою, якою така додаткова інформація необхідна з огляду на особливі обставини, за яких дані обробляються, для гарантії справедливого оброблення по відношенню до суб'єкта оброблення даних.

Держави-члени надають відповідні гарантії при обробленні даних у статистичних цілях чи з метою історичних чи наукових досліджень, коли надання такої інформації виявляється неможливим чи може спричинити непропорційні зусилля або коли реєстрація чи надання даних чітко передбачене законодавством.

У Директиві зазначається:

– держави-члени гарантують кожному суб'єкту право отримати від контролера підтвердження того, обробляються чи ні дані, які його стосуються, і інформацію про цілі оброблення, категорії розглянутих даних і про одержувачів чи категорії одержувачів, яким надаються дані;

– повідомлення суб'єкту в зрозумілій формі про те, що дані знаходяться в процесі оброблення, і будь-яку іншу доступну інформацію щодо їхнього джерела;

– інформацію про логіку, використовувану під час автоматизованого оброблення даних, що стосуються суб'єкта, принаймні у випадку автоматизованих рішень;

– залежно від ситуації – виправлення, стирання чи блокування даних, оброблення яких не відповідає положенням даної Директиви, зокрема через неповноту чи неточність даних;

– повідомлення третім сторонам, яким були надані дані, про будь-яке виправлення, стирання чи блокування, виконане відповідно до попереднього пункту, якщо це можливо чи не вимагає непропорційних зусиль.

Безпека оброблення гарантується ст. 17 Директиви свідчить, що: «Держави-члени передбачають, що контролер повинен здійснювати відповідні технічні й організаційні заходи для захисту персональних даних від випадкового або незаконного знищення чи випадкової втрати, зміни, несанкціонованого розкриття чи доступу, зокрема якщо оброблення включає передання даних через мережу, і від усіх інших незаконних форм оброблення».

Директива Європейського Союзу стосовно оброблення персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі від 15 грудня 1997 р. № 97/66/ЄС передбачає необхідність забезпечення однакового рівня захисту основних прав і свобод, зокрема в тому, що стосується права на невтручання в особисте життя, при обробленні персональних даних у телекомунікаційному секторі та для забезпечення вільного переміщення таких даних, а також телекомунікаційного обладнання і послуг Співтовариства. Ця Директива не застосовується до діяльності, що виходить за межі права Співтовариства і в жодному разі до діяльності, що стосується громадського порядку, оборони, державної безпеки (включаючи економічний добробут держави, коли діяльність стосується питань безпеки держави), а також діяльності держави у сфері кримінального права.

У Директиві приділяється значна увага використанню відповідних технічних та організаційних заходів для гарантування безпеки своїх послуг, якщо потрібно – з оператором телекомунікаційної мережі загального користування[62], у тому, що стосується безпеки мережі із врахуванням сучасного стану науки і тех-

[62] Телекомунікаційна мережа загального користування означає системи передавання і, у відповідних випадках, комутаційне обладнання та інші ресурси, що дозволяють передавати сигнали між визначеними кінцевими пунктами за допомогою телеграфу, радіо, оптичних чи інших електромагнітних засобів, що використовуються, повністю чи частково, для надання загальнодоступних телекомунікаційних послуг.

ніки, а також вартості їхньої реалізації, що відповідає представленому ризику. Держави-члени забезпечують у національних положеннях конфіденційність зв'язку за допомогою телекомунікаційної мережі загального користування та загальнодоступних телекомунікаційних послуг, забороняючи прослуховування, перехоплення, зберігання та інші види перехоплювання і нагляду за зв'язком, окрім того, що здійснюється користувачами, без згоди відповідних користувачів, за винятком випадків, коли на це існує законний дозвіл. Ця норма не торкається законно санкціонованого записування зв'язку в ході законної економічної діяльності з метою надання доказів комерційної трансакції чи будь-якого іншого економічного зв'язку.

Також передбачається, що держави-члени можуть приймати законодавчі положення для обмеження сфери дії обов'язків та прав цієї Директиви, коли таке обмеження є необхідним заходом для гарантування національної безпеки, громадського порядку, запобігання, розслідування, розкриття і переслідування кримінальних злочинів чи несанкціонованого використання телекомунікаційної системи.

Ідейна сутність європейських стандартів, їх направленість і принципи захисту передбачають можливість введення в національне законодавство додаткових заходів захисту персональних даних фізичних осіб.

Згідно з європейським законодавством персональні дані поділяються на «ідентифікуючі» і на «вразливі» дані про особу. До «вразливих» даних відноситься інформація щодо здоров'я, расової та іншої приналежності людини, політичних переконань. Саме ця інформація підлягає контролю над її використанням та поширенням з боку фізичної особи щодо якої вона зібрана. Ідентифікуюча інформація має більш вільний порядок звернення, контролюючи мету її збору і право доступу до неї. Таким чином, «вразливі дані» є основною прерогативою захисту, що дає можливість суб'єктам професійної діяльності, пов'язаної з накопиченням персональних даних, більш вільно, не ускладнюючи технологічний процес обробки, користуватися персональними даними.

Згідно із законодавством більшості європейських держав персональні дані розділяються за критерієм «чутливості» на дані загального характеру (прізвище, ім'я по батькові, дата і місце народження, громадянство, місце проживання) і «чутливі» (вразливі) персональні дані (дані про стан здоров'я – історія хвороби, діагнози; етнічна приналежність, ставлення до релігії, ідентифікаційні коди чи номери, відбитки пальців, записи голосу, фотографії, кредитна історія, дані про судимість і т.д.). Для чутливих персональних даних передбачена більш висока ступінь захисту. Так, забороняється збирання, зберігання, використання та передача без згоди суб'єкта даних саме чутливих, а не всіх персональних даних.

Відповідно до Постанови Кабінету Міністрів України № 373 від 29 березня 2006 р. «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»[63], ідентифікація – процедура розпізнавання користувача в системі, як правило, за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою. Першим кроком реалізації вимог Закону України «Про персональні дані» є Указ Президента України «Про оптимізацію системи центральних органів виконавчої влади»[64], яким передбачено створення Державної служби України з питань захисту персональних даних.

3.4.2. ПРАВОВИЙ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

Участь України в міжнародному обміні інформацією, у міжнародних проектах, які засновані на використанні нових інформаційно-комунікаційних технологій, зокрема, Інтернет, в різних секторах економічної, соціальної та науково-технічної діяльності, вимагає захисту персональних даних при їх автоматизованій обробці, за умов гармонізації правових норм, що діють в Україні, з європейськими стандартами.

[63] Постанова Кабінету Міністрів України № 373 від 29.03.2006 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=373-2006-%EF

[64] Указ Президента України № 1085/2010 від 09.12.2010 «Про оптимізацію системи центральних органів виконавчої влади». [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1085%2F2010

Для України актуальність й об'єктивна необхідність захисту прав людини і громадянина в інформаційній сфері визначається великою активністю у формуванні баз даних (соціального, фінансового, маркетингового, медичного, екологічного, адміністративного, правоохоронного та іншого характеру), розвитком і поширенням автоматизованих засобів і способів збирання, оброблення, зберігання і передання інформації.

Персональні дані – це інформація, котра з огляду на її унікальність, характерні особливості і делікатність у поводженні з нею дозволяє ввести нову юридичну категорію і створити новий правовий механізм присвоєння і регулювання взаємовідносин саме для сфери захисту персональних даних. Підґрунтям для такого механізму є категорія «виключне право власності на персональні дані». Виключне право – це можливість законодавчого обмеження прав особи на персональні дані з позиції інтересів інших фізичних осіб, суспільства і держави, а право власності надає особі монопольні права володіння, користування і розпорядження своїми персональними даними, що юридично підтверджується положеннями ст. 32 Конституції України, Законом України «Про захист персональних даних» від 1 червня 2010 р. № 2297-VI, а також міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Отже, *персональні дані* – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Слід зазначити, що: джерелом права власності на персональні дані є природно-конституційне право людини на унікальні, власні і делікатні відомості, які не тільки однозначно ототожнюють людину, характеризують її особистість, але й вміщують у собі предмет споживчої та мінової вартості, тобто можна стверджувати, що захист персональних даних повинен ґрунтуватися на спеціальному методі спільного регулювання відносин на основі принципів права власності на матеріальні об'єкти і принципів виключного права на нематеріальні об'єкти.

Будь-які відомості стосовно фізичних осіб є винятковим видом приватної власності, що юридично виступає у формі виключного права власності, моно-

полія на яке обмежується в інтересах дотримання балансу інтересів особистості, суспільства і держави.

Стаття 23 Закону України «Про інформацію» визначає, що інформація про особу являє сукупність документованих або публічно оголошених відомостей про особу. Джерелами документованої інформації про особу є видані на її ім'я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень.

Основними даними про особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров'я (факт звернення за медичною допомогою, діагноз, результат медичного обстеження), адреса, дата і місце народження, майнове становище тощо.

Первинними джерелами відомостей про фізичну особу є: видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе. Обсяг персональних даних, які можуть бути включені до бази персональних даних, визначається умовами згоди суб'єкта персональних даних або відповідно до закону (ст. 6 Закону України «Про захист персональних даних»).

Стаття 23 Закону України «Про інформацію» встановлює такі *правові гарантії конфіденційності інформації про особу*:

– забороняється збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених законом;

– кожна особа має право на ознайомлення з інформацією, зібраною про неї;

– інформація про особу охороняється законом.

Стаття 4 Закону України «Про захист персональних даних» визначає, що *суб'єктами відносин, пов'язаних із персональними даними*, є:

– суб'єкт персональних даних;

– володілець бази персональних даних;

– розпорядник бази персональних даних;

– третя особа;

– уповноважений державний орган з питань захисту персональних даних;

– інші органи державної влади та органи місцевого самоврядування, до повноважень яких належить здійснення захисту персональних даних.

Оброблення персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому чинним законодавством. Не допускається оброблення даних про фізичну особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки.

Забороняється оброблення персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, а також даних, що стосуються здоров'я чи статевого життя.

Згідно ст.6 Закону України «Про захист персональних даних» використання персональних даних в історичних, статистичних чи наукових цілях може здійснюватися лише в знеособленому вигляді.

Поширення персональних даних передбачає дії щодо передання відомостей про фізичну особу з баз персональних даних за згодою суб'єкта персональних даних або у випадках, передбачених законом (ст. 14 Закону України «Про захист персональних даних»).

Відповідно до положень ст. 8 цього Закону, особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними.

Суб'єкт персональних даних має право:

– знати про місцезнаходження бази персональних даних, яка містить його персональні дані;

– отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;

– на доступ до своїх персональних даних;

– отримувати не пізніш як за 30 календарних днів з дня надходження запиту відповідь про те, чи зберігаються його персональні дані у відповідній базі пер-

сональних даних, а також отримувати зміст його персональних даних, які зберігаються;

– пред'являти вмотивовану вимогу із запереченням проти обробленання своїх персональних даних;

– пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних, якщо ці дані опрацьовуються незаконно чи є недостовірними;

– на захист своїх персональних даних від незаконного обробленання та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням;

– звертатися з питань захисту своїх прав щодо персональних даних до органів державної влади;

– застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних.

Використання персональних даних працівниками суб'єктів відносин, пов'язаних із персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків, що виключає розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків.

Відомості про особисте життя фізичної особи не можуть використовуватися як чинник, що підтверджує чи спростовує її ділові якості (ст. 10).

Порядок доступу до персональних даних (ст. 16) третіх осіб визначається умовами згоди суб'єкта персональних даних, наданої володільцю бази персональних даних, на оброблення цих даних, або відповідно до вимог закону. Доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог Закону України «Про захист персональних даних» або неспроможна їх забезпечити.

Правові гарантії захисту особистої інформації встановлені і Цивільним кодексом України, у якому зазначається:

– негативна інформація, поширена про особу, уважається недостовірною, якщо особа, яка її поширила, не доведе протилежного;

– якщо особисте немайнове право фізичної особи порушене в газеті, книзі, кінофільмі, теле-, радіопередачі тощо, які готуються до випуску у світ, суд може заборонити розповсюдження відповідної інформації; якщо особисте немайнове право фізичної особи порушене в номері (випуску) газети, книзі, кінофільмі, теле-, радіопередачі тощо, які випущені у світ, суд може заборонити (припинити) їх розповсюдження до усунення цього порушення, а якщо усунення порушення неможливе, вилучити тираж газети, книги тощо з метою його знищення;

– ім'я фізичної особи, яка затримана, підозрюється чи обвинувачується у вчиненні злочину, або особи, яка скоїла адміністративне правопорушення, може бути використане (обнародуване) лише в разі набрання законної сили обвинувальним вироком суду щодо неї або винесення постанови у справі про адміністративне правопорушення та в інших випадках, передбачених законом;

– збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини; фізична особа, яка поширює інформацію, зобов'язана переконатися в її достовірності; фізична особа, яка поширює інформацію, отриману з офіційних джерел (інформація органів державної влади, органів місцевого самоврядування, звіти, стенограми тощо), не зобов'язана перевіряти її достовірність та не несе відповідальності в разі її спростування; фізична особа, яка поширює інформацію, отриману з офіційних джерел, зобов'язана робити посилання на таке джерело.

Україна спізнюється майже на чверть століття як з підписанням міжнародних угод, так й з впровадженням відповідних норм міжнародного прав. Лише у 2005 р. підписано Конвенцію 1981 р. Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних», яку до цього часу не подано на ратифікацію. Європейське право охоплює майже два десятки загальноєвропейських конвенцій, директив та рекомендацій з питань захисту пер-

сональних даних, кожна країна ЄС видала свої базові нормативно-законодавчі акти, приймалися конкретні закони: щодо діяльності з персональними даними у медичній, статистичній, державній, журналістській, поліцейській та інших сферах.

Нагальність приведення норм права вітчизняного законодавства у відповідність до вимог міжнародних стандартів убачається і в аспекті пріоритетності співробітництва України з Євросоюзом і його окремими державами-учасницями у зв'язку з активізацією процесів трансграничного телекомунікаційно-інформаційного обміну.

ЧАСТИНА ІІІ. ІНОВАТИКА: ЗАСОБИ, МЕТОДИ І ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

РОЗДІЛ 1. ПРАВОВІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ТЕХНІЧНИХ ЗАСОБІВ

1.1. Правовий захист комп'ютерних програм

1.1. 1. Міжнародно-правові засади охорони комп'ютерних програм

Технологічні можливості, що виникли в результаті об'єднання комп'ютерних і телекомунікаційних технологій, багато в чому змінили сучасний світ: вплив мереж помітний у змінах економіки й соціальної динаміки[65]. Поряд із доступністю глобальних мереж увага переноситься з їхніх технічних характеристик на соціальні наслідки використання. Суспільство рухається до того моменту, коли можна буде стверджувати, що все у світі залежить від програмного забезпечення.

Стрімке зростання вартості об'єктів інтелектуальної власності робить здобутки інтелектуальної діяльності людини, суспільства і держави його значним капіталом. Особливе місце серед об'єктів інтелектуальної власності посідає комп'ютерне програмне забезпечення, яке сьогодні є не тільки підґрунтям науково-технічного розвитку, а й товаром.

Як будь-який інший продукт інтелектуальної діяльності людини, комп'ютерні програми потребують правового захисту від незаконного привласнення без дозволу осіб, які мають на них охоронні документи.

Сьогодні виділяють три *типи правової охорони комп'ютерних програм*:

– за допомогою патентів;

– за допомогою авторського права;

– за допомогою положень, спрямованих проти порушень промислових секретів.

Поява наприкінці 70-х рр. XX ст. персональних комп'ютерів, набуття комп'ютерними програмами ознак уніфікованості викликали перегляд чинних

[65] Світові витрати на інформацію та комунікації в 1998 р. досягли 45–50 млрд дол. США. На початок 2002 р. ринок значно розширився і в нього було вкладено до 200 млрд дол. США.

на той час правових підходів щодо законодавчого захисту програм і віднесення їх до об'єктів авторського права.

Думку про те, що комп'ютерні програми можуть сприйматися лише як винахід, але не як об'єкт авторського права, ще в 1957 р. висловив К. Шарм. У США до початку 80-х рр. XX ст. інтереси виробників комп'ютерних програм захищалися законодавством про комерційну таємницю та положеннями договірного права.

З початку 90-х рр. минулого століття комп'ютерні програми, незалежно від засобу й форми вираження, законодавчо охороняються як літературні твори, згідно зі ст. 2 Бернської конвенції про охорону літературних і художніх творів (Паризький акт від 24 липня 1971 р., змінений 2 жовтня 1979 р.) та відповідно до Угоди про торговельні аспекти прав інтелектуальної власності (Угода ТРІПС) від 15 квітня 1994 р.

Частина 1 ст. 2 Бернської конвенції про охорону літературних і художніх творів встановлює: термін «літературні і художні твори» охоплює всі твори в галузі літератури, науки і мистецтва, яким би способом і в якій би формі вони не були виражені.

У Директиві Європейського Економічного Співтовариства про правову охорону комп'ютерних програм від 14 травня 1991 р. № 91/250/ЄЕС зазначено, що в цілях цієї Директиви термін «комп'ютерна програма» буде включати: програми в будь-якій формі, у тому числі й ті, котрі вбудовані в металеві деталі; враховуючи, що цей термін також включає підготовчі оформлювальні роботи, які ведуть до розвитку комп'ютерної програми, передбачаючи, що сутність підготовчих робіт є такою, що комп'ютерна програма має від них результат на останньому етапі; приймаючи до уваги, що у відношенні критерію, який повинен застосовуватися для визначення того, чи являється комп'ютерна програма оригінальним твором, ніякі тести, що стосуються якості чи естетики програми, не повинні використовуватися.

Правова охорона відповідно до цієї Директиви буде застосовуватися до комп'ютерної програми, яка виражена в будь-якій формі; комп'ютерна програ-

ма буде такою, яка охороняється, якщо вона є оригіналом у тому значенні, що це є інтелектуальне творіння автора.

Автором комп'ютерної програми повинна бути фізична особа чи група фізичних осіб, які створили програму, або, якщо законодавство держав-членів дозволяє це, – юридична особа, котра розглядається в якості носія прав з цього законодавства.

Якщо колективні твори визнаються законодавством держав-членів, окрема людина, яка розглядається законодавством держав-членів як творець, уважається його автором. По відношенню до комп'ютерної програми, яка створена групою фізичних осіб, виключні права будуть належати спільно.

Якщо комп'ютерна програма створена робітником при виконанні його обов'язків або у відповідності з інструкціями, отриманими від його роботодавця, тільки роботодавець має повноваження здійснювати всі економічні права по відношенню до такої програми, якщо інше не передбачено в контракті.

Договір Всесвітньої організації інтелектуальної власності від 20 грудня 1996 р. встановлює:

– статтею 4, що комп'ютерні програми охороняються як літературні твори в розумінні ст. 2 Бернської конвенції. Така охорона застосовується до комп'ютерних програм, незалежно від способу або форми їх вираження[66];

– статтею 5, що компіляції даних (бази даних) або іншої інформації в будь-якій формі, які за підбором і розміщенням змісту є результатом інтелектуальної творчості, охороняються як такі. Така охорона не поширюється на самі дані або інформацію і не обмежує будь-яке авторське право, яке відноситься до самих даних або інформації, що містяться в компіляції[67].

Згідно з нормами Бернської конвенції правова охорона комп'ютерних програм виникає внаслідок їх створення, незалежно від реєстрації або виконання інших формальностей, що дає можливість автору контролювати копіювання, розпродаж своїх програм і тим самим гарантувати собі фінансові надходження.

66 Узгоджені заяви щодо ст. 4: сфера захисту комп'ютерних програм, відповідно до ст. 4 цього Договору, включаючи ст. 2, співпадає зі ст. 2 Бернської конвенції і відповідними положеннями Угоди ТРІПС.

67 Узгоджені заяви щодо ст. 5: сфера захисту компіляції даних (баз даних), відповідно до ст. 5 цього Договору, включаючи ст. 2, співпадає зі ст. 2 Бернської конвенції і відповідними положеннями Угоди ТРІПС.

Термін правової охорони комп'ютерних програм у більшості країн світу збігався з термінами правової охорони інших об'єктів авторського права, а за умови приєднання до Угоди ТРІПС регламентується ст. 12 цієї Угоди: при обчисленні строку охорони твору, за винятком фотографічних творів або творів прикладного мистецтва, на іншій підставі, ніж людське життя, такий строк складає не менше ніж 50 років від кінця календарного року, у якому зі згоди автора була здійснена публікація, або, за відсутності такої публікації протягом 50 років з моменту створення твору, 50 років від кінця календарного року створення твору.

Виникнення правових колізій при захисті комп'ютерних програм свідчить, що існуючий захист комп'ютерних програм авторським правом є недостатнім. Сучасні комп'ютерні програми мають ознаки об'єкта інтелектуальної власності – винаходу (наявність дій або сукупності дій, порядок виконання дій у часі, умови виконання дій, режим) і тому захищаються патентним правом[68].

За визначенням Європейського патентного відомства, «комп'ютерна програма як така є своєрідним інструментом для здійснення способу, набором інструкцій та команд для комп'ютера, викладених зрозумілою мовою, і лише перекладена людською мовою та позбавлена несуттєвих елементів з огляду на потрібний ступінь узагальнення ознак вона може бути трансформованою в опис способу як об'єкт винаходу».

Сьогодні в США патент видається не тільки на винахід, що вміщує комп'ютерну програму і відповідає вимогам патентоздатності (новизна, винахідницький рівень, промислова придатність), а й на комп'ютерну програму, згідно з § 101 Патентного закону США, якщо вона записана в реальному середовищі. Такі комп'ютерні програми є патентоздатними і до них проводиться відповідна експертиза, згідно з § 101 і § 103 того ж Закону.

Спеціальні правила з експертизи винаходів, пов'язаних з комп'ютерними програмами, встановлено патентними відомствами Австралії, Канади, Японії.

[68] В основу патентної системи покладено поняття «патент» (лат. *littoral patenis*), що означає відкриту грамоту, відрізняється від звичайної тим, що її зміст можна продемонструвати не зламуючи печатки. Патент як документ посвідчує монопольне (виключне) право на виробництво і продаж певного виду товару та послуг.

У Європі для надання патентної охорони комп'ютерним технологіям використовується прогалина у ст. 52 Європейської патентної конвенції, яка виключає з патентної охорони програми для оброблення даних на ЕОМ як такі, тобто патент видається на винахід, здійснений за допомогою комп'ютерної програми (комп'ютерної технології). На сьогодні Європейським патентним відомством видано понад 130 тис. патентів на винаходи, що були здійснені за допомогою комп'ютерних програм. Наприклад, у Франції запропоновано систему охорони комп'ютерних програм, що поєднує норми авторського і патентного права.

1.1.2. Законодавче забезпечення захисту комп'ютерних програм в Україні

Зараз в Україні, як і в багатьох країнах світу, законодавство зараховує комп'ютерні програми до об'єктів, що охороняються авторським правом.

Затверджений Постановою Кабінету Міністрів України Порядок локалізації програмних продуктів (програмних засобів) для виконання Національної програми інформатизації[69] визначає *програмний засіб* як взаємопов'язану сукупність програм, процедур, правил, документації та даних, що стосуються функціонування обчислювальної системи.

У ст. 1 Закону України «Про авторське право і суміжні права» визначається, що «*комп'ютерна програма* – набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи в будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його в дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктивному кодах)».

[69] Про затвердження Порядку локалізації програмних продуктів (програмних засобів) для виконання Національної програми інформатизації [Електронний ресурс] : постанова Кабінету Міністрів України від 16 листоп. 1998 р. № 1815. – Режим доступу: http:/zakon.rada.gov.ua/cgi-bin/main.cgi?nreg=1815-98-%EF.

Для порівняння наведемо аналогічну дефініцію із Кримінального закону штату Нью-Йорк (США): «Комп'ютерна програма розглядається як власність і визначає упорядкований набір даних, що подає кодовані команди або приписи, котрі при виконанні комп'ютером є причиною, з якої комп'ютер обробляє дані чи керується з метою виконання однієї чи більшої кількості операцій, та може існувати в будь-якій формі, включаючи магнітні носії даних, перфоровані стрічки, плати, або можуть бути збережені в пам'яті комп'ютера».

Авторське право на комп'ютерну програму виникає внаслідок самого факту її створення і не потребує реєстрації, спеціального оформлення чи дотримання будь-яких інших формальностей (ст. 437 ЦК України). Первинним суб'єктом, якому належить авторське право, є автор комп'ютерної програми, тобто фізична особа, яка своєю творчою працею створила програму і якій належать особисті немайнові та майнові права на цю програму. Крім того, суб'єктами авторського права можуть бути інші фізичні та юридичні особи, які набули права на комп'ютерну програму відповідно до договору або Закону.

Особисті немайнові права авторів (право на ім'я, на заборону його використання, на псевдонім та на недоторканність твору) тісно пов'язані з особистістю, а тому є невідчужуваними.

Майновими правами інтелектуальної власності на комп'ютерну програму є право на використання твору (що згідно зі ст. 441 ЦК України включає права на опублікування (випуск у світ); відтворення будь-яким способом та у будь-якій формі; переклад; переробку, адаптацію та інші подібні зміни; включення складовою частиною до збірників, баз даних тощо; продаж, передання в найм (оренду); імпорт його примірників, примірників його перекладів, переробок тощо); виключне право дозволяти використання твору іншими особами та право пере шкоджати неправомірному використанню твору, у тому числі забороняти таке використання. Зазначені права можуть бути передані повністю або частково ін-

шій особі на умовах, визначених договором щодо розпоряджання майновими правами[70] інтелектуальної власності.

Розпорядженням Кабінету Міністрів України від 15 травня 2002 р. № 247-р було затверджено Концепцію легалізації програмного забезпечення та боротьби з нелегальним його використанням, яка визначила основні наукові та практичні заходи, спрямовані на вдосконалення нормативно-правової бази з питань легалізації програмного забезпечення та боротьби з нелегальним його використанням, розроблення рекомендацій щодо підвищення ефективності застосування законодавства в зазначеній сфері, створення механізму протидії нелегальному використанню програмного забезпечення.

Для досягнення зазначеної мети необхідно вирішити ряд завдань, зокрема:

– розробити та прийняти нормативно-правові акти, спрямовані на вдосконалення та розвиток законодавства щодо охорони прав інтелектуальної власності у сфері програмного забезпечення;

– розробити рекомендації щодо вдосконалення організації боротьби з незаконним відтворенням, розповсюдженням і використанням програмного забезпечення;

– здійснити заходи щодо розбудови вітчизняної індустрії програмного забезпечення.

З метою запобігання поширенню використання неліцензійного програмного забезпечення та оптимізації використання комп'ютерних програм було прийнято Постанову Кабінету Міністрів України «Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади» від 10 вересня 2003 р. № 1433. Зазначена Постанова визначає процедуру використання в органах виконавчої влади комп'ютерних програм як об'єктів авторського права. У Поста-

[70] Розпоряджання майновими правами інтелектуальної власності на комп'ютерну програму, відповідно до ст. 1107 ЦК України, здійснюється на підставі: ліцензії на використання об'єкта права інтелектуальної власності; ліцензійного договору; договору про створення за замовленням і використання об'єкта права інтелектуальної власності; договору про передання виключних майнових прав інтелектуальної власності; іншого договору щодо розпоряджання майновими правами інтелектуальної власності. Договір щодо розпоряджання майновими правами інтелектуальної власності має бути укладеним у письмовій формі. У разі недодержання письмової форми договору щодо розпоряджання майновими правами інтелектуальної власності такий договір є недійсним.

нові встановлюється порядок створення підрозділу, відповідального за дотримання вимог законодавства з питань правової охорони комп'ютерних програм під час їх придбання, встановлення, застосування, обліку та інвентаризації.

Постанова передбачає:

– щорічні інвентаризації програмного забезпечення;

– можливість здійснення раптових перевірок використання комп'ютерних програм в органах виконавчої влади;

– обов'язки користувачів комп'ютерів та інші механізми, які дозволять здійснювати поточний контроль за дотриманням авторських прав у державних органах.

Постановою Кабінету Міністрів України від 4 квітня 2000 р. у складі Міністерства освіти та науки України утворено Державний департамент інтелектуальної власності.

Основними завданнями Департаменту є:

– участь у межах своєї компетенції у забезпеченні реалізації державної політики у сфері інтелектуальної власності;

– прогнозування і визначення перспектив і пріоритетних напрямів розвитку у сфері інтелектуальної власності;

– організаційне забезпечення охорони прав на об'єкти інтелектуальної власності.

У системі Державного департаменту інтелектуальної власності створено Реєстр виробників та розповсюджувачів програмного забезпечення та інформаційно-довідкову систему з питань розповсюдження і використання програмного забезпечення. Ведення Реєстру надає можливість органам державної влади, бюджетним установам і організаціям мати достовірні дані про діяльність суб'єктів підприємницької діяльності, які пропонують їм для придбання програмні продукти, та встановити правомірність таких пропозицій. У разі виникнення питань з приводу використання комп'ютерних програм при їх придбанні та введенні в обіг можна звернутись за роз'ясненнями до інформаційно-довідкової системи, яка працює наразі в інтерактивному режимі на сайті Держдепартаменту.

Розвиток власної індустрії програмного забезпечення має стати однією з важливих передумов цивілізованого функціонування ринку інформаційних технологій у країні. Виробництво програмного забезпечення повинно базуватися на сучасних технологіях, експортній орієнтації, привабливості для іноземних інвестицій, взаємодії з навчальними закладами, охороні прав інтелектуальної власності тощо.

Стратегія розвитку індустрії програмного забезпечення повинна будуватися з урахуванням відмінностей, що відрізняють її від продукції інших сфер виробництва, зокрема:

– кінцевий продукт є інформаційно-аналітичним інструментарієм для ефективнішого управління процесами матеріального виробництва, самою інформацією і знаннями;

– вартість затрачених інтелектуальних ресурсів значно перевищує вартість використаних матеріальних ресурсів;

– програмне забезпечення постійно перебуває під загрозою несанкціонованого копіювання, що ускладнює отримання правовласником належної винагороди тощо.

До основних заходів з розвитку індустрії програмного забезпечення належать:

– створення дієвих механізмів захисту від несанкціонованого копіювання;

– підтримка наукових та освітніх процесів, спрямованих на розвиток інтелектуальних ресурсів;

– законодавче та організаційне сприяння залученню інвестиційних ресурсів;

– збільшення квот підготовки спеціалістів зі спеціальностей, пов’язаних зі створенням програмного забезпечення, та підготовка нових навчальних програм, що відображають сучасні міжнародні вимоги до спеціалістів-програмістів;

– сприяння залученню виробників програмного забезпечення до процесу інвестування частки прибутків у відповідні навчальні заклади;

– пропагування привабливості інвестицій міжнародного капіталу в індустрію програмного забезпечення;

– вирішення на міждержавному рівні питань щодо порядку виїзду спеціалістів-програмістів за кордон та впровадження компенсаційних механізмів для відтворення інтелектуального потенціалу;

– звільнення від експортного мита виробленої продукції та наданих послуг.

Для створення ефективного правового та економічного механізму функціонування ринку програмного забезпечення передбачається:

– приведення законодавства щодо об'єктів авторського права і суміжних прав, до яких належить і програмне забезпечення, у відповідність з міжнародними нормами;

– створення сприятливих умов для залучення іноземних інвестицій у сферу виробництва програмного забезпечення;

– заборона незаконного встановлення нового програмного забезпечення;

– першочергове розроблення стандартів у сфері інформаційних технологій;

– включення вимог щодо ліцензійної чистоти програмного забезпечення до комплекту нормативно-правових документів сертифікації прикладного програмного забезпечення навчального призначення;

– забезпечення кадрами створених у системі МВС України спеціальних підрозділів із питань боротьби з правопорушеннями у сфері інтелектуальної власності;

– налагодження співробітництва з міжнародними організаціями, які захищають інтереси правовласників на програмне забезпечення;

– створення національного електронного реєстру виробників та розповсюджувачів програмного забезпечення і навчальних програм.

Види незаконного використання програмного забезпечення, котрі можуть бути кваліфіковані як порушення авторського права:

– продаж комп'ютерної техніки разом із незаконно встановленим програмним забезпеченням;

– тиражування і розповсюдження примірників програмного забезпечення на носіях інформації без дозволу власника авторських прав;

– незаконне розповсюдження програмного забезпечення через телекомунікаційні мережі (інтернет, електронна пошта тощо);

– незаконне використання програмного забезпечення користувачем.

Одним із основних видів правопорушень щодо програмного забезпечення є контрафакція, різновидом якої є відтворення, розповсюдження та використання програмного забезпечення без дозволу власника авторських прав на ці твори (комп'ютерне піратство).

За формами порушення авторських прав, що зустрічаються в процесі придбання та використання комп'ютерних програм, можна виділити наступні:

– придбання контрафактних примірників комп'ютерних програм, виготовлених, наприклад, шляхом запису програм на магнітні або оптичні диски та їх розповсюдження за цінами, що значно нижчі за оригінальні примірники;

– придбання комп'ютерної техніки з попередньо встановленим на жорсткі диски таких комп'ютерів неліцензійним програмним забезпеченням;

– створення в організації контрафактних примірників програм як шляхом запису на магнітні диски, так і шляхом встановлення на жорсткі диски персональних комп'ютерів в об'ємі, що перевищує кількість примірників комп'ютерних програм, дозволену правовласником за умовами договору щодо розпорядження майновими правами інтелектуальної власності.

Використання комп'ютерної програми без відповідного дозволу (ліцензії) автора, невиконання умов договору є порушенням авторських прав і може бути підставою для притягнення особи-порушника до наступних видів відповідальності згідно з чинним законодавством України:

– цивільно-правової (майнової) – ст. 431 ЦК України та ст. 52 Закону України «Про авторське право і суміжні права»;

– адміністративної – ст. 51-2 КУпАП;

– кримінальної – ст. 176 КК України.

Так, ст. 431 ЦК України встановлює, що порушення права інтелектуальної власності, у тому числі невизнання цього права чи посягання на нього, тягне за собою відповідальність, встановлену цим Кодексом, іншим законом чи договором. З цього визначення випливає, що порушення права інтелектуальної власності можливе як у формі дій (посягання на право інтелектуальної власності), так і у формі бездіяльності (невизнання права інтелектуальної власності). При цьому порушником права інтелектуальної власності може бути фізична або юридична особа.

1.1.3. Судовий розгляд матеріалів щодо неправомірного використання комп'ютерних програм

Сьогодні у судовій практиці розгляду даної категорії справ існують такі проблеми, як неправильна кваліфікація дій правопорушників та неоперативність розгляду справ.

Так, судді не розмежовують незаконне використання та незаконне розповсюдження об'єктів інтелектуальної власності. Наприклад, за незаконне використання, комп'ютерної програми помилково притягають до адміністративної відповідальності за ст. 164-9 КУпАП та, навпаки, за наявності факту незаконного розповсюдження (шляхом продажу) примірників комп'ютерних програм, баз даних притягують до адміністративної відповідальності за ст. 51-2 КУпАП.

Під час розгляду справ щодо неправомірного використання комп'ютерних програм не всі судді враховують, що важливою є оперативність, оскільки відповідно до п. 7 ст. 247 КУпАП, закінчення на момент розгляду справи про адміністративне правопорушення строків, передбачених ст. 38 КУпАП (два місяці), є обставиною, що виключає провадження в такій справі, і, як наслідок, справа має бути закрита, а вилучена контрафактна продукція повернена власнику.

Під час розгляду справ про правопорушення у сфері інтелектуальної власності судді, вирішуючи питання про притягнення правопорушника до адміністративної відповідальності та накладення адміністративного стягнення, мають одночасно вирішувати й питання про відшкодування винним майнової шкоди за

завдані суб'єкту права протиправними діями збитки. У такому разі в постанові суду суддя має зазначити розмір шкоди, що підлягає стягненню, порядок і строк її відшкодування. Розмір спричинених збитків має істотне значення і для правильної кваліфікації дій правопорушника, розмежування адміністративної та кримінальної відповідальності.

Для правомірного використання комп'ютерної програми у своїй діяльності покупець повинен отримати ліцензію або укласти договір з автором комп'ютерної програми чи з особою, яка правомірно володіє авторськими майновими правами на таку комп'ютерну програму. А при придбанні ліцензійних примірників комп'ютерних програм або примірників програм вільного користування покупець має отримати від продавця документальне підтвердження правомірності використання комп'ютерних програм, якими будуть слугувати саме перераховані вище ліцензії та договори. Крім того, слід пам'ятати, що примірники комп'ютерних програм, що реалізуються на дисках для лазерних систем зчитування (CD-дисках), обов'язково мають бути марковані контрольними марками.

При використанні комп'ютерних програм відповідно до вимог законодавства у сфері авторських прав користувачі зобов'язані дотримуватись певних умов, визначених у ліцензії чи в ліцензійному договорі або в іншому договорі щодо розпорядження майновими правами інтелектуальної власності. Комп'ютерні програми можуть використовуватись виключно в обсязі, формі та способом, вказаними в зазначених договорах (ліцензіях).

1.2. Юридичні гарантії використання електронного підпису в Україні

1.2.1. Історичні витоки використання підпису

Підпис як засвідчуваний знак з'явився з розвитком писемності, котра обслуговувала потреби держави, торгівлі, майнових відносин, суспільне життя, побут тощо. У зв'язку з розвитком ремесел і торгівлі застосовувані раніше родові знаки власності на предметах замінювалися підписами імені майстра і власника. Указані записи з часом почали застосовуватися і в ділових паперах, грошових, майнових і особистих документах. Так з'явився особистий підпис.

З подальшим зростанням документообігу використання особистого підпису для посвідчення документів оформлюється законодавчо: король Франції Генріх II у 1554 р. видав указ, котрим зобов'язав ставити особистий підпис на всіх документах. З часом чимало уваги приділяється питанням встановленню справжності особистого підпису та покарання за його підробку.

У судебнику царя Івана Грозного (1497 і 1550 рр.) згадується підробка чужого підпису. Звід законів Російської імперії 1842 р. регламентував порядок огляду документів при оспорюванні підпису і порівнянні зі зразками. Судові устави 1864 р. також вказували на можливість дослідження документів шляхом звіряння підпису на ньому з підписом тієї ж особи на інших несумнівних актах. Особи, які не володіли грамотністю, під документами ставили відбиток пальця руки.

1.2.2. Електронний підпис: поняття, характеристика, правове регулювання

Швидкий технологічний розвиток та глобальна сутність мережі інтернет вимагають розробки підходу, відкритого для різних технологій та послуг, який дає можливість засвідчувати інформацію електронним шляхом.

16 квітня 1997 р. Комісія ЄС представила до Європейського парламенту, Ради, Комітету з економічних і соціальних питань та Комітету у справах регіонів Комюніке про європейську ініціативу у сфері електронної комерції, а 8 жовтня 1997 р. – Комюніке про забезпечення безпеки та довіри у сфері електронного зв'язку – для входження до європейської системи електронних цифрових підписів та шифрування.

1 грудня 1997 р. Рада запропонувала Комісії якомога швидше подати пропозиції щодо Директиви Європейського парламенту та Ради про електронні цифрові підписи.

Електронний підпис не є прямим аналогом власноручного підпису і пов'язаний із певною технологією, що допускає специфічні умови і методики його застосування. Якщо обіг звичайного паперового документа пов'язаний із діяльністю двох сторін, то в разі застосування електронного підпису необхід-

ною є третя сторона – особа, яка користується довірою і може засвідчити вимогу однієї або двох сторін, що підпис було згенеровано особою, зазначеною в документі як людина, котра його підписала. Сукупність таких гарантів повинна становити інфраструктуру центрів сертифікації відкритих ключів, головне завдання яких полягає в тому, щоб гарантувати новому учаснику електронного документообігу, що наявні в нього копії відкритих ключів інших учасників, котрі він використовує для перевірки їхніх підписів, належать їм.

Основна мета застосування електронного підпису разом з інститутом сертифікації відкритих ключів – це надання електронному повідомленню статусу електронного документа за принципом функціональної еквівалентності, що зафіксовано в модельному законі Комісії ООН з міжнародного торговельного права про електронну комерцію, схваленому Резолюцією Генеральної асамблеї ООН від 16 грудня 1996 р. № А/31/628. Основним принципом використання електронного підпису є те, що повідомлення даних з таким підписом повинно розглядатися як еквівалент паперового документа з власноручним підписом.

Електронний зв'язок та комерція обумовлюють використання електронних підписів та суміжних послуг, що роблять можливим засвідчення достовірності інформації. Директива Європейського парламенту та Ради про систему електронних підписів, що застосовується в межах Співтовариств від 13 грудня 1999 р. № 1999/93/ЄС сприяє використанню електронних підписів та їх юридичному визнанню. Вона закладає правову основу для використання електронних підписів і певних послуг із сертифікації з метою забезпечення належного функціонування внутрішнього ринку. Для цілей цієї Директиви введені такі терміни:

– *електронний підпис* – дані, подані в електронній формі, які додаються чи логічно поєднуються з іншими електронними даними та які служать у якості методу засвідчення достовірності;

– *удосконалений електронний підпис* – електронний підпис, який відповідає наступним вимогам: пов'язаний винятково з особою, що підписалась; дає можливість ідентифікувати особу, що підписалась; створений за допомогою

засобів, які особа, що підписалась, може тримати під своїм повним контролем; пов'язаний із даними, до яких він відноситься, у такий спосіб, що будь-яку подальшу зміну даних можна виявити.

Стаття 5 Директиви Європейського парламенту про систему електронних підписів вказує: «Держави-члени забезпечують, щоб удосконалені електронні підписи, засновані на чинних сертифікатах і створені за допомогою безпечних механізмів створення підпису:

а) задовольняли юридичним вимогам до підписів стосовно даних, поданих у електронній формі, так само як підпис, написаний власноручно, задовольняє вимоги стосовно даних, нанесених на папір;

б) були прийнятними в якості доказів у судочинстві.

Держави-члени забезпечують неможливість позбавлення електронного підпису юридичної сили і прийнятності в якості доказу в судочинстві лише на тій підставі, що він:

– виконаний у електронній формі;

– не заснований на чинному сертифікаті;

– не заснований на чинному сертифікаті, виданому акредитованим постачальником послуг з сертифікації;

– не створений за допомогою безпечного механізму створення підпису.

Захист інформації визначається як забезпечення виконання постачальниками послуг із сертифікації та державними органами, відповідальними за акредитацію чи нагляд, вимог, передбачених Директивою Європейського парламенту та Ради про захист осіб від втручання у зв'язку із обробленням особистої інформації та вільним переміщенням такої інформації від 24 жовтня 1995 р. № 95/46/ЄС.

Директива Європейського парламенту та Ради про систему електронних підписів, що застосовуються в межах Співтовариства від 13 грудня 1999 р. № 1999/93 ЄС сприяє використанню підписів та їх юридичному визнанню, закладаючи правову основу для використання електронних підписів і певних послуг сертифікації з метою забезпечення належного функціонування внутріш-

нього ринку, а також містить вимоги до безпечних засобів створення підпису з метою забезпечення функціонування вдосконалених електронних підписів. Безпечні механізми створення підпису за допомогою відповідних технічних та процедурних засобів дозволяють забезпечувати таку ситуацію, за якої:

– дані, які використовуються для формування підпису, можуть виникнути на практиці лише один раз, а їх секретність забезпечується;

– дані, які використовуються для формування підпису, із значною часткою впевненості не можуть вилучатися з цих механізмів, а підпис захищається від підробки за допомогою використання доступних технологій;

– дані, що створюють підпис і які використовуються для вироблення підпису, можуть бути надійно захищені законною особою, яка підтверджує, що інші особи не матимуть змоги його використовувати.

Відповідно до рекомендацій для забезпечення перевірки підпису під час процесу перевірки із вмотивованою впевненістю має забезпечуватись, що:

– дані, які використовуються для перевірки підпису, відповідають інформації, котра надається контролюючому пристрою;

– контролюючий пристрій може у випадку необхідності точно встановлювати зміст підписаної інформації;

– дійсність сертифіката, що вимагається під час перевірки підпису, ретельно перевіряється;

– результат перевірки та ідентичність підпису виводяться на екран;

– використання псевдоніму чітко вказується;

– будь-які зміни, що стосуються безпеки, можуть бути виявлені.

Закон України «Про електроні довірчі послуги» від 5 жовтня 2017 р. № 2155-VIII визначає правові та організаційні засади надання електронних довірчих послуг, у тому числі транскордонних, права та обов’язки суб’єктів правових відносин у сфері електронних довірчих послуг, порядок здійснення державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також правові та організаційні засади здійснення електронної ідентифікації.

Цей Закон визначає основні терміни в цій сфері:

автентифікація – електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-телекомунікаційної системи та/або походження та цілісність електронних даних;

електронна довірча послуга – послуга, яка надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги;

електронна ідентифікація – процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи;

електронна позначка часу – електронні дані, які пов'язують інші електронні дані з конкретним моментом часу для засвідчення наявності цих електронних даних на цей момент часу;

електронна послуга – будь-яка послуга, що надається через інформаційно-телекомунікаційну систему;

електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис;

електронні дані – будь-яка інформація в електронній формі;

ідентифікація особи – процедура використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи;

інтероперабельність – технологічна сумісність технічних рішень, що використовуються під час надання електронних послуг, та їх здатність взаємодіяти між собою;

кваліфікований електронний підпис – удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа;

компрометація особистого ключа – будь-яка подія, що призвела або може призвести до несанкціонованого доступу до особистого ключа;

користувачі електронних довірчих послуг – підписувачі, створювачі електронних печаток, відправники та отримувачі електронних даних, інші фізичні та юридичні особи, які отримують електронні довірчі послуги у надавачів таких послуг відповідно до вимог цього Закону;

особистий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;

сертифікат відкритого ключа – електронний документ, який засвідчує належність відкритого ключа фізичній або юридичній особі, підтверджує її ідентифікаційні дані та/або надає можливість здійснити автентифікацію веб-сайту;

технологічна нейтральність національних технічних рішень – невтручання органів, що здійснюють державне регулювання у сфері електронних довірчих послуг, у процес розроблення програмно-технічних комплексів, засобів електронного підпису чи печатки та засобів криптографічного захисту інформації, який не перешкоджатиме досягненню інтероперабельності між ними;

удосконалений електронний підпис – електронний підпис, створений за результатом криптографічного перетворення електронних даних, з якими пов’язаний цей електронний підпис, з використанням засобу удосконаленого електронного підпису та особистого ключа, однозначно пов’язаного з підписувачем, і який дає змогу здійснити електронну ідентифікацію підписувача та виявити порушення цілісності електронних даних, з якими пов’язаний цей електронний підпис.

Інші терміни вживаються у значеннях, наведених у Цивільному кодексі України, законах України «Про електронні документи та електронний документообіг», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про стандартизацію», «Про технічні регламенти та оцінку відповідно-

ті», «Про наукову і науково-технічну експертизу», «Про Національний банк України».

Державне регулювання та управління у сферах електронних довірчих послуг та електронної ідентифікації здійснюється на засадах:

– забезпечення принципу верховенства права у процесі надання і отримання електронних довірчих послуг та електронної ідентифікації;

– вільного обігу електронних довірчих послуг в Україні, а також можливості вільного надання електронних довірчих послуг надавачами електронних довірчих послуг, розташованими в інших державах, діяльність яких відповідає вимогам Закону України «Про електронні довірчі послуги»;

– відповідності вимог до надання електронних довірчих послуг та електронної ідентифікації європейським та міжнародним стандартам;

– забезпечення захисту персональних даних, що обробляються під час надання електронних довірчих послуг та електронної ідентифікації.

Метою здійснення державного регулювання та управління у сферах електронних довірчих послуг та електронної ідентифікації є проведення єдиної та ефективної державної політики у сферах електронних довірчих послуг та електронної ідентифікації та сприяння інтеграції України у світовий електронний інформаційний простір.

Електронний підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів.

Електронний підпис використовується фізичними та юридичними особами – суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Використання електронного підпису не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі.

Нотаріальні дії з використанням кваліфікованого електронного підпису чи печатки або інших засобів електронної ідентифікації вчиняються в порядку,

визначеному головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері нотаріату.

Здійснення правосуддя з використанням кваліфікованого електронного підпису чи печатки або інших засобів електронної ідентифікації вчиняється в порядку, встановленому законом.

Використання електронних довірчих послуг не змінює порядку вчинення правочинів, встановленого законом.

Правочини, що підлягають нотаріальному посвідченню та/або державній реєстрації у випадках, встановлених законом, вчиняються в електронній формі виключно із застосуванням кваліфікованих електронних довірчих послуг та у встановленому порядку. Правочин, вчинений в електронній формі, може бути визнаний судом недійсним у разі, коли під час його вчинення використовувався кваліфікований електронний підпис чи печатка, кваліфікований сертифікат якого/якої не містить відомостей, передбачених частиною другою цієї статті, або містить недостовірні відомості.

Кваліфікований електронний підпис має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису. Кваліфікована електронна печатка має презумпцію цілісності електронних даних і достовірності походження електронних даних, з якими вона пов’язана. Електронний підпис чи печатка не можуть бути визнані недійсними та позбавлені можливості розглядатися як доказ у судових справах виключно на тій підставі, що вони мають електронний вигляд або не відповідають вимогам до кваліфікованого електронного підпису чи печатки.

Засоби кваліфікованого електронного підпису чи печатки повинні забезпечувати належний рівень унікальності пари ключів, що ними генеруються, конфіденційність особистих ключів під час їх генерації, зберігання та створення кваліфікованого електронного підпису чи печатки, а також захист від доступу до особистих ключів сторонніх осіб. Кваліфікований сертифікат відкритого ключа вважається чинним у разі, якщо на момент перевірки чинності строк дії, зазначений у кваліфікованому сертифікаті відкритого ключа, не закінчився.

Допускається ідентифікація фізичної особи кваліфікованим надавачем електронних довірчих послуг за ідентифікаційними даними, що містяться у раніше сформованому ним кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифіката.

Електронні дані, які відправлені та отримані з використанням кваліфікованої електронної довірчої послуги реєстрованої електронної доставки, не можуть бути позбавлені юридичної сили і можливості розглядатися як доказ у судових справах виключно на тій підставі, що вони мають електронну форму, якщо такі дані відповідають вимогам до кваліфікованої електронної довірчої послуги реєстрованої електронної доставки. Електронні дані, які відправлені та отримані з використанням кваліфікованої електронної довірчої послуги реєстрованої електронної доставки, мають презумпцію цілісності електронних даних, їх гарантованої передачі ідентифікованим відправником та гарантованого отримання ідентифікованим отримувачем, а також точності дати і часу відправки та отримання електронних даних, які вказуються під час надання цієї послуги.

Оцінка відповідності вимогам до кваліфікованих надавачів електронних довірчих послуг та послуг, що ними надаються, здійснюється з урахуванням вимог законодавства щодо порядку надання і використання кваліфікованих електронних довірчих послуг, у тому числі у банківській системі України та при здійсненні переказу коштів, а також з урахуванням вимог законодавства у сфері захисту інформації. Кваліфіковані надавачі електронних довірчих послуг, які пройшли процедуру оцінки відповідності у сфері електронних довірчих послуг та відомості про яких були внесені до Довірчого списку, повинні кожні 24 місяці за власний рахунок проходити процедуру оцінки відповідності для доведення того, що вони та електронні довірчі послуги, які ними надаються, відповідають вимогам до кваліфікованих надавачів електронних довірчих послуг та послуг, що ними надаються.

Україна бере участь у міжнародному співробітництві у сферах електронних довірчих послуг та електронної ідентифікації, зокрема на основі міжнарод-

них договорів України. Порядок використання інформаційно-телекомунікаційної системи центрального засвідчувального органу для забезпечення визнання в Україні електронних довірчих послуг, іноземних сертифікатів відкритих ключів, що використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб'єктами різних держав, встановлюється Кабінетом Міністрів України.

Електронний зв'язок та комерція обумовлюють використання електронних підписів та суміжних послуг, що роблять можливим засвідчення достовірності інформації.

1.2.3. Електронна комерція: поняття і правове регулювання

Стрімкий розвиток комп'ютерних мереж публічного доступу сприяв виникненню таких економічних і правових понять, як «електронна комерція», «економіка в режимі реального часу», що внесло відповідні зміни у сферу правового регулювання бізнесу.

Електронна комерція в юридичному значенні являє собою укладання на міжнародному і внутрішньому ринках в електронному вигляді цілого ряду підприємницьких угод, таких як купівля-продаж, поставка, угоди про поділ продукції, страхування, банківські угоди, перевезення вантажів або пасажирів повітряним, морським, залізничним транспортом, а також інших угод, пов'язаних із промисловою та діловою співпрацею.

Основу електронної комерції складає електронний обмін даними – відомостями у формі електронних повідомлень, що створюються, зберігаються або передаються з використанням електронних, оптичних або аналогових засобів. На основі електронного обміну даними будується система електронного документообігу.

Розвитку інформаційних послуг перешкоджає ряд правових перепон на шляху до ефективного функціонування внутрішнього ринку, які роблять реалізацію свободи організації та свободи надання послуг менш привабливою. Ці перешкоди виникають із розбіжностей у законодавстві та з правової невизначеності щодо вибору тих норм національного законодавства, які мають бути засто-

совані до таких послуг, а за умов відсутності координації та адаптації законодавства у відповідних сферах, перешкоди можуть бути обґрунтовані на підставі прецедентного права, відповідно до якого здійснює судочинство Європейський суд справедливості; має місце правова невизначеність щодо того, до якої міри держави-члени можуть контролювати послуги, що надаються іншою державою-членом.

У 1996 р. з метою усунення юридичних перешкод у використанні сучасних засобів зв'язку для укладання міжнародних торгових договорів і для встановлення визначеності щодо юридичної сили та дійсності угод, що укладаються таким способом Комісія ООН з права міжнародної торгівлі Резолюцією № 51/162 від 16 грудня 1996 р. прийняла Типовий закон про електронну торгівлю, який пропонує законодавцям зібрання міжнародних норм, що встановлюють можливий порядок усунення юридичних перешкод і створення більш надійної бази для електронної торгівлі.

Метою Директиви Європейського парламенту та Ради «Про деякі правові аспекти інформаційних послуг, зокрема електронної комерції, на внутрішньому ринку» (Директива про електронну комерцію) від 8 червня 2000 р. № 2000/31/ЄС є створення правової структури для забезпечення вільного переміщення інформаційних послуг між державами-членами, а не гармонізація сфер дії кримінального права як такого.

Інформаційні послуги охоплюють широкий спектр сфер економічної діяльності, що здійснюється в оперативному режимі[71]. Інформаційні послуги не обмежуються виключно послугами, які забезпечують інтерактивне укладання договорів, але, оскільки вони є економічною діяльністю, то включають у себе й послуги, надання яких не оплачується їх одержувачами – такими, як ті, хто пропонує інтерактивну інформацію чи комерційні повідомлення, або ті, хто забезпечує механізми, що дозволяють пошук, доступ та отримання інформації; інформаційні послуги також включають у себе послуги, що складаються з передання інформації через мережу зв'язку, надання доступу до мережі зв'язку чи послуги

[71] Конвенція про інформаційне та правове співробітництво стосовно «Інформаційних суспільних послуг» (ETS № 180).

з розміщення інформації, що надається одержувачем послуг. Використання електронної пошти чи еквівалентного індивідуального зв'язку, наприклад, фізичними особами, які діють не з метою здійснення професійної чи комерційної діяльності, у тому числі використання ними вищезазначеного виду пошти та зв'язку для укладання контрактів між такими особами, не є інформаційними послугами. З метою безперешкодного розвитку електронної комерції правова система має бути чіткою та простою, передбачливою та узгодженою із нормами, що застосовуються на міжнародному рівні таким чином, щоб їх застосування не справляло негативного впливу на конкурентоспроможність промисловості чи не перешкоджало інноваціям у цій сфері.

У тих випадках, коли сторони, що укладають договір, є резидентами України, не виникає будь-яких проблем. Складніше питання вирішується, коли продавець – іноземна компанія, оскільки це спричиняє проблему ідентифікації суб'єкта. Якщо учасники торгових відносин є представниками різних держав, то при укладанні електронних договорів доцільно звертатися до норм міжнародного права. Електронну торгівлю за участю іноземних суб'єктів можна розглядати як зовнішньоекономічну діяльність, а отже, для регулювання таких відносин використовуються положення Закону України «Про зовнішньоекономічну діяльність» від 16 квітня 1991 р. № 959-XII.

1.2.4. Електронний документ і електронний документообіг

Якщо ж сторони, що укладають договір у межах електронної комерції, є резидентами України, то на них поширюється дія Закону України «Про електронні документи та електронний документообіг» від 22 травня 2003 р. № 851-IV. Це, зокрема, стосується відносин, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів.

Крім даного Закону, відносини, пов'язані з електронним документообігом та використанням електронних документів, регулюються Конституцією України, Цивільним кодексом України, законами України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю»,

«Про телекомунікації» від 18 листопада 2003 р. № 1280-IV, «Про обов'язковий примірник документів» від 9 квітня 1999 р. № 595-XIV, «Про Національний архівний фонд та архівні установи» від 24 грудня 1993 р. № 3814-XII, а також іншими нормативно-правовими актами.

Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається чинним законодавством. *Обов'язковий реквізит електронного документа* – обов'язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили.

Електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу. Накладанням електронного підпису завершується створення електронного документа. Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

Електронний документообіг (обіг електронних документів) – сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та в разі необхідності з підтвердженням факту одержання таких документів.

Електронний документообіг здійснюється відповідно до чинного законодавства України або на підставі договорів, що визначають взаємовідносини суб'єктів електронного документообігу. Використання електронного документа в цивільних відносинах здійснюється згідно із загальними вимогами вчинення правочинів, встановлених цивільним законодавством. При зберіганні електронних документів обов'язкове додержання таких вимог:

– інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;

– має бути забезпечена можливість відновлення електронного документа в тому форматі, у якому він був створений, відправлений або одержаний;

– у разі наявності повинна зберігатися інформація, яка дає змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання.

Суб'єкти електронного документообігу, які здійснюють його на договірних засадах, самостійно визначають режим доступу до електронних документів, що містять конфіденційну інформацію, та встановлюють для них систему (способи) захисту.

В інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах, які забезпечують обмін електронними документами, що містять інформацію, яка є власністю держави, або інформацію з обмеженим доступом, повинен забезпечуватися захист цієї інформації відповідно до чинного законодавства. Особи, винні в порушенні законодавства про електронні документи та електронний документообіг, несуть відповідальність згідно з законами України.

Отже, сучасний документообіг викликав необхідність введення нового виду документа – електронного, у якому інформація представлена у формі електронних даних, включаючи відповідні реквізити, у тому числі й електронний підпис. Значення електронного підпису як посвідчення, що покликане підтвердити цілісність документа, а також необхідність ідентифікації особи, яка його підписала, зберігається.

Хоча електронний підпис не залежить від навичок особи, при його безпосередньому виконанні також можуть виникнути певні проблеми, зокрема йдеться про можливість ненавмисного викривлення через незвичні умови виконання та навмисне викривлення з метою подальшої відмови від підпису, а тому перед законодавцем стоять питання необхідності удосконалення наявних та розроблення нових способів захисту такої інформації від несанкціонованого доступу.

1.3. Криптографічний захист конфіденційної інформації в Україні

Захист конфіденційної інформації, що циркулює (передається, приймається), опрацьовується та/або зберігається в спеціальних інформаційно-телекомунікаційних та інших системах, забезпечується застосуванням засобів криптографічного захисту інформації (КЗІ), а також виконанням відповідних організаційно-технічних та режимних заходів.

Основними нормативними актами, що регулюють використання криптографії в Україні, є закони України «Про інформацію», «Про науково-технічну інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про Національну систему конфіденційного зв'язку» від 10 січня 2002 р. № 2919-III, «Про електроні довірчі послуги»

Криптографічний захист інформації (КЗІ) – вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Засіб криптографічного захисту інформації – апаратний, програмний, апаратно-програмний або інший засіб, призначений для криптографічного захисту інформації.

Криптографічний алгоритм – алгоритм, який визначає правила перетворення інформації з метою її криптографічного захисту.

Криптографічна система – сукупність засобів КЗІ, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи безпеки), використання яких забезпечує належний рівень захищеності інформації, що опрацьовується, зберігається та/або передається.

Залежно від призначення встановлюються такі категорії засобів КЗІ:

– засоби шифрування інформації;

– засоби, призначені для виготовлення ключових даних або ключових документів (незалежно від виду носія ключової інформації) та управління ключовими даними, що використовуються в засобах КЗІ;

– засоби захисту від нав’язування неправдивої інформації або захисту від несанкціонованої модифікації, що реалізовують алгоритми криптографічного перетворення інформації, у тому числі засоби імітозахисту та електронного підпису;

– засоби захисту інформації від несанкціонованого доступу (у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки), у яких реалізовані криптоалгоритми.

До засобів КЗІ належать:

– *ключові дані* – деякий набір значень змінних параметрів криптографічного перетворення, використання яких дає змогу досягти мети цього перетворення;

– *ключові документи* – матеріальні об’єкти із зафіксованими відповідним чином ключовими даними для подальшого практичного застосування щодо криптографічного перетворення повідомлення;

– обладнання КЗІ – технічні засоби, що взаємодіють із засобами КЗІ або керують ними та можуть впливати на їх криптографічні якості;

– *режим безпеки* – реалізована система правових норм, організаційних та організаційно-технічних заходів, яка створюється на підприємствах під час опрацювання, дослідження, виробництва та експлуатації засобів КЗІ з метою обмеження доступу до конфіденційної інформації;

– спеціальні вимоги – вимоги до принципів побудови засобів КЗІ та технічної реалізації криптографічних алгоритмів у засобах КЗІ, вимоги до криптографічних якостей, а також вимоги і норми щодо захисту від можливих каналів витоку небезпечних сигналів засобів КЗІ;

– спеціальні інформаційно-телекомунікаційні системи – інформаційно-телекомунікаційні системи, призначені для обробки інформації з обмеженим доступом, у яких захист інформації забезпечується у тому числі з використанням засобів КЗІ;

– технічний засіб обробки інформації – технічний засіб, призначений для приймання, накопичення, зберігання, пошуку, перетворення, відображення та передавання інформації каналами зв’язку;

– управління ключовими даними – дії, пов’язані з генерацією, розподіленням, доставлянням, уведенням у дію, зміненням, зберіганням, обліком та знищенням ключових даних, а також носіїв ключових даних;

– експертиза в галузі КЗІ (далі – експертиза) – науково-технічна діяльність, метою якої є дослідження, аналіз, оцінка або перевірка рівня захисту інформації в засобах КЗІ;

– експертний висновок – відповідним чином документально оформлені результати експертизи.

Засоби КЗІ повинні розроблятися з урахуванням можливих загроз з боку середовища, у якому передбачається їх застосування. Розробник повинен передбачити організаційно-технічні заходи щодо захисту від несанкціонованого доступу, контролю цілісності програмного забезпечення засобу КЗІ, забезпечення надійного механізму тестування засобу КЗІ на правильність функціонування, а також обов’язкового блокування роботи засобу КЗІ у разі виявлення порушень. У засобах КЗІ повинні використовуватися криптоалгоритми та криптопротоколи, які є державними стандартами України або рекомендовані Департаментом. Для розробки засобів КЗІ використовується тільки ліцензійне програмне забезпечення.

Залежно від способу реалізації розрізняють такі типи засобів КЗІ:

– апаратні засоби, алгоритм функціонування (у тому числі криптографічні функції) яких реалізовується в оптичних, механічних мікроелектронних або інших спеціалізованих пристроях та не може бути змінений під час експлуатації;

– апаратно-програмні засоби, алгоритм функціонування (у тому числі криптографічні функції) яких реалізується програмним забезпеченням, яке встановлюється під час виробництва засобу КЗІ у спеціальному запам’ятовуючому пристрої, виконується в ньому та може бути змінено лише під час виробництва;

– програмні засоби, алгоритм функціонування яких реалізується програмним забезпеченням, що функціонує під управлінням операційних систем електронно-обчислювальної техніки; окремі функції програмного засобу КЗІ (у тому чис-

лі криптографічні перетворення) можуть виконуватися апаратними або апаратно-програмними пристроями, що функціонують під управлінням програмного забезпечення засобу КЗІ.

Звичайно користувач апаратних засобів криптографічного захисту інформації не має доступу до змісту запам'ятовувальних елементів, що зберігають мікропрограми керування пристроєм, алгоритм функціонування пристрою змінюється тільки їх розробником або виробником.

Засоби криптографічного захисту інформації без уведених ключових даних мають *гриф обмеження доступу*, який відповідає грифу обмеження доступу опису криптосхеми. Гриф обмеження доступу засобів криптографічного захисту інформації з уведеними ключовими даними визначається грифом обмеження доступу ключових документів, але не нижче грифа обмеження доступу опису криптосхеми.

Гриф обмеження доступу ключових документів, що використовуються для криптографічного захисту інформації, повинен відповідати грифу обмеження доступу інформації, що захищається.

Суб'єкти господарювання, які здійснюють розроблення, виробництво, сертифікаційні випробування (експертні роботи) та експлуатацію засобів криптографічного захисту інформації, повинні мати відповідні ліцензії на розроблення, виробництво, сертифікаційні випробування, експертизу та експлуатацію криптосистем та засобів криптографічного захисту інформації, крім випадків, передбачених законодавством України. Суб'єкти, які здійснюють розроблення, виробництво та експлуатацію засобів КЗІ, визначають режим доступу до інформації про ці засоби, установлюють і підтримують відповідний режим безпеки з урахуванням вимог замовника та відповідно до нормативно-правових актів у сфері КЗІ.

Застосування засобів криптографічного захисту інформації під час міжнародного обміну інформацією здійснюється відповідно до законодавства та міжнародних угод (договорів) України.

На теперішній час методи і засоби криптографії використовують для забезпечення інформаційної безпеки не тільки держави, а й приватних осіб та організацій, реалізуючи різноманітні механізми захисту конфіденційності, цілісності, доступності та повноти інформації.

РОЗДІЛ 2. ІННОВАЦІЙНІ ЗАСОБИ ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

2.1. Державна політика у сфері технічного захисту інформації

2.1.1. Правове забезпечення технічного захисту інформації в Україні

Впровадження в усі сфери життєдіяльності людини і громадянина, суспільства та держави інформаційних технологій зумовило поширення великих масивів інформації в обчислювальних та інформаційних мережах на значних територіях.

Прогрес у різних галузях науки і техніки призвів до створення компактних та високоефективних технічних засобів, за допомогою яких можна підключатись до ліній телекомунікацій та різноманітних технічних засобів опрацювання інформації вітчизняного та іноземного виробництва з метою здобування, пересилання та аналізу розвідувальних даних. Для цього може використовуватись апаратура радіо, радіотехнічної, оптико-електронної, радіотеплової, акустичної, хімічної, магнітометричної, сейсмічної та радіаційної розвідок. Комунікаційне обладнання іноземного виробництва, яке використовується в мережах зв’язку, передбачає дистанційний доступ до його апаратних та програмних засобів, у тому числі з-за кордону, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв’язку та змістом повідомлень, які пересилаються.

За таких умов створились можливості витоку інформації, порушення її цілісності та блокування. Витік інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю дер-

жави, – це одна з основних можливих загроз національній безпеці України в інформаційній сфері.

Правову основу технічного захисту інформації в Україні становлять Конституція України, закони України, акти Президента України та Кабінету Міністрів України, нормативно-правові акти Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України, інших державних органів, міжнародні договори України з питань технічного захисту інформації, згода на обов'язковість яких надана Верховною Радою України, а також Положення про технічний захист інформації в Україні.

2.1.2. Концепція технічного захисту інформації в Україні

Концепція технічного захисту інформації в Україні[72] визначає основи державної політики у сфері захисту інформації інженерно-технічними заходами, забезпечуючи єдність принципів формування і проведення такої політики в усіх сферах життєдіяльності особи, суспільства та держави (соціальній, політичній, економічній, військовій, екологічній, науково-технологічній, інформаційній тощо). Технічний захист інформації є складовою частиною забезпечення національної безпеки України.

Технічний захист інформації (ТЗІ) – це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

Система ТЗІ – це сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та матеріально-технічна база.

[72] Про затвердження Концепції технічного захисту інформації в Україні [Електронний ресурс] : постанова Кабінету Міністрів України від 8 жовт. 1997 р. № 1126. – Режим доступу: http:/zakon.rada.gov.ua/cgi–bin/laws/mair.cgi?nreg=1126-97-%EF/.

Комплекс технічного захисту інформації – це сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об'єкті.

Загрози безпеці інформації в Україні зумовлені:

– невиваженістю державної політики в галузі інформаційних технологій, що може призвести до безконтрольного та неправомочного доступу до інформації та її використання;

– діяльністю інших держав, спрямованою на одержання переваги в зовнішньополітичній, економічній, військовій та інших сферах;

– недосконалістю організації в Україні міжнародних виставок апаратури різного призначення (особливо пересувних) та заходів екологічного моніторингу, що може використовуватися для здобування інформації розвідувального характеру;

– діяльністю політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб, спрямованою на одержання переваги в політичній боротьбі та конкуренції;

– злочинною діяльністю, спрямованою на протизаконне одержання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним чи фізичним особам;

– використанням інформаційних технологій низького рівня, що призводить до впровадження недосконалих технічних засобів із захистом інформації, засобів контролю за ефективністю технічного захисту інформації та засобів технічного захисту інформації (засоби забезпечення технічного захисту інформації);

– недостатністю документації на засоби забезпечення ТЗІ іноземного виробництва, а також низькою кваліфікацією технічного персоналу.

2.1.3. Пріоритетні напрями інноваційної державної політики у сфері технічного захисту інформації

Державна політика у сфері ТЗІ визначається пріоритетністю національних інтересів, має на меті унеможливлення реалізації загроз для інформації та

здійснюється шляхом виконання положень цієї Концепції, а також програм розвитку ТЗІ та окремих проектів.

Основними напрямами державної політики у сфері ТЗІ є:

1) нормативно-правове забезпечення:

– удосконалення чинних та створення нових нормативно-правових актів щодо захисту інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що належить державі;

– розроблення нормативно-правових актів щодо захисту відкритої інформації, важливої для особи, суспільства та держави;

– удосконалення правових механізмів організаційного забезпечення ТЗІ;

– удосконалення нормативно-правових актів щодо умов і правил провадження діяльності у сфері ТЗІ;

– розроблення нормативно-правових актів щодо визначення статусу головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій;

– удосконалення нормативно-правових актів щодо здійснення контролю за імпортом з метою впровадження в Україні іноземних інформаційних технологій із захистом інформації та засобів забезпечення ТЗІ;

– розроблення нормативних документів з питань формування та розвитку моделі загроз для інформації;

– розроблення нормативних документів з питань сертифікації засобів забезпечення ТЗІ та атестації на відповідність вимогам ТЗІ об’єктів, робота яких пов’язана з інформацією, що підлягає технічному захисту;

– удосконалення чинних та розроблення нових нормативних документів з питань ТЗІ:

а) у засобах обчислювальної техніки, в автоматизованих системах, оргтехніці, мережах зв’язку, комп’ютерних мережах та приміщеннях, де циркулює інформація, що підлягає технічному захисту;

б) під час створення, експлуатації та утилізації зразків озброєнь, військової та спеціальної техніки;

в) під час проектування, будівництва і реконструкції військово-промислових, екологічно небезпечних та інших особливо важливих об’єктів;

2) організаційне забезпечення:

– забезпечення створення підрозділів ТЗІ в органах державної влади та органах місцевого самоврядування, академіях наук, Збройних силах, інших військових формуваннях, органах внутрішніх справ, на підприємствах, в установах і організаціях усіх форм власності, діяльність яких пов’язана з інформацією, що підлягає технічному захисту;

– створення головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій, а також лабораторій системи сертифікації засобів забезпечення ТЗІ;

– підготовка кадрів для роботи у сфері ТЗІ;

– залучення до розв’язання проблем ТЗІ вітчизняних учених та висококваліфікованих спеціалістів;

– розвиток міжнародного співробітництва у сфері ТЗІ;

3) науково-технічна та виробнича діяльність:

– моніторинг і оцінка стану ТЗІ, підготовка аналітичних матеріалів і пропозицій щодо стратегії його розвитку;

– створення інформаційно-аналітичних моделей загроз для інформації та методології їх прогнозування;

– обґрунтування критеріїв та показників рівнів ТЗІ;

– створення методології синтезу систем багаторівневого захисту інформації, адекватних масштабам загроз безпеці інформації та режиму доступу до неї;

– створення методології, призначеної для визначення зниження ефективності продукції, зумовленої витоком інформації про неї, порушенням її цілісності чи блокуванням, та методології обґрунтування заходів ТЗІ;

– системне і поетапне розроблення сучасних засобів забезпечення ТЗІ;

– пріоритетне створення вітчизняних конкурентоспроможних інформаційних технологій та розвиток виробництва засобів забезпечення ТЗІ;

– створення умов для забезпечення головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій, а також лабораторій системи сертифікації засобів забезпечення ТЗІ науковим, контрольно-вимірювальним, випробувальним та виробничим обладнанням.

Першочерговими заходами щодо реалізації державної політики у сфері ТЗІ є:

– створення правових засад реалізації державної політики у сфері ТЗІ, визначення послідовності та порядку розроблення відповідних нормативно-правових актів;

– визначення перспективних напрямів обробленання нормативних документів з питань ТЗІ на основі аналізу стану відповідної вітчизняної та зарубіжної нормативної бази, розроблення зазначених нормативних документів;

– визначення номенклатури вітчизняних засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв’язку, призначених для оброблення інформації з обмеженим доступом, інших засобів забезпечення ТЗІ в органах державної влади та органах місцевого самоврядування, Національній академії наук, Збройних силах, інших військових формуваннях, органах внутрішніх справ;

– налагодження згідно з визначеною номенклатурою виробництва засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв’язку із захистом інформації, інших вітчизняних засобів забезпечення ТЗІ;

– завершення створення та розвиток системи сертифікації вітчизняних та закордонних засобів забезпечення ТЗІ;

– визначення реальних потреб системи ТЗІ у фахівцях, розвиток та вдосконалення системи підготовки, перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ.

Необхідно розуміти, що не може бути інформаційної безпеки без застосування спеціальних технічних засобів та методів для захисту інформації від несанкціонованого доступу.

Реалізація державної політики щодо захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах полягає у:

– підготовці пропозицій до визначення загальної стратегії та пріоритетних напрямів діяльності у сфері захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

– виконанні обов’язків уповноваженого органу у сфері захисту інформації в інформаційно-телекомунікаційних системах;

– розробленні порядку та вимог до захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також погодження проектів нормативно-правових актів з цих питань;

– розробленні критеріїв та порядку оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо.

Реалізація державної політики забезпечується шляхом виконання низки заходів відповідно до визначених завдань, а саме:

– методичного керівництва та координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності з питань, пов'язаних із запобіганням вчиненню порушень безпеки інформації в інформаційно-телекомунікаційних системах, виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

– накопичення та аналізу даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також про їх наслідки;

– організації та здійснення оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, надання відповідних рекомендацій.

Витік інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, – це одна з основних можливих загроз національній безпеці України в інформаційній сфері.

З метою забезпечення єдиного підходу щодо захисту державних інформаційних ресурсів на виконання постанови Кабінету Міністрів України від 24.02.2003 № 208 «Про заходи щодо створення електронної інформаційної системи «Електронний Уряд» в рамках Національної системи конфіденційного зв'язку у м. Києві, створено окрему підсистему для телекомунікаційного забезпечення функціонування Єдиного веб-порталу органів виконавчої влади.

На виконання завдань Національної програми інформатизації у межах виконання проекту «Забезпечити антивірусний захист державних інформаційних ресурсів» створено Центр антивірусного захисту інформації (ЦАЗІ). Одним із основних завдань ЦАЗІ є впровадження єдиної технологічної політики щодо антивірусного захисту інформації в інформаційно-телекомунікаційних системах органів державної влади, а також централізованого забезпечення їх антивірусними програмними продуктами, сертифікованими у встановленому законодавством України порядку.

Сьогодні до бази антивірусного програмного забезпечення ЦАЗІ з використанням мережі Інтернет підключено 66 адміністраторів безпеки інформаційно-телекомунікаційних систем органів державної влади. Також з використанням ресурсів ЦАЗІ проводяться державні експертизи антивірусних програмних засобів з метою визначення можливості їх застосування в Україні та експрес-експертизи антивірусних оновлень до них.

З метою проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах відповідно до затвердженого постановою Кабінету Міністрів України від 03.08.2005 № 688 Положення утворено Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління. Забезпечення функ-

ціонування цього Реєстру покладено на Департамент безпеки інформаційно-телекомунікаційних систем.

Реалізація вимог Положення створює передумови для:

– запровадження єдиної системи обліку відомостей про ІТС органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління;

– проведення аналізу стану захисту державних електронних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

– надання методичної допомоги і координування діяльності міністерств та інших центральних органів виконавчої влади, пов’язаної із захистом державних електронних інформаційних ресурсів в інформаційно-телекомунікаційних системах.

З метою оптимізації дій щодо недопущення реалізації загроз інформаційним ресурсам держави необхідно здійснювати проведення оцінювання (аудиту) стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, зокрема тих, що мають доступ до мережі Інтернет.

Подальшим кроком у напрямку організації та здійснення оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах має стати підготовка та видання відповідних нормативно-правових актів та нормативних документів, які б, з урахуванням міжнародного досвіду, дозволили оптимізувати вироблення єдиних критеріїв та порядку такого оцінювання.

На сьогодні з метою здійснення упереджувальних заходів та розвитку методології запобігання порушенню цілісності, доступності та конфіденційності державних інформаційних ресурсів проводяться заходи, спрямовані на підготовку до ліквідації наслідків несанкціонованих дій, що порушили безперебійне функціонування інформаційно-телекомунікаційних систем органів державної влади, поширюється інформація щодо наявних та ймовірних загроз, інструментів і засобів забезпечення безпеки інформації тощо.

В Адміністрації Держспецзв'язку України функціонує підрозділ, діяльність якого спрямована саме на вирішення таких завдань. Надання, в подальшому, відповідних повноважень та реєстрація встановленим порядком українського аналога CSIRT (Computer Security Incident Response Teams – структури швидкого реагування на інциденти, що загрожують безпеці інформаційних ресурсів) сприятиме ефективній реалізації державної політики у сфері захисту державних інформаційних ресурсів в ІТС, та підвищенню загального стану захисту національного інформаційного простору.[73]

Указом Президента України «Про Положення про технічний захист інформації в Україні» визначається, що технічний захист інформації здійснюється щодо органів державної влади, органів місцевого самоврядування, органів управління Збройних сил України та інших військових формувань, утворених згідно із законодавством України, відповідних підприємств, установ, організацій.

Рівень безпеки інформації, що обробляється в системах та на об'єктах інформаційної інфраструктури, визначається такими властивостями:

– *конфіденційність* – властивість інформації бути захищеною від несанкціонованого ознайомлення;

– *цілісність* – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;

– *доступність* – властивість інформації бути захищеною від несанкціонованого блокування.

Суб'єктами системи технічного захисту інформації є:

1) Державна служба спеціального зв'язку та захисту інформації України;

2) органи, щодо яких здійснюється ТЗІ;

3) науково-дослідні та науково-виробничі установи Держспецзв'язку України, державні підприємства, що перебувають в управлінні Держспецзв'язку України та виконують завдання з питань технічного захисту інформації;

[73] Згідно ст. 9 Закону України «Про основні засади забезпечення кібербезпеки України» в нашій державі регламентується правовий порядок діяльності урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

4) військові частини, підприємства, установи та організації всіх форм власності й громадяни-підприємці, які провадять діяльність з технічного захисту інформації за відповідними дозволами або ліцензіями;

5) навчальні заклади з підготовки, перепідготовки та підвищення кваліфікації фахівців з технічного захисту інформації.

Основними завданнями органів, щодо яких здійснюється ТЗІ, є:

– забезпечення технічного захисту інформації згідно з вимогами нормативно-правових актів з питань технічного захисту інформації;

– видання в межах своїх повноважень нормативно-правових актів із зазначених питань;

– здійснення контролю за станом технічного захисту інформації.

Організаційно-технічні принципи, порядок здійснення заходів із технічного захисту інформації, порядок контролю в цій сфері, характеристики загроз для інформації, норми та вимоги з технічного захисту інформації, порядок атестації та експертизи комплексів технічного захисту інформації визначаються нормативно-правовими актами, прийнятими в установленому порядку відповідними органами.

Згідно з наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Положення про державний контроль за станом технічного захисту інформації» від 16 травня 2007 р. № 87 визначаються порядок організації та здійснення державного контролю за станом технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Контрольно-інспекторська робота з питань ТЗІ – діяльність, спрямована на визначення та вдосконалення стану ТЗІ в органах, щодо яких здійснюється ТЗІ. Вона включає планування, проведення інспекційних перевірок стану ТЗІ в органах, щодо яких здійснюється ТЗІ (далі – перевірка), аналіз їх результатів та надання рекомендацій щодо вдосконалення стану ТЗІ в зазначених органах.

При *комплексній перевірці* визначається відповідність комплексу ТЗІ (комплексної системи захисту інформації) та заходів протидії технічним розвід-

кам вимогам нормативно-правових актів та нормативних документів системи ТЗІ.

При *цільовій (тематичній) перевірці* перевіряються окремі складові комплексу ТЗІ (комплексної системи захисту інформації) та заходів протидії технічним розвідкам на відповідність упроваджених заходів вимогам нормативно-правових актів та нормативних документів системи ТЗІ.

При *контрольній перевірці* перевіряється повнота та достатність проведених заходів щодо усунення недоліків, які були виявлені в ході проведення попередньої комплексної або цільової перевірки. Контрольні перевірки проводяться за потреби, як правило, після отримання повідомлення про усунення недоліків.

Планові перевірки здійснюються згідно з річним планом контрольно-інспекторської роботи з питань ТЗІ, затвердженим Головою Держспецзв'язку України. Витяги з плану контрольно-інспекторської роботи надсилаються до центральних органів виконавчої влади та в разі потреби до підприємств, установ і організацій.

Позапланові перевірки здійснюються у разі наявності відомостей щодо порушень виконання вимог нормативно-правових актів з питань ТЗІ або з метою визначення повноти та достатності заходів з ТЗІ, вжитих органами, щодо яких здійснюється ТЗІ. Зазначені перевірки можуть проводитися з попередженням або без попередження.

Перевірки стану ТЗІ здійснюються посадовими особами структурного підрозділу адміністрації Держспецзв'язку України з питань державного контролю за станом криптографічного та технічного захисту інформації і регіональних органів Держспецзв'язку України. До перевірок можуть залучатися фахівці інших підрозділів Держспецзв'язку України, а також органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій за погодженням з їх керівниками.

При проведенні перевірки стану ТЗІ контролю підлягають повнота та достатність упроваджених на об'єктах інформаційної діяльності та об'єктах проти-

дії заходів з ТЗІ, їх відповідність вимогам нормативно-правових актів, виконання рекомендацій щодо усунення порушень з ТЗІ.

Напрями розвитку ТЗІ обумовлюються необхідністю своєчасного використання заходів, адекватних масштабам загроз для інформації, і ґрунтуються на засадах правової, соціальної, демократичної держави відповідно до прав суб'єктів інформаційних відносин на доступ до інформації та її захист. Приведення інформаційних відносин у сфері ТЗІ у відповідність із міжнародними стандартами сприятиме утвердженню України у світі як демократичної, соціальної, правової держави. Слід звернути увагу на важливе положення, що має бути покладене в основу формування системи захисту даних при міждержавній співпраці, оскільки гарантувати інформаційний суверенітет України при міжнародному інформаційному обміні без створення ефективної системи технічного захисту інформації практично неможливо.

Контрольні питання

1. Назвіть типи правової охорони комп'ютерних програм.

2. Дайте визначення програмного засобу.

3. У чому полягає доцільність введення Реєстру виробників та розповсюджувачів програмного забезпечення?

4. Які проблеми існують у судовому розгляді справ щодо неправомірного використання комп'ютерних програм?

5. У чому полягає основна мета використання електронного підпису?

6. Визначте поняття електронного підпису.

7. Які обов'язкові дані містить сертифікат відкритого ключа?

8. Поясніть юридичне значення поняття «електронна комерція». Що є основою електронної комерції?

9. Яких вимог необхідно дотримуватися при збереженні електронних документів?

10. Які існують типи засобів криптографічного захисту інформації залежно від способу реалізації?

11. У чому полягають основні напрями державної політики у сфері технічного захисту інформації?

12. Якими властивостями визначається рівень безпеки інформації, що обробляється в системах та на об’єктах інформаційної інфраструктури?

13. У яких випадках проводяться позапланові контрольно-інспекторські перевірки з питань технічного захисту інформації?

14. Назвіть основні завдання органів, щодо яких здійснюється технічний захист інформації.

ЗАКОНОДАВЧЕ, ДЖЕРЕЛОЗНАВЧЕ ТА ІНФОРМАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ

1. ЗАКОНОДАВЧЕ ТА НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ: ЗАКОНИ І НОРМАТИВНО-ПРАВОВІ АКТИ

1. Господарський кодекс України [Електронний ресурс] : станом на 21 січ. 2017 р. – Режим доступу: http://search.ligazakon.ua/

2. Господарський процесуальний кодекс України [Електронний ресурс] : станом на 7 січн. 2018 р. – Режим достпу:http://zakon.rada.gov.ua/laws/show/1798-12.

3. Кодекс законів про працю України [Електронний ресурс] : станом на 20 січн. 2018 р. – Режим доступу: http://search.ligazakon.ua/

4. Кодекс України про адміністративні правопорушення [Електронний рсурс] : станом на 6 лют. 2018 р. – Режим доступу: http://zakon.rada.gov.ua/laws/show/80731-10.

5. Конституція України [Електронний ресурс] : станом на 30 верс. 2016 р. – Режим доступу: http://zakon.rada.gov.ua/laws/show/254к/96-вр.

6. Кримінальний кодекс України [Електронний ресурс] : станом на 12 січн. 2018 р. – Режим доступу: http:// zakon0.rada.gov.ua/laws/show/2341-14

7. Кримінально-процесуальний кодекс України [Електронний ресурс] : станом на 7 січн. 2018 р. – Режим доступу: http:// zakon3.rada.gov.ua/laws/show/4651-17

8. Митний кодекс України [Електронний ресурс] : станом на 3 груд. 2017 р. – Режим доступу: http:// zakon2.rada.gov.ua/laws/show/4495-17

9. Основи законодавства України про охорону здоров’я: закон України від 19 листоп. 1992 р. № 2801-XII // Відомості Верховної Ради України. – 1993. – № 4. – Ст. 19. – Редакція від 30 січн. 2018 р.

10. Про авторське право і суміжні права : закон України від 23 груд. 1993 р. № 3792-XII // Відомості Верховної Ради України. – 1994. – № 13. – Ст. 64. – Редакція від 26 квіт. 2017 р.

11. Про адвокатуру і адвокатську діяльність : закон України від 19 груд. 1992 р. № 2887-XII // Відомості Верховної Ради України. – 1993. – № 9. – Ст. 62. – Редакція від 19 лист. 2012 р.

12. Про банки і банківську діяльність : закон України від 7 груд. 2000 р. № 2121-III // Відомості Верховної Ради України. – 2001. – № 5-6. – Ст. 30. – Редакція від 19 лист. 2012 р.

13. Про державну податкову службу в Україні : закон України від 4 груд. 1990 р. № 509-XII // Відомості Верховної Ради УРСР. – 1991. – № 6. – Ст. 37. – Редакція від 1 січ. 2011 р.

14. Про державну службу : закон України від 10 груд. 2015 р. № 889-VIII // Відомості Верховної Ради України. – 2016. – № 4. – Ст. 43. – Редакція від 19 груд. 2017 р.

15. Про Державну службу спеціального зв'язку та захисту інформації України : закон України від 23 лют. 2006 р. № 3475-IV // Відомості Верховної Ради України. – 2006. – № 30. – Ст. 258. – Редакція від 13 жовт. 2010 р.

16. Про державну статистику : закон України від 17 верес. 1992 р. № 2614-XII // Відомості Верховної Ради України. – 1992. – № 43. – Ст. 608. – Редакція від 19 трав. 2014 р.

17. Про державну таємницю : закон України від 21 січ. 1994 р. № 3855-XII // Відомості Верховної Ради України. – 1994. – № 16. – Ст. 93. – Редакція від 5 січн. 2017 р.

18. Про деякі питання передачі державної таємниці іноземній державі чи міжнародній організації : указ Президента України від 14 груд. 2004 р. № 1483/2004 //Офіційний вісник України. – 2004. – № 50. – Ст. 3264.

19. Про Дисциплінарний статут митної служби України : закон України від 6 верес. 2005 р. № 2805-IV // Відомості Верховної Ради України. – 2005. – № 42. – Ст. 467. Редакція станом на 11.08.2013 р.

20. Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади [Електронний ресурс] : указ Президента України від 1 серп. 2002 р. № 683/2002. – Режим доступу: http://zakon.rada.gov.ua/laws/

show/683/2002.

21. Про доступ до публічної інформації [Електронний ресурс] : закон України від 1 травн. 2015 р. № 2939-VI . – Редакція від 9 квіт. 2015 р.

22. Про доступ до судових рішень : закон України від 22 груд. 2005 р. № 3262-IV // Відомості Верховної Ради України. – 2006. – № 15. – Ст. 128. – Редакція від15 груд. 2017 р.

23. Про електронний цифровий підпис : закон України від 22 трав. 2003 р. № 852-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 276. – Редакція від 2 лист. 2016 р.

24. Про електронні документи та електронний документообіг : закон України від 22 трав. 2003 р. № 851-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 275. – Редакція від 30 верес. 2015 р.

25. Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які службову інформацію[Електронний ресурс] : постанова Кабінету Міністрів України від 29 лист. 2001 р. № 1893. – Режим доступу: http:// zakon3.rada.gov.ua /laws/show/1893-98-п. – Редакція від 4 лист. 2016 р.

26. Про затвердження Положення про Державну службу інтелектуальної власності України [Електронний ресурс] : указ Президента України від 18 трав. 2017 р. № 436/2011. – Режим доступу: http:// www.president.gov.ua /documents/13415.html.

27. Про затвердження Положення про державний контроль за станом технічного захисту інформації [Електронний ресурс] : наказ Адміністрації Держ. служби спеціал. зв'язку та захисту інформації України від 16 трав. 2007 р. № 87. – Режим доступу: http:// zakon.rada.gov.ua/laws/show/z0785-07. – Редакція від 10 берез. 2015 р.

28. Про затвердження Положення про Реєстр виробників та розповсюджувачів програмного забезпечення [Електронний ресурс] : наказ М-ва освіти і науки, молоді та спорту України від 22 берез. 2012 р. № 332. – Режим доступу: http:// search.ligazakon.ua/l_doc2.nsf/link1/RE20871.html

29. Про затвердження Загальних правил поведінки державного службовця[Електронний ресурс] : наказ Голов. упр. держ. служби України від 27 верес. 2016 р. № 214. – Режим доступу: http://search.ligazakon.ua/ l_doc2.nsf /link1/RE20871.html. – Редакція від 22груд. 2017 р.

30. Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади [Електронний ресурс] : постанова Кабінету Міністрів України від 10 верес. 2003 р. № 1433. – Режим доступу: http://zakon.rada.gov.ua/ laws/show/1433-2003-п. – Редакція від 22 груд. 2017 р.

31. Про захист від недобросовісної конкуренції : закон України від 7 черв. 1996 р. № 236/96-ВР // Відомості Верховної Ради України. – 1996. – № 36. – Ст. 164. – Редакція від 3 берез. 2016 р.

32. Про захист економічної конкуренції : закон України від 11 січ. 2001 р. № 2210-III // Відомості Верховної Ради України. – 2001. – № 12. – Ст. 64. – Редакція від 9 лист. 2017 р.

33. Про захист інформації в інформаційно-телекомунікаційних системах: закон України від 5 лип. 1994 р. № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286. – Редакція від 19.04.2014 р.

34. Про захист персональних даних: закон України від 1 черв. 2010 р. № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481. – Редакція від 9 лист. 2017 р.

35. Про заходи щодо охорони інтелектуальної власності в Україні [Електронний ресурс] : указ Президента України від 27 квіт. 2001 р. № 285/2001. – Режим доступу: http://zakon.rada.gov.ua/laws/show/285/2001.

36. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні [Електронний ресурс] : указ Президента України від 31 лип. 2000 р. № 928/2000. – Режим доступу: http://zakon.rada.gov.ua/laws/show/928/2000.

37. Про зовнішньоекономічну діяльність: закон України від 16 квіт. 1991 р. № 959-XII // Відомості Верховної Ради УРСР. – 1991. – № 29. – Ст. 377. – Редакція від 03.01.2017 р.

38. Про інформацію : закон України від 2 жовт. 1992 р. № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650. – Редакція від 01.01.2017

39. Про Концепцію Національної програми інформатизації : закон України від 4 лют. 1998 р. № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28. – Ст. 182. – Редакція від від 11.08.2013 р.

40. Про ліцензування певних видів господарської діяльності : закон України від 1 черв. 2000 р. № 1775-III // Відомості Верховної Ради України. – 2000. – № 36. – Ст. 299. – Редакція від 17 листоп. 2010 р. Втрата чинності від 28.06.2015

41. Про міжнародні договори України : закон України від 29 черв. 2004 р. № 1906-IV // Відомості Верховної Ради України. – 2004. – № 50. – Ст. 540. – Редакція станом на 20.07.2014 р.

42. Про поліцію : закон України від 20 груд. 1990 р. № 565-XII // Відомості Верховної Ради УРСР. – 1991. – № 4. – Ст. 20. – Редакція від 06.02.2018 р.

43. Про науково-технічну інформацію : закон України від 25 черв. 1993 р. № 3322-XII // Відомості Верховної Ради України. – 1993. – № 33. – Ст. 345. – Редакція від 19.04.2014 р.

44. Про Національний банк України : закон України від 20 трав. 1999 р. № 679-XIV // Відомості Верховної Ради України. – 1999. – № 29. – Ст. 238. – Редакція станом на 06.01.2018 р.

45. Про Національну програму інформатизації України : закон України від 4 лют. 1998 р. № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28. – Ст. 181. – Редакція від 01.08.2016 р.

46. Про Національну систему конфіденційного зв’язку : закон України від 10 січ. 2002 р. № 2919-III // Відомості Верховної Ради України. – 2002. – № 15. – Ст. 103. – Редакція від 19.04.2014 р.

47. Про нотаріат : закон України від 2 верес. 1993 р. № 3425-XII // Відомості Верховної Ради України. – 1993. – № 39. – Ст. 383. – Редакція від 11.10.2017 р.

48. Про обов'язковий примірник документів : закон України від 9 квіт. 1999 р. № 595-XIV // Відомості Верховної Ради України. – 1999. – № 22–23. – Ст. 199. – Редакція від 13.01.2016 р.

49. Про оперативно-розшукову діяльність : закон України від 18 лют. 1992 р. № 2135-XII // Відомості Верховної Ради України. – 1992. – № 22. – Ст. 303. Редакція від 12.04.2017 р.

50. Про основи національної безпеки України : закон України від 19 черв. 2003 р. № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351. – Редакція від 30.11.2017 р.

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

52. Про платіжні системи та переказ коштів в Україні : закон України від 5 квіт. 2001 р. № 2346-III // Відомості Верховної Ради України. – 2001. – № 29. – Ст. 137. – Редакція від 04.06.2017 р.

53. Про Положення про технічний захист інформації в Україні [Електронний ресурс] : указ Президента України від 27 верес. 1999 р. № 1229/99. – Режим доступу: http://zakon.rada.gov.ua/laws/show/1229/99. – Редакція від 4 трав. 2008 р.

54. Про приєднання України до Бернської конвенції про охорону літературних і художніх творів (Паризького акта від 24 липня 1971 року, зміненого 2 жовтня 1979 року) : закон України від 31 трав. 1995 р. № 189/95-ВР // Відомості Верховної Ради України. – 1995. – № 21. – Ст. 155. – Редакція від 16 серп. 2001 р.

55. Про приєднання України до Договору Всесвітньої організації інтелектуальної власності про авторське право : закон України від 20 верес. 2001 р. № 2733-III // Відомості Верховної Ради України. – 2002. – № 2. – Ст. 16.

56. Про прокуратуру : закон України від 5 листоп. 1991 р. № 1789-XII // Відомості Верховної Ради України. – 1991. – № 53. – Ст. 793. – Редакція від 20.01.2018 р.

57. Про психіатричну допомогу : закон України від 22 лют. 2000 р. № 1489-III // Відомості Верховної Ради України. – 2000. – № 19. – Ст. 143. – Редакція від 20.01.2018 р.

58. Про Службу безпеки України : закон України від 25 берез. 1992 р. № 2229-XII // Відомості Верховної Ради України. – 1992. – № 27. – Ст. 382. – Редакція від 28.12.2015 р.

59. Про службу в органах місцевого самоврядування: закон України від 7 черв. 2001 р. № 2493-III // Відомості Верховної Ради України. – 2001. – № 33. – Ст. 175. – Редакція від 11.10.2017 р.

60. Про Стратегію національної безпеки України [Електронний ресурс] : указ Президента України від 12 лют. 2007 р. № 105/2007. – Режим доступу: http://zakon.rada.gov.ua/laws/show/105/2007. – Стратегія в редакції указу Президента України Редакція станом на 29.05.2015 р.

61. Про телекомунікації : закон України від 18 листоп. 2003 р. № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155. – Редакція від 18.12.2017 р.

62. Цивільний кодекс України [Електронний ресурс] : станом 7 берез. 2018 р. – Режим доступу: http:// zakon4.rada.gov.ua/laws/show/435-15.

63. Цивільний процесуальний кодекс України [Електронний ресурс] : станом на 24 лют. 2018 р. – Режим доступу: http:// zakon.rada.gov.ua/laws/show/1618-15

2. Джерелознавче та інформаційно-бібліографічне забезпечення: навчально-методична і наукова література

2.1. Основна рекомендована література

1. Антонюк А. О. Основи захисту інформації в автоматизованих системах : навч. посіб. / А. О. Антонюк. – К. : Академія, 2003. – 242 с.

2. Архипов О. Є. Оцінювання ефективності системи охорони державної таємниці : монографія / О. Є. Архипов, І. Т. Бородавко, В. П. Ворожко. – К. : Наук.-вид. відділ НА СБ України, 2007. – 63 с.

3. Афанасьев В. Г. Социальная информация / В. Г. Афанасьев. – М. : Наука, 1994. – 200 с.

4. Афанасьев В. Г. Социальная информация и управление обществом / В. Г. Афанасьев. – М. : Политиздат, 1975. – 408 с.

5. Баранов А. А. Права человека и защита персональных данных / А. А. Баранов, В. М. Брыжко, Ю. К. Базанов. – Киев : Гос. комитет связи и информатизации Украины, 2000. – 280 с.

6. Батурин Ю. М. Право и политика в компьютерном круге / Ю. М. Батурин. – М. : Наука, 1987. – 110 с.

7. Бачило И. Л. Информационное право: основы практической информатики : учеб. пособие / И. Л. Бачило. – М. : Изд. г-на Тихомирова М. Ю., 2001. – 352 с.

8. Беляков К. И. Управление и право в период информатизации : монография / К. И. Беляков. – К. : КВІЦ, 2001. – 308 с.

9. Богуш В. М. Інформаційна безпека держави : навч. посіб. / В. М. Богуш, О. К. Юдін. – К. : МК-Прес, 2005. – 432 с.

10. Ботвінкін О. В. Історія охорони державної таємниці в Україні : монографія / О. В. Ботвінкін, В. М. Шлапаченко, В. П. Ворожко, А. С. Пашков. – К. : Наук.-вид. відділ НА СБ України, 2008. – 155 с.

11. Брижко В. М. Правовий механізм захисту персональних даних : монографія / В. М. Брижко ; за ред. М. Я. Щвеця, Р. А. Калюжного. – К. : Парлам. вид-во, 2003. – 120 с.

12. Венгеров А. Б. Право и информация в условиях автоматизации управления (теоретические вопросы) / А. Б. Венгеров. – М. : Юрид. лит., 1978. – 208 с.

13. Вернадский В. И. Размышления натуралиста. Кн. 2. Научная мысль как планетное явление / В. И. Вернадский. – М. : Наука, 1977. – 192 с.

14. Винер Н. Кибернетика и общество / Н. Винер. – М. : Сов. радио, 1958. – 200 с.

15. Вступ до інформаційної культури та інформаційного права : монографія / [В. М. Брижко, В. Д. Гавловський, Р. А. Калюжний та ін.]; за ред. М. Я. Щвеця, Р. А. Калюжного. – Ужгород : ІВА, 2003. – 240 с.

16. Гаврилов О. А. Курс правовой информатики : учеб. для вузов / О. А. Гаврилов. – М. : НОРМА; ИНФРА-М, 2000. – 419 с.

17. Готт В. С. Категории современной науки: становление и развитие / В. С. Готт, Э. П. Семенюк, А. Д. Урсул. – М. : Мысль, 1984. – 268 с.

18. Державне управління: проблеми адміністративно-правової теорії та практики / за ред. В. Б. Авер'янова. – К. : Факт, 2003. – 384 с.

19. Домарев В. В. Защита информации и безопасность компьютерных систем / В. В. Домарев. – Киев : DiaSoft, 1999. – 453 с.

20. Завгородний В. И. Комплексная защита информации в компьютерных системах : учеб. пособие / В. И. Завгородний. – М. : Логос ; ПБОЮЛ Н. А. Егоров, 2001. – 264 с.

21. Збірка документів Ради Європи. Офіційне видання. – К. : Парлам. вид-во, 2000. – 654 с.

22. Компьютерные технологии в юридической деятельности : учеб. и практ. пособие / под ред. Н. Полевого, В. Крылова. – М. : БЕК, 1994. – 306 с.

23. Копылов В. А. Информационное право : учебник / В. А. Копылов. – 2-е изд., перераб. и доп. – М. : Юристъ, 2002. – 512 с.

24. Кормич Б. А. Інформаційна безпека : навч. посіб. / Б. А. Кормич. – К. : Кондор, 2004. – 384 с.

25. Машуков В. Компьютерное право : практ. руководство / В. Машуков. – Львов : Аверс, 1998. – 256 с.

26. Международное право : ученик / отв. ред. Ю. М. Колосов, В. И. Кузнецов. – М. : Междунар. отношения, 1996. – 608 с.

27. Международные акты по правам человека : сб. док. – М. : НОРМА ; ИНФРА-М, 2000 (1999). – 784 с.

28. Новик И. Б. Введение в информационный мир : монография / И. Б. Новик, А. Ш. Абдулаев. – М. : Наука, 1991. – 228 с.

29. Осуга С. Обработка знаний : пер. с яп. / С. Осуга. – М. : Мир, 1989. – 293 с.

30. Офіційний переклад нормативних актів Євросоюзу в сфері інформаційно-комунікаційних технологій / Громадська організація «Інтерньюз-Україна». – К., 2002. – 219 с.

31. Пилипчук В. Г. Система і компетенція державних органів зі спеціальним статусом у сфері національної безпеки України : монографія / В. Г. Пилипчук, О. П. Дзьобань, В. Я. Настюк. – Х. : Право, 2009. – 200 с.

32. Полевой Н. С. Правовая информатика и кибернетика / Н. С. Полевой. – М. : Юрид. лит., 1993. – 527 с.

33. Права людини і професійні стандарти для юристів у документах міжнародних організацій / упоряд. Т. Яблонської. – К. : Сфера, 1999. – 342 с.

34. Правовое обеспечение информационной безопасности : учебник / В. А. Минаев, А. П. Фисун, С. В. Скрыль, С. В. Дворянкин. – М. : Маросейка, 2008. – 368 с.

35. Основи правової охорони інтелектуальної власності в Україні : підруч. для студ. юрид. вузів / [В. С. Дроб'язко, О. М. Мельник, П. П. Крайнєв, Д. М. Притика] ; за заг. ред. О. А. Підопригори, О. Д. Святоцького. – К. : Ін-Юре, 2003. – 236 с.

36. Представление и использование знаний / под ред. Х. Уєно, М. Исидзука. – М. : Мир, 1989. – 220 с.

37. Приобретение знаний / под ред. С. Осуги, Ю. Саэки. – М. : Мир, 1990. – 304 с.

38. Прієшкіна О. В. Місцеве самоврядування: правове регулювання безпосередньої демократії : навч. посіб. / О. В. Прієшкіна. – К. : Кондор, 2004. – 135 с.

39. Ровенский В. Машина и мысль. Философский очерк об информатике / В. Ровенский, А. Уемов, Е. Уемова. – М. : Госполотиздат, 1960. – 126 с.

40. Сиверс В. А. Измерение ценности / В. А. Сиверс. – Калининград : Свободная зона, 1996. – 128 с.

41. Смирнов В. И. Философия / В. И. Смирнов, В. Ф. Титов. – 2-е изд., испр. и доп. – М. : [Б. и.], 1998. – 286 с.

42. Советский энциклопедический словарь / науч.-ред. совет: А. М. Прохоров (пред.). – М. : Сов. энцикл., 1981. – 1600 с.

43. Степанов Е. А. Информационная безопасность и защита информации : учеб. пособие / Е. А. Степанов, И. К. Корнеев. – М. : ИНФРА-М, 2001. – 304 с.

44. Столяров В. И. Диалектика как логика и методология науки / В. И. Столяров. – М. : Политиздат, 1975. – 247 с.

45. Судова практика Верховного Суду України у справах про адміністративні правопорушення / за ред. П. П. Пилипчука. – К. : Ін-Юре, 2007. – 328 с.

46. Урсул А. Д. Проблема информации в современной науке / А. Д. Урсул. – М. : Наука, 1975. – 287 с.

47. Философский словарь / под ред. И. Т. Фролова. – 6-е изд., перераб. и доп. – М. : Политиздат, 1991. – 560 с.

48. Шевчук В. П. Історія української державності. Курс лекцій : навч. посіб. / В. П. Шевчук, М. Г. Тараненко. – К. : Либідь, 1999. – 342 с.

49. Щвець М. Я. Інформаційна культура : навч. посіб. / М. Я. Щвець, Р. А. Калюжний. – Ірпінь : Нац. ун-т ДПС України, 2007. – 254 с.

50. Эшби У. Р. Введение в кибернетику / У. Р. Эшби. – М. : Изд-во иностр. лит., 1959. – 516 с.

2.2. Додаткова рекомендована література

1. Биленчук П. Д. Знание – информация, организованная для конкретной цели / П. Д. Биленчук, Л. В. Борисова, А. А. Борисов // Сб. науч. трудов Нац. аэрокосмич. ун-та им. Н. Е. Жуковского «ХАИ». Открытые информационные технологии. – 2002. – Вып. 14. – С. 161–173.

2. Блюменау Д. И. Информация: миф или реальность? (О состоянии понятий «знание» и «социальная информация») / Д. И. Блюменау // НТИ. Сер. 2. – 1985. – № 2. – С. 1–4.

3. Вус М. А. Аттестация специалистов по безопасности в США / М. А. Вус // Защита информации. Конфидент. – 1994. – № 2. – С. 9–10.

4. Гавловський В. Д. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект) / В. Д. Гавловський // Правове, нормативне та метрологічне забезпечення систем захисту інформації в автоматизованих системах України. – К. : ЕКМР, 2000. – С. 50–53.

5. Дмитришин В. Легалізація та ефективне використання програмного забезпечення в Україні / В. Дмитришин // Інтелектуальна власність. – 2002. – № 10. – С. 16–19.

6. Дорохов В. Я. Понятие документа в советском праве / В. Я. Дорохов // Известия высш. учеб. завед. Сер. Правоведение. – 1982. – № 2. – С. 53–60.

7. Ершов А. П. Информация: от информационной грамотности учащихся к информационной культуре общества / А. П. Ершов // Коммунист. – 1988. – № 2. – С. 82–92.

8. Зегжда П. Д. Теория и практика обеспечения информационной безопасности / П. Д. Зегжда. – М. : Яхтсмен, 1996. – 192 с.

9. Іщенко В. Поняття документа як джерела доказів у кримінальному судочинстві / В. Іщенко // Право України. – 1997. – № 2. – С. 42–44.

10. Карась И. З. Вопросы правового обеспечения информатики / И. З. Карась // Микропроцессорные средства и системы. – 1986. – № 1. – С. 3–9.

11. Карась И. З. Экономический и правовой режим информационных ресурсов / И. З. Карась. – К. : ИК, 1988. – 22 с.

12. Копылов В. А. Информация и собственность / В. А. Копылов // Информационные ресурсы России. – 1996. – № 3. – С. 10–12.

13. Копылов В. А. Информация как объект правового регулирования / В. А. Копылов // Научно-техническая информация. Сер. 1. Организация и методика информац. работы. –1996. – № 8. – С. 1–17.

14. Ландик В. Доцільність і можливості охорони комп'ютерних програм нормами патентного права / В. Ландик // Інтелектуальна власність. – 2002. – № 9. – С. 12–16.

15. Литвинов А. В. Правовые вопросы охраны компьютерной информации / А. В. Литвинов // Сов. государство и право. – 1987. – № 8. – С. 84–88.

16. Ляш А. О. Недопустимість розголошення даних досудового слідства або дізнання / А. О. Ляш // Актуальні питання реформування правової системи України: Збірник наукових статей за матеріалами VI Міжнародної науково-практичної конференції, м. Луцьк, 29-30 травня 2009 р. / Уклад. Т. Д. Климчук. – Луцьк: Волинська обласна друкарня, 2009.– С. 579-581.

17. Макаренко В. В. Повноваження органів державної влади, які провадять діяльність, пов'язану з державною таємницею / В. В. Макаренко, І. П. Касперський // Зб. наук. праць НА СБ України. – 2003. – № 8. – С. 50–56.

18. Макаренко ЄА. Інформаційна політика Європейського Союзу. – К: 2000. – 288 с.

19. Международное право : учеб. пособие для вузов / Г. В. Игнатенко, В. Я. Суворова, И. О. Туинов [и др.] ; под ред. Г. В. Игнатенко. – 2-е изд., перераб. и доп. – М. : Высш. шк., 1995. – 399 с.

20. Наука и политика: место встречи – Будапешт // Наука и жизнь. – 2004. – № 1. – С. 5–12, 106–107.

21. Новицький Г. В. Теоретико-правові основи забезпечення національної безпеки України : монографія / Г. В. Новицький ; Ін-т проблем нац. безпеки ; НА СБ України. – К. : Інтертехнологія, 2008. – 496 с.

22. Нюттен Ж. Мотивация / Жозеф Нюттен // Экспериментальная психология : пер. с фр. / ред.-сост. П. Фресс, Ж. Пиаже. – Вып. 5. – М. : Прогресс, 1975. – С. 15–110.

23. Паскуаль К. Заочний круглий стіл / К. Паскуаль // Національна безпека і оборона. – 2001. – № 10. – С. 53.

24. Пашков А. С. Основні елементи системи охорони державної таємниці / А. С. Пашков //Зб. наук. праць НА СБ України. – 2003. – № 8. – С. 15–20.

25. Першиков В. И. Толковый словарь по информатике / В. И. Першиков, В. М. Савинов. – 2-е изд., доп. – М. : Финансы и статистика, 1991. – 536 с.

26. Петренко С. Правовий захист програмного забезпечення / С. Петренко // Право України. – 2003. – № 6. – С. 62–65.

27. Семенюк Э. П. Глобализация и социальная роль информации / Э. П. Семенюк // НТИ. Сер. 1. – 2003. – № 1. – С. 1–10.

28. Семенюк Э. П. Развитие информационного пространства и прогресс общества / Э. П. Семенюк // НТИ. Сер. 1. – 1997. – № 2. – С. 1–12.

29. Стенг Д. Секреты безопасности сетей / Д. Стенг, С. Мун. – Киев : Диалектика, 1995. – 544 с.

30. Туском Ж. Міжнародне право : підручник : пер. з фр. / Жан Туском. – К. : АртЕк, 1998. – 416 с.

31. Урсул А. Д. Природа безопасности / А. Д. Урсул // Безопасность информации. – 1997. – № 2. – С. 1–12.

32. Цветков В. Я. Технологии и системы информационной безопасности : аналит. обзор / В. Я. Цветков. – М. : ВНТИЦ, 2001. – 88 с.

33. Черемных Г. Г. Развитие нотариата как системы органов превентивного правосудия: единство и различие с судебными органами / Г. Г. Черемных // Нотариальный вестник. – 1998. – № 12. – С. 40–43.

34. Черных А. В. Обеспечение безопасности автоматизированных информационных систем (уголовно-правовые аспекты) / А. В. Черных // Сов. государство и право. – 1990. – № 6. – С. 116–120.

Додаток А

Основні документи, які діють у сфері правового регулювання інформаційних технологій

Міжнародне публічне і міжнародне приватне право

1. Держави «Великої вісімки»:

Окінавська Хартія Глобального інформаційного суспільства від 22 липня 2000 р.;

2. Комісія ООН по праву міжнародної торгівлі (ЮНСІТРАЛ):

– типовий закон «Про електронну комерцію»1996 р. (з додатковою статтею 5 bis, що прийнята у 1998 р.);

– типовий закон «Про електронні підписи» 2001 р.;

– правове управління по електронному переказу коштів 1987 р.;

– рекомендації про правову цінність комп'ютерних записів 1985 р.;

3. Рада Європи:

– Конвенція»Про захист фізичних осіб у відношенні автоматичної обробки персональних даних» від 28 січня 1981 р. (Страсбург);

– додатковий протокол до Конвенції про захист фізичних осіб у відношенні автоматичної обробки персональних даних, що стосуються наглядових органів і трансграничних потоків даних від 8 листопада 2001 р. (Страсбург);

– Конвенція про інформаційне і правове співробітництво, що стосується «послуг інформаційного суспільства» від 4 жовтня 2001 р;

– Конвенція Ради Європи з кіберзлочинності від 23 грудня 2001 р.

4. Всесвітня організація інтелектуальної власності:

– Угода про авторське право від 20 грудня 1996 р.;

– Угода про виконання і фонограмах від 20 грудня 1996 р.

5. Всесвітня торгова організація:

– Генеральна угода про торгівлю послугами від 15 квітня 1994 р. (додаток по телекомунікаціям);

– Угода по торгівельним аспектам прав інтелектуальної власності 1994 р.

6. Міжнародна торгівельна палата:

– Загальні звичаї для посвідчення цифровим способом міжнародної комерції 1997 р.;

– Загальні принципи реклами і маркетингу в Інтернет 1998 р.;

– Уніфіковані правила поведінки при обміні торгівельними даними шляхом телетрансмісії (UN-CID) 1987 р.

7. Міжнародний морський комітет:

– Правила для електронних коносаментів від 29 червня 1990 р.

8. Організація економічного співробітництва і розвитку (ОЕСР):

– Загальні принципи захисту прав споживачів у контексті електронної комерції 2000 р.

9. Європейська економічна комісія ООН:

– Типова угода обміну при міжнародному комерційному використанні електронного обміну даними (Додаток до Рекомендації № 26 „Комерційне використання угод обміну даними" прийнятій Робочою групою по сприянню міжнародним торговим процедурам Європейської економічної комісії ООН від 23 червня 1995 р.

10. Центр ООН по сприянню торгівлі та електронному бізнесу:

– Угода про електронну комерцію (Рекомендація № 31, прийнятій Центром ООН по сприянню торгівлі та електронному бізнесу (UN/CEFACT), березень 2000 р., Женева.

II. Європейське право

1. Регламенти:

– Регламент № 733/2002 Європейського парламенту і Ради від 22 квітня 2002 р. про введення домену верхнього рівня «. eu»;

– Директива 95/46/ ЄС Європейського парламенту і Ради від 24 жовтня 1995 р. про захист фізичних осіб у відношенні обробки персональних даних і вільному руху таких даних;

– Директива 97/5/ЄС Європейського парламенту і Ради від 27 січня 1997 р. про трансграничні кредитні перекази;

– Директива 97/7/ЄС Європейського парламенту і Ради від 20 травня 1997 р. про захист споживачів у відношенні дистанційних угод (дистанційний продаж);

– Директива 97/66/ЄС Європейського парламенту і Ради від 15 грудня 1997 р. стосовно обробки персональних даних і охорони таємниці приватного життя в телекомунікаційному секторі;

– Директива 1999/93/ЄС Європейського парламенту і Ради від 13 грудня 1999 р. про правові основи Співтовариства для електронних підписів;

– Директива 2000/31/ЄС Європейського парламенту і Ради від 8 червня 2000 р. про деякі правові аспекти послуг інформаційного суспільства, в тому числі електронної комерції на внутрішньому ринку (Директива про електронну комерцію);

– Директива 2000/46/ЄС Європейського парламенту і Ради від 18 серпня 2000 р. про заняття, здійснення і нагляду за підприємницькою діяльністю в сфері електронних грошей;

– Директива 2001/29/ЄС Європейського парламенту і Ради від 22 травня 2001 р. про гармонізацію деяких аспектів авторського та суміжних прав у інформацій інформаційному суспільстві;

– Директива 2002/58/ЄС Європейського парламенту і Ради від 12 липня 2002 р. стосовно обробки персональних даних і охороні таємниці приватного життя в секторі електронних комунікацій.

2. Рекомендації:

– Рекомендація Комісії № 94/820/ЄС від 19 жовтня 1994 р. стосовно правових аспектів електронного обміну даними;

– Рекомендація Комісії № 97/489/ЄС від 30 липня 1997 р. стосовно угод, укладених з використанням електронних кошторисних інструментів і, загалом, відношень між емітентом і утримувачем.

III. Право СНД

1. Угода про співробітництво держав-учасниць Співтовариства Незалежних Держав у боротьбі зі злочинами в сфері комп'ютерної інформації від 1 червня 2001 р.;

2. Модельний закон «Про електронний цифровий підпис» від 9 грудня 2000 р.

VI. Право держав СНД

1. Азербайджан

– Закон Азербайджанської республіки від 3 квітня 1998 р. № 460-IQ «Про інформації, інформатизації і захист інформації».

2. Вірменія

– Закон Республіки Арсенія від 7 січня 1997 р. № ЗР-100 «Про переказ коштів по кошторисному дорученню».

3. Білорусь

– Закон Республіки Білорусь від 10 січня 2000 р. № 357-З «Про електронний документ»;

– Банківський кодекс Республіки Білорусь від 25 жовтня 2000 р. № 441-3;

– Закон Республіки Білорусь від 16 травня 1996 р. № 370-XIII «Про авторське право і суміжних правах».

4. Казахстан

– Закон від 29 червня 1998 р. № 237-1 ЗКР «Про платежі і перекази коштів».

5. Киргизстан

– Закон Киргизької Республіки від 6 листопада 1999 р. № 121 «Про електронні платежі»;

– Закон Киргизької Республіки від 8 жовтня 1999 р. № 107 «Про інформацію»;

– Закон Киргизької Республіки від 30 березня 1998 р. № 28 «Про правову охорону програм для електронних обчислювальних машин і баз даних».

6. Росія

– Федеральний закон від 20 лютого 1995 р. № 24-ФЗ «Про інформацію, інформатизацію і захист інформації»;

– Федеральний закон від 4 червня 1996 р. № 85-ФЗ «Про участь у міжнародному інформаційному обміні»;

– Федеральний закон від 10 січня 2002 р. № 1-ФЗ «Про електронний цифровий підпис»;

– Федеральний закон від 23 вересня 1992 р. № 3523-I «Про правову охорону програм для електронних обчислювальних машин і баз даних».

7. Таджикистан

– Закон Республіки Таджикистан від 10 травня 2002 р. «Про електронний документ».

8. Туркменистан

– Закон Туркменистану від 19 грудня 2000 р. «Про електронний документ».

9. Узбекистан

– Закон Республіки Узбекистан від 7 травня 1993 р. «Про інформатизацію»;

– Закон Республіки Узбекистан від 6 травня 1994 р. № 1060-XII «Про правову охорону програм для електронно-обчислювальних машин і баз даних».

10. Україна

– Закон України від 4 квітня 2001 р. № 2346-III «Про кошторисні системи і переказ грошей в Україні»;

– Закон України від 10 грудня 1997 р. № 710/97-ВР «Про національну депозитарній системі та особливостях електронного оберту цінних паперів в Україні»;

– Закон України від 5 червня 1994 р. № 80-94-ВР «Про захист інформації в автоматизованих системах»;

– Закон України від 2 жовтня 1992 р. № 2657-XII «Про інформацію».

V. Право зарубіжних країн

1. Австралія

– Закон, прийнятий, щоб сприяти електронним угодам і в інших цілях № 62 від 10 грудня 1999 р. «Про електронні угоди».

2. Австрія

– Федеральний закон від 19 серпня 1999 р. «Про електронних підписи» (Закон про підпис – SigG).

3. Бельгія

– Закон від 20 жовтня 2000 р. «Про введення телекомунікаційних засобів і електронного підпису в судові та позасудові процедури».

4. Болгарія

– Закон від 7 жовтня 2001 р. № 15 «Про електронний документ і електронний підпис».

5. Велика Британія

– Закон від 25 травня 2000 р. № 1798 «Про електронні комунікації».

6. Гонконг (спеціальний адміністративний район Китаю)

– Ордонанс 3 553 від 2000 р. «Про електронні угоди».

7. Данія

– Закон від 31 травня 2000 р. № 417 «Про електронні підписи»;

– Закон від 31 травня 2000 р. № 414 «Про деякі платіжні інструменти».

8. Індія

– Закон від 9 червня 2000 р. № 21 «Про інформаційні технології».

9. Ірландія

– Закон від 10 червня 2000 р. № 27 „Про електронну комерцію”.

10. Канада

– Закон від 13 квітня 2000 р. «Про захист персональної інформації та електронних документах»;

– Закон Канади від 13 квітня 2000 р. «Про докази» із змінами, внесеними Законом «Про захист персональної інформації та електронних документах».

11. Корея

– Закон від 5 лютого 1999 р. № 5792 «Про цифровий підпис».

12. Литва

– Закон Литовської Республіки від 11 червня 2000 р. № VIII-1822 «Про електронний підпис»;

– Закон Литовської Республіки від 18 травня 1999 р. № VIII-1185 «Про авторські та суміжні права».

13. Люксембург

– Закон від 14 серпня 2000 р. № 96 про електронну, змінюючи Цивільний кодекс, Новий цивільний процесуальний кодекс, Торговий кодекс, Кримінальний кодекс та імплементируючий Директиву 1999/93 про правові основи Співтовариств для електронних підписів, Директиву про деякі правові аспекти послуг інформаційного суспільства, деякі положення Директиви 97/7/ СЄЄ про дистанційний продаж товарів і інших послуг, ніж фінансові послуги.

14. Малайзія

– Закон від 26 березня 1997 р. «Про цифровий підпис».

15. Сінгапур

– Закон від 10 червня 1998 р. «Про електронні угоди».

16. США (федеральне законодавство)

– Закон від 30 червня 2000 р. «Про електронні підписи в глобальній і національній комерції»;

– Закон від 21 жовтня 1998 р. «Про виключення урядового паперообігу»;

– Закон від 10 листопада 1978 р. «Про електронний переказ грошей» (із змінами 1982, 1989,1991 ,1996 и 1999 р.р.);

– Закон від 11 лютого 2000 р. «Про операційну взаємодію і мобільність електронного переказу виплат»;

– Закон від 28 жовтня 1998 р. «Про авторське право в цифровому тисячолітті»;

– Закон від 29 грудня 1999 р. «Про захист прав споживачів проти захоплень у кіберпросторі».

17. США (законодавство штатів)

– Закон штату Юта від 9 березня 1995 р. «Про цифровий підпис»;

– Однаковий закон штату Юта від 3 липня 2000 р. «Про електронні угоди»;

– Однаковий Закон штату Вірджинія від 14 березня 2000 р. «Про угоди з комп'ютерною інформацією».

18. Туніс

– Закон від 9 серпня 2000 р. № 2000-83 «Стосовно електронного обміну і електронної комерції».

19. Філіппіни

– Закон від 14 червня 2000 р. № 8792 «Про електронну комерцію».

20. Франція

– Закон від 13 березня 2000 р. № 2000-230 «Про надання доказової сили інформаційним технологіям і про електронний підпис».

21. ФРН

– Закон від 16 травня 2001 р. «Про рамочні умови для електронних підписів і зміни інших правових актів».

22. Швеція

– Закон від 2000 р. № 832 «Про кваліфікованих електронних підписах».

23. Естонія

– Закон Естонської Республіки від 8 березня 2000 р. «Про цифровий підпис».

24. Японія

– Основний закон від 24 листопада 2000 р. «Про формування суспільства перспективних інформаційних і телекомунікаційних мереж»;

– Закон від 24 травня 2000 р. «Про електронні підписи і сертифікаційні послуги».

Додаток В

Законодавче регулювання інституту банківської таємниці з позиції інформаційних відносин матеріалами «Taurus group» Risk Management

(Taurus group. Taurus Ltd. 2015.)

Австрія	Закон «Про банківську діяльність» регулює встановлення банківської таємниці: кредитні інститути, їх власники, члени правління, працівники банків та інші особи, що діють від імені банків, не повинні розкривати або використовувати секрети, які стали їм відомі або доступні виключно внаслідок їх ділових відносин з клієнтами та в процесі виконання офіційних функцій. Обов'язок зберігати отриману конфіденційну інформацію в таємниці не має обмежень за часом. Закон передбачає незначну кількість винятків, коли така інформація може бути розкрита.
Бельгія	Банківська таємниця визначена як професійна таємниця, порушення якої передбачає тільки цивільно-правове покарання. Бельгійське законодавство встановлює окремі гарантії нерозголошення банківської інформації третім особам (зокрема податковим органам), які нівелюються винятками, встановленими окремими законами.
Греція	Законодавчий декрет 1059/1971 встановлює, що «будь-які види депозитів в кредитних інститутах містяться в таємниці». Банки не повинні розкривати третім особам деталі і характер своїх відносин з клієнтами, включаючи угоди. За порушення положень про банківську таємницю передбачене кримінальне покарання. Однак істотні винятки дозволяють отримати доступ до банківської інформації певному колу третіх осіб: податковим органам, судам, банку Греції, в деяких випадках кредиторам.

Данія	Законом «Про фінансову діяльність» передбачено, що члени ради директорів, засновники, працівники банків, ліквідатори, аудитори, інспектори банківського нагляду й інші посадові особи фінансово-кредитних установ, одержувачі такої інформації не можуть розкривати або використовувати конфіденційну інформацію без належної підстави. Порушення такого зобов'язання карається кримінальними і цивільно-правовими санкціями. У порядку, визначеному законодавством, правоохоронні органи мають юридичні підстави отримати відповідну інформацію.
Ірландія	Діють норми загального права (common law), які зобов'язують банки зберігати конфіденційність щодо своїх справ з клієнтами, що забезпечується чинним контрактом між банком і клієнтом і повністю визнається судами. Кримінального покарання за порушення конфіденційності загальне право не передбачає.
Іспанія	Закон № 44 2002 р. «Про банки» покладає на банки обов'язок зберігати в таємниці дані і операції своїх клієнтів, прирівнюючи банківську таємницю до таємниці особистого та сімейного життя. Механізм забезпечення банківської таємниці ґрунтується на підставі укладених контрактів.
Італія	Національне законодавство щодо банківської таємниці сформоване на підставі директив ЄС та існуючих у банківській системі традицій та адміністративної практики судів і численних правил, встановлених банками.
Латвія	Законом «Про кредитні інститути» 1995 р. встановлено, що обов'язком кредитного інституту є збереження конфіденційності особи, рахунків, депозитів і угод клієнта. Обов'язок зберігати професійну таємницю поширюється на менеджерів, адміністраторів, працівників кредитного інституту, представників державних органів, яким у силу виконання посадових обов'язків стала відома конфіденційна інформація. Розкрити конфіденційну інформацію можна на підставі адміністративних рішень податкових органів, прокуратури, суду, Банку Латвії та Комісії з фінансового ринку і ринку капіталу, на які не поширюється зобов'язання зберігати професійну таємницю у випадку протиправного використання фінансових ресурсів.
Литва	Закон «Про банки» 2004 р. містить визначення «секрети банку», до яких належать будь-які дані та інформація про: рахунки, відкриті у банку, баланс за рахунком, здійснення операцій, умови, на яких надаються послуги, зобов'язання клієнта, фінансова ситуація клієнта та інші дані фінансового характеру. Банк, банківські співробітники і треті особи, яким інформація стала відома, не повинні розкривати її третім особам, крім випадків, встановлених Законом про банки та іншими законами. Адміністратив-

	ний і кримінальний кодекси встановлюють санкції за порушення банківської таємниці.
Ліхтенштейн	Закон «Про банки і фінансові компанії» 1992 р. визначає, що персонал банків зобов'язаний зберігати в таємниці інформацію, яка стала їм відома внаслідок виконання ними своїх обов'язків. Обов'язок, не маючи тимчасового обмеження, стосується співробітників державних органів, яким інформація стала відома в силу виконання своїх функцій. За співробітниками банків зберігається обов'язок давати свідчення перед місцевими кримінальними судами, а також інформувати про підозри у вчиненні злочинів.
Люксембург	Закон «Про фінансовий сектор» накладає на співробітника фінансової установи обов'язок тримати в таємниці інформацію, отриману ним при виконанні професійних обов'язків відповідно до положень про професійну таємницю, встановлених кримінальним законом. Нормативний акт встановлює випадки, коли інформація може бути розкрита третім особам у процесі нагляду за банківською діяльністю, але інформація, отримана для одних цілей, не може бути використана для інших.
Німеччина	Положення про банківську таємницю ґрунтується на нормах цивільного права і на контрактних зобов'язаннях, що виникають між банком і клієнтом, відповідно до якого банк зобов'язаний зберігати конфіденційність справ клієнта. Спеціальними федеральними законами встановлено обов'язок банків, з низкою суттєвих обмежень, передавати інформацію про клієнтів і їхні справи податковим органам.
Польща	Закон «Про банківську діяльність» від 29 серпня 1997 р. визначає, що банківською таємницею є інформація, що стосується банківської діяльності, зокрема інформація, що стосується клієнтів. Банки, їх співробітники та особи, через яких банки здійснюють свою діяльність, зобов'язані зберігати банківську таємницю. Банківська таємниця може бутирозкрита тільки у випадках, визначених законом на підставі процесуальних рішень правоохоронних органів
Португалія	Декретом № 298, прийнятим у 1992 р., визначено банківську таємницю як професійне зобов'язання працівників фінансових установ, які надають послуги на постійній або тимчасовій основі, не публікувати або використовувати інформацію, що стосується діяльності кредитних інститутів та їх взаємовідносин з клієнтами. Імена клієнтів, рахунки і рух за рахунками знаходяться під захистом професійної таємниці. Закон передбачає розкриття інформації третім особам, зокрема правоохоронним органам
Словаччина	Закон № 483 «Про банківську діяльність», прийнятий у 2001 р.,

	визначив поняття банківської таємниці. Працівники банків, члени органів управління та нагляду зобов'язані зберігати інформацію, що зачіпає інтереси банків і клієнтів, у таємниці і під час перебування на посаді і після припинення виконання своїх обов'язків. Будь-яка інформація і документи, що стосуються клієнтів банку та їх діяльності, які не можуть бути отримані з відкритих джерел, особливо інформація про операції та баланси рахунків, підпадає під дію положень про банківську таємницю. Банківською таємницею є також умови угоди, яка не була здійснена. Закон допускає надання інформації у визначених випадках правоохоронним органам на підставі адміністративних рішень
Словенія	Закон «Про банківську діяльність» 1999 р. вважає конфіденційними відомості про стан рахунків, умови угод, укладених клієнтами та банками. Перелік посадових осіб, які несуть відповідальність за порушення Положення банківської таємниці, поширюються на членів правління, акціонерів, працівників банку та інших осіб, які у зв'язку зі своєю роботою в банку або наданням послуг банком отримують доступ до конфіденційної інформації. Відповідно до закону банк повинен розглядати як конфіденційні всі дані, факти та обставини, які стали відомі банку при наданні послуг клієнтові або здійсненні угод. Надання інформації правоохоронним органам визначено нормативними актами, які регулюють їх діяльність
Фінляндія	Закон «Про кредитні інститути» зобов'язує працівника банку або кредитного інституту зберігати в таємниці отриману ним в процесі виконання своїх професійних обов'язків інформацію, що стосується стану, особистих обставин клієнтів або інших осіб, їхніх торговельних або ділових секретів, за винятком випадків, коли особи, яких ця інформація стосується, дозволять її розкрити. В адміністративному порядку надається інформація за запитами правоохоронних органів та суду.
Угорщина	Закон «Про кредитні інститути і фінансові підприємства» накладає на працівників банків обов'язок зберігати в таємниці інформацію, що стосується інтересів своїх клієнтів: особисті дані, діяльність, угоди і баланси за рахунками. Передбачено кримінальне покарання за несанкціоноване законом розкриття інформації, що належить до банківської таємниці.
Франція	Співробітники та керівники банків зобов'язані зберігати інформацію в таємниці відповідно до переліку відомостей, які віднесені до банківської таємниці. За порушення професійного обов'язку передбачено кримінальне та цивільне покарання.
Чехія	Банківська таємниця охоплює взаємини, що стосуються інтересів банку та клієнтів. Обов'язок зберігати банківську інфор-

	мацію в таємниці покладено на всіх працівників банківських і парабанківських установ. В окремих випадках керівні органи банку можуть звільнити працівника від обов'язку зберігати банківську таємницю. У випадку підозри щодо отримання коштів незаконним шляхом правоохоронні органи мають право отримати інформацію на підставі умотивованого запиту на підставі закону, який визначає порядок діяльності правоохоронного органу.
Швейцарія	Федеральний закон «Про банки» від 8 листопада 1934 р. забороняє посадовим особам банку, комісіонерам банку, представникам Федеральної банківської комісії, співробітникам або посадовим особам аудиторської компанії розкривати інформацію про клієнтів, яка їм стала відома в результаті здійснення своєї діяльності. Закон забороняє їм давати третім особам підтвердження, що їм відома будь-яка інформація, яка стосується клієнтів. Розкриття банківської таємниці здійснюється на підставі рішення суду за клопотанням правоохоронного органу
Швеція	Закон «Про банківську діяльність» від 1987 р. встановлює, що інформація між клієнтом і банком не може бути розкрита третім особам без належної юридичної підстави. Законодавство та судова практика встановлює ряд винятків із банківської таємниці.
Естонія	Закон Естонії «Про кредитні інститути», прийнятий у 1999 р., визначає банківською таємницею дані, що стосуються фінансового стану, особистих даних, угод, економічної діяльності, ділових і професійних секретів, прав власності або бізнесу клієнтів кредитного інституту. Інформація може бути розкрита третім особам тільки з письмової згоди клієнта або на підставі інших положень зазначеного закону.

ПРЕДМЕТНИЙ ПОКАЖЧИК

– національна

Види безпеки

Гриф
– секретності
– обмеження доступу

Державна служба *8*
Державний службовець
Договір про патентне право
Допуск до державної таємниці
Доступ до державної таємниці

Електронна комерція
Електронний
– документообіг
– цифровий підпис

Загрози
– інформаційній безпеці
– національній безпеці
Захист інформації
– криптографічний (КЗІ) *1*
– технічний (ТЗІ)
Звід відомостей, що становлять державну таємницю (ЗВДТ)

Інтелектуальна власність

Інформаційне

– середовище

– суспільство

Інформаційні

– відносини

– ресурси

Інформація

– відкрита

– конфіденційна

– службова

– таємна

Комп’ютерна програма

Криптографія

Криптографічна система

Криптографічний алгоритм

Об’єкти

– державної безпеки

– національної безпеки

Обмеження доступу

– в інтересах слідства і судочинства

Особа

– посадова

– службова

Патент

Персональні дані

Принципи безпеки

Пріоритети безпеки

ІМЕННИЙ ПОКАЖЧИК

Гаврилов О. А.

Ешбі У. Р.

Єршов А. П.

Копилов В. О.

Ласуелл Г.

Маккарті Дж.

Мартін Дж.

Масуда І.

Моргентау Г.

Ровенський В.

Сциллард Л.

Уємов А. І.

Урсул А. Д.

Фішер Р.

Хартлі Р.

Шарм К.

Шенон К.

Шиллінг фон Каштадт П. Л., барон