Науково-дослідний інститут інформатики і права
Національної академії правових наук України

Національна бібліотека України ім. В.І. Вернадського
Національної академії наук України

Відкритий міжнародний університет розвитку людини "Україна"

Інформація і право

НАУКОВИЙ ЖУРНАЛ

№ 3(9)

2013

Зареєстрований Міністерством юстиції України
(Свідоцтво про державну реєстрацію друкованого засобу масової інформації:
Серія КВ № 17541-6291Р від 18.03.11 р.)

Згідно з Постановою ВАК України від 31.05.11 р. № 1-05/5
у журналі можуть публікуватися матеріали стосовно дисертаційних робіт
на здобуття наукових ступенів доктора і кандидата наук у галузі юридичних наук

м. Київ

УДК 002:340+316.4+338.46:002

З М І С Т

І н ф о р м а ц і й н е п р а в о

І н ф о р м а ц і й н і т е х н о л о г і ї

І н ф о р м а ц і й н і р е с у р с и з і н ш и х с п е ц і а л ь н о с т е й ю р и д и ч н и х н а у к

Європейські правові стандарти

Рекомендовано до друку Вченою радою НДІІП НАПрН України, протокол № 9 від 31.10.13 р.

І н ф о р м а ц і й н е п р а в о

УДК 342.9 (477) (075.8)

ЖИЛЯЄВ І.Б., *доктор економічних наук, професор*
ФУРАШЕВ В.М., *кандидат технічних наук, старший науковий співробітник, доцент, професор РАЕ*

ЗДОБУТКИ В СИСТЕМІ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ ІНФОРМАТИЗАЦІЇ ТА ПОБУДОВИ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА УПРОДОВЖ 2012 – 2013 РОКІВ

Анотація. *Про зміни та удосконалення системи нормативно-правового забезпечення розвитку інформатизації та побудову інформаційного суспільства в Україні упродовж 2012 – 2013 років.*

Ключові слова: *інформатизація, інформаційне суспільство, національна політика у сфері інформатизації, правове регулювання, електронна взаємодія.*

Аннотация. *Об изменениях и усовершенствовании системы нормативно-правового обеспечения развития информатизации и построение информационного общества в Украине на протяжение 2012 – 2013 годов.*

Ключевые слова: *информатизация, информационное общество, национальная политика в сфере информатизации, правовое регулирование, электронное взаимодействие.*

Summary. *About the changes and improvement in the system of the regulatory and legal support of development of informatization and construction of informative society in Ukraine during 2012 – 2013.*

Keywords: *informatization, informational society, national policy in the field of informatization, legal regulation, electronic interaction.*

Постановка проблеми. Під час проведення Паризького саміту у 2008 році лідери Європейського Союзу (далі – ЄС) і України домовилися, що Угода про асоціацію між ЄС і Україною замінить відповідну Угоду про партнерство і співробітництво, яка діяла з 1998 року.

19 грудня 2011року під час роботи п’ятнадцятого самміту “Україна-ЄС” лідери України і ЄС заявили про досягнення взаєморозуміння щодо тексту Угоди про асоціацію, інтенсивна робота над яким велася з 2008 року.

30 березня 2012 року глави делегацій України та ЄС парафували текст Угоди про асоціацію, у тому числі й положення про створення глибокої і всеохоплюючої зони вільної торгівлі.

19 липня 2012 року було парафовано частину Угоди про асоціацію стосовно створення глибокої і всеохоплюючої зони вільної торгівлі, а також погоджено спільні забов’язання щодо вжиття подальших технічних кроків, необхідних для завершення укладання даної угоди.

28 – 29 листопада 2013 року під час Вільнюського саміту ”Східного партнерства” очікується підписання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом і його державами-членами, з іншої сторони.

Знайомство зі структурою та змістом проекту Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом і його державами-членами, з

іншої сторони, а також додатків до неї[1] свідчить про те, що реалізація багатьох положень цієї угоди спирається на визначений рівень інформатизації та побудову інформаційного суспільства в нашій країни, особливо в частині нормативно-правового забезпечення.

Метою статті є визначення здобутків у системі нормативно-правового забезпечення розвитку інформатизації та побудови інформаційного суспільства упродовж 2012 – 2013 років, тобто у ті роки, коли велася найбільш інтенсивна робота з підготовки Угоди про асоціацію.

Виклад основних положень. З точки зору змін у системі нормативно-правового забезпечення розвитку інформатизації та побудови інформаційного суспільства в Україні упродовж 2012 – 2013 років, проводилися дослідження у двох основних напрямах:

– динамізму правового забезпечення процесів інформатизації, електронного урядування та розвитку інформаційного суспільства;

– пріоритетів та завдань національної політики у сферах інформатизації, електронного урядування та розвитку інформаційного суспільства.

1. Динамізм правового забезпечення процесів інформатизації, електронного урядування та розвитку інформаційного суспільства

Українська правова система на початку другого десятиліття XXI століття продовжує інтенсивно розвиватися. Насамперед, значно збільшується кількість нормативно-правових актів, що модернізують регуляторну систему багатьох сфер суспільно-політичних відносин (Табл. 1).

Таблиця 1. Кількість нормативно-правових актів, прийнятих у 2011 – 2013 рр. Верховною Радою України, Президентом України, Кабінетом Міністрів України[2].

	2011 р.	2012 р.	За станом на 15.08.13 р.
закони України	388	357	88
постанови Верховної Ради України	962	833	314
укази Президента України	1130	699	385
розпорядження Президента України	318	207	230
постанови Кабінету Міністрів України	1413	1212	518
розпорядження Кабінету Міністрів України	1368	1063	549

У 2012 році значна увага приділялася питанням удосконалення законодавчого забезпечення національної політики з розвитку інформаційного суспільства, інформатизації та електронного урядування в Україні. Усіма органами державної влади видавалася значна кількість нормативно-правових актів (Рис. 1), деякі з яких будуть мати середньо- та довгостроковий вплив на здійснення зазначеної діяльності.

У 2012 – 2013 рр. органи державної влади приділяли значну увагу досконаленню правового забезпечення процесів інформатизації, електронного урядування та розвитку інформаційного суспільства. Якість державної політики у зазначених сферах, по-перше, напряму залежить від якості розробки відповідного правового забезпечення. У цьому питанні є певні проблеми. Як зазначено у Посланні Президента України, *“Непоодинокими є випадки внесення до Верховної Ради України на виконання Національного плану законопроектів із низькою якістю, непрорахованістю ресурсного забезпечення та наслідків, невідповідністю стратегічній лінії реформ”* [1].

[1] Режим доступу : //www.kmu.gov.ua/kmu/control/uk/publish/article?art_id=246581344&cat_id=223223535

[2] За станом на 15.08.13 р. база даних “Законодавство України” складає 189067 документів.

Рис.1. Кількість затверджених нормативно-правових актів (помісячно), які використовують у тексті ключові слова “інформатизація”, “електронний (електронна)”, “інформація (інформаційний)”.

По-друге, забезпечення модернізації національної політики в зазначених сферах хоча й залежить від наявності регуляторних актів, їх якості, однак у першу чергу ця політика може бути ефективною лише за наявності інституційної структури, у тому числі – сформованих структур державного управління, державно-приватного партнерства, що не суперечить одна одній, чіткої системи аналізу та моніторингу виконання рішень та гнучкого реагування на обставини, що змінюються (перегляд та скасування актів, що є малоефективними або негативно впливають на процеси; міжгалузеве узгодження актів, що пропонуються до схвалення, підготовки нових державних рішень тощо). Тобто, окрім ефективної системи правового забезпечення процесів інформатизації, електронного урядування та розвитку інформаційного суспільства, має бути сформовано адекватну та підконтрольну громадськості систему державного управління, націлену на результат, а також, оскільки зазначені процеси залежать від їх сприйняття бізнесом та громадськістю, створено систему взаємодії влади з бізнесом та громадянами. Саме тому у Посланні наголошувалося: *“На порядку денному – подальше реформування системи державного управління, перехід до моделі держави, орієнтованої на обслуговування потреб громадян. У кожному місті, районі має з’явитися сучасний центр надання адміністративних послуг. У кожному з них повинен надаватися гарантований перелік найбільш запитуваних громадянами та бізнесом послуг. Вони мають надаватися протягом мінімального терміну”* [1, с. 17].

2. Пріоритети та завдання національної політики у сферах інформатизації, електронного урядування та розвитку інформаційного суспільства

Україна у 2012 – 2103 рр. здійснила низку заходів, спрямованих як на впровадження принципів інформаційного суспільства загалом, так і на розвиток електронного урядування як одного з його головних компонентів. Передусім це стосується розробки Державним агентством з питань науки, інновацій та інформатизації України за участю представників громадянського суспільства та науковців Стратегії

розвитку інформаційного суспільства в Україні, в якій розбудову електронного урядування визначено однією зі стратегічних цілей.

Одним з важливих завдань щодо соціально-економічного та політичного розвитку України за допомогою широкого впровадження інформаційно-комунікаційних технологій (далі – ІКТ) є формування довго- та середньострокових цілей національної політики у сферах інформатизації, електронного урядування та розвитку інформаційного суспільства.

Протягом 2012 – 2013 рр. формуванню пріоритетів та довго- і середньострокових цілей у цих сферах приділялася значна увага.

Важливу роль відігриває *Стратегія розвитку інформаційного суспільства в Україні,* схвалена розпорядженням Кабінету Міністрів України від 15.05.13 р. № 386-р [2], яка визначає мету, базові принципи, стратегічні цілі розвитку інформаційного суспільства в Україні, завдання, спрямовані на їх досягнення, а також основні напрями, етапи і механізм реалізації цієї стратегії з урахуванням сучасних тенденцій та особливостей розвитку України в перспективі до 2020 року.

Стратегією, зокрема, визначено основні стратегічні цілі розвитку інформаційного суспільства та суспільства знань: 1) прискорення процесу розроблення та впровадження сучасних інформаційно-комунікаційних технологій у державне управління, охорону здоров’я, культуру, освіту, науку, охорону навколишнього природного середовища, бізнес тощо; 2) розвиток електронної економіки; 3) забезпечення комп’ютерної та інформаційної грамотності громадян насамперед шляхом створення системи освіти, орієнтованої на використання новітніх інформаційно-комунікаційних технологій у формуванні всебічно розвиненої особистості, та забезпечення неперервності навчання; 4) розвиток національної інформаційної інфраструктури та її інтеграція до світової інфраструктури; 5) підвищення якості та доступності адміністративних послуг, спрощення процедур їх надання і скорочення відповідних витрат, деперсоніфікація надання адміністративних послуг як інструмент зниження рівня корупції; 6) розвиток електронної демократії; 7) збереження культурної спадщини України шляхом документування її об’єктів на цифрових носіях, забезпечення накопичення і збереженості електронних документів та електронних інформаційних ресурсів; 8) забезпечення ефективної участі регіонів України у процесах становлення інформаційного суспільства, підтримка регіональних і місцевих ініціатив; 9) захист інформаційних прав громадян та організацій, авторського права, підтримка демократичних інститутів та мінімізацію ризиків “інформаційної нерівності”; 10) захист персональних даних; 11) забезпечення відкритості інформації про діяльність державних органів влади та органів місцевого самоврядування, розширення доступу до неї та надання можливості безпосередньої участі як інститутів громадянського суспільства, так і громадян у процесах підготовки і проведення експертизи проектів актів законодавства, здійснення контролю за результативністю і ефективністю діяльності органів державної влади та органів місцевого самоврядування; 12) удосконалення інформаційного законодавства; 13) поліпшення стану інформаційної безпеки.

Стратегією затверджено 14 контрольних показники та індикатори розвитку інформаційного суспільства.

Національна система індикаторів розвитку інформаційного суспільства, затверджена постановою Кабінету Міністрів України від 28.11.12 р. № 1134, спрямована на отримання об’єктивної інформації про сучасний стан розвитку інформаційного суспільства, включає 31 індикатор. Проведення такого моніторингу є невід’ємною частиною державної політики у цій сфері, що дозволятиме сформувати відповідні заходи з покращення ситуації у цій сфері.

Конкретні річні завдання у зазначених сферах затверджувалися різними нормативно-правовими актами органів державної влади. Важливе місце в формування завдань щодо здійснення державної політики у цих сферах належить національним планам дій на відповідний рік щодо впровадження Програми економічних реформ на 2010 – 2014 роки “Заможне суспільство, конкурентоспроможна економіка, ефективна держава”, що затверджувалися відповідними указами Президента України. Так, розділ “XV. Електронне урядування” Національного плану дій на 2012 рік щодо впровадження Програми економічних реформ на 2010 – 2014 роки “Заможне суспільство, конкурентоспроможна економіка, ефективна держава” передбачав реалізацію у 2012 році 22 заходів, зокрема щодо: Удосконалення законодавства у сфері інформаційно-комунікаційних технологій – 3 заходи; удосконалення державного регулювання та контролю за додержанням законодавства про електронний цифровий підпис – 4; створення інформаційної системи електронної взаємодії державних інформаційних ресурсів – 4; створення автоматизованої системи “Єдине вікно подання електронної звітності” – 4; створення Єдиного державного порталу адміністративних послуг – 3; модернізація системи електронної взаємодії між центральними органами виконавчої влади, Радою міністрів Автономної Республіки Крим та обласними, Київською і Севастопольською міськими державними адміністраціями, іншими державними органами – 1; впровадження інформаційної системи “Звернення громадян” – 1; розроблення та ухвалення Стратегії розвитку сфери ІКТ в Україні – 2 заходи.

Національний план дій на 2013 рік щодо впровадження Програми економічних реформ на 2010 – 2014 роки “Заможне суспільство, конкурентоспроможна економіка, ефективна держава” в розділі “Розбудова електронного урядування” передбачав виконання 7 заходів у двох розділах [3]:

1. Забезпечення роботи систем електронного урядування (реалізація системи електронної взаємодії державних баз даних) – 4 заходи, зокрема: 1) схвалення Концепції створення та функціонування інформаційної системи електронної взаємодії державних баз даних; 2) видання Кабінетом Міністрів України актів з питань функціонування інформаційної системи електронної взаємодії державних баз даних; 3) внесення на розгляд Верховної Ради України проекту Закону України щодо врегулювання питань роботи інформаційної системи електронної взаємодії державних баз даних; 4) впровадження інформаційної системи електронної взаємодії державних баз даних (інтеграція не менше 50 % державних баз даних в інформаційну систему електронної взаємодії державних баз даних);

2. Реалізація Концепції розвитку електронного урядування в Україні – 3 заходи, зокрема: 1) забезпечення електронної взаємодії між центральними органами виконавчої влади, Радою міністрів Автономної Республіки Крим та обласними, Київською, Севастопольською міськими державними адміністраціями; 2) створення та забезпечення функціонування автоматизованої системи “Єдине вікно подання електронної звітності” (впровадження першої черги системи “Єдине вікно подання електронної звітності”); 3) впровадження інформаційної системи “Звернення громадян” (створення єдиного інформаційного веб-порталу звернень громадян до органів державної влади та органів місцевого самоврядування).

Стратегія співробітництва держав-учасниць СНД у побудові та розвитку інформаційного суспільства та План дій щодо її реалізації на період до 2015 року, затверджено рішенням Ради глав урядів СНД (м. Ялта, 28.09.12 р.). Основними напрямами співробітництва держав-учасниць СНД у побудові та розвитку інформаційного суспільства в Стратегії-2015 запропоновані: 1) гармонізація законодавства та нормативно-технічної бази у сфері ІКТ; 2) розробка і впровадження сучасних додатків ІКТ; 3) розвиток інформаційно-комунікаційної інфраструктури і створення загального інформаційного

простору; 4) вдосконалення механізму взаємодії держав Співдружності щодо розвитку ринку у сфері ІКТ; 5) забезпечення інформаційної безпеки.

У Стратегії-2015 передбачається співробітництво держав-учасниць СНД у галузі сучасних додатків ІКТ: “електронний уряд”, електронне та дистанційне навчання, електронна охорона здоров’я, розвиток систем електронної торгівлі, створення і розвиток інтегрованих регістрів фізичних та юридичних осіб, застосування інформаційних і біометричних технологій у системах паспортно-візових та інших ідентифікаційних документів нового покоління, збереження культурної спадщини. У Плані дій-2015 конкретизовані заходи та забезпечено їх орієнтування на реалізацію кооперційних проектів, на активізацію інформаційного та науково-технічного обміну з використання ІКТ в освіті, науці, культурі, охороні здоров’я, державному управлінні, у наданні послуг населенню та по інших напрямах.

Реалізація Стратегії та Плану дій з її реалізації стане важливим чинником формування інформаційного простору СНД на базі ІКТ, матиме позитивний вплив на модернізацію економік держав-учасниць СНД. У результаті реалізації основних напрямів Стратегії-2015 і заходів Плану дій-2015 планується збільшення вкладу ІКТ у зміцнення економічного потенціалу держав-учасниць СНД, посилення конкурентоспроможності національних економік, підвищення рівня добробуту і якості життя населення. Держави-учасниці СНД вийдуть на новий рівень співпраці і широкої кооперації в галузі використання ІКТ, отримає розвиток загальний ринок продукції та послуг у сфері ІКТ. На теренах СНД буде створено транскордонний простір довіри на основі мережі Інтернет. Істотно покращаться показники держав-учасниць СНД у міжнародних рейтингах в галузі розвитку інформаційного суспільства і в міжнародних рейтингах за рівнем доступності національної інформаційно-комунікаційної інфраструктури для суб’єктів інформаційної сфери. Скоротиться “цифровий розрив” між державами Співдружності.

2.1. Державна політика у сфері інформатизації

Процеси інформатизації у 2012 році у першу чергу регламентувалися *Переліком завдань (проектів) Національної програми інформатизації на 2012 рік, їх державних замовників та обсягів фінансування*, затвердженим розпорядженням Кабінету Міністрів України від 17.10.12 р. № 813-р.

Важливе значення у запровадженні сучасних ІКТ у парламентській діяльності відіграватиме *Програма інформатизації законотворчого процесу у Верховній Раді України на 2012-2017 роки*, затверджена постановою Верховної Ради України від 05.07.12 р. № 5096-VI, що спрямована на досягнення максимально можливої автоматизації інформаційно-організаційних процесів у діяльності депутатського корпусу загалом, у тому числі комітетів Верховної Ради України, депутатських фракцій, а також Апарату Верховної Ради України шляхом створення сучасних систем управління законотворчим процесом та документообігом у парламенті; оперативне інформаційно-аналітичне забезпечення народних депутатів України, помічників-консультантів народних депутатів України, фахівців Апарату Верховної Ради України; створення нової автоматизованої системи обробки вхідних, вихідних, внутрішніх інформаційно-документальних потоків та контролю за виконанням доручень, оперативне формування аналітично-звітної та довідкової документації; технічне удосконалення систем зв’язку для забезпечення оперативності у роботі народних депутатів України, комітетів Верховної Ради України, Апарату Верховної Ради України, у тому числі щодо питань, пов’язаних з діяльністю органів виконавчої влади, органів місцевого самоврядування, інформуванням громадян. Пріоритетним завданням програми є створення інтегрованої електронної інформаційно-аналітичної системи “Електронний парламент” та її

центральних підсистем: “Електронний офіс народного депутата України”; “Електронний комітет”; “Електронна Погоджувальна рада”; “Електронна бібліотека та архів”; “Електронна зала пленарних засідань: система електронного голосування та підрахунку голосів, система стенографування, система ведення аудіо- та відеотрансляцій та архіву пленарних засідань Верховної Ради України”; “Система електронного документообігу і контролю виконання доручень Верховної Ради України”; “Система електронного цифрового підпису”; “Комплексна система захисту інформації в автоматизованих системах Верховної Ради України”. Основу системи складуть діючі автоматизовані системи Верховної Ради України: інтегрована база даних законотворчого процесу, “Система електронного документообігу і контролю виконання доручень Верховної Ради України”, “Система електронного цифрового підпису”, “Комплексна система захисту інформації в автоматизованих системах Верховної Ради України”, “Електронний офіс народного депутата України” (стаціонарний і мобільний), система підтримки прийняття рішень комітетом (“Електронний комітет”), центр ситуативного аналізу (“Електронна Погоджувальна рада”), “Електронна бібліотека та архів” (мережева збірка парламентської інформації, доступна депутатському корпусу, співробітникам Апарату Верховної Ради України та суспільству), “Електронна зала пленарних засідань”, єдиний веб-портал Верховної Ради України та інтегровані до нього веб-сайти Голови Верховної Ради України, комітетів Верховної Ради України, депутатських фракцій, структурних підрозділів Апарату Верховної Ради України.

Важливим документом для підвищення рівня довіри суспільства до виборів, забезпечення публічності та відкритості виборчого процесу, доступу громадськості до спостереження в режимі реального часу під час голосування і можливості отримання відеозапису процесу підрахунку голосів виборців у приміщенні для голосування звичайної виборчої дільниці із застосуванням переваг ІКТ став *Закон України “Про внесення змін до Закону України “Про особливості забезпечення відкритості, прозорості та демократичності виборів народних депутатів України 28 жовтня 2012 року”* [4], яким уточнюється правовий режим використання у виборчому процесі системи відеоспостереження, відеозапису і трансляції зображення, яка забезпечує створення інформації, передачу зображення з приміщення для голосування звичайної виборчої дільниці з можливістю його перегляду на відповідному веб-сайті у мережі Інтернет та подальше збереження створеної в процесі відеоспостереження інформації, спрямованої на підвищення рівня довіри суспільства до виборів, публічності та відкритості виборчого процесу, доступу громадськості до спостереження у режимі реального часу під час голосування, а також створення відеозапису підрахунку голосів виборців у приміщенні для голосування звичайної виборчої дільниці. На виконання закону постановою Кабінету Міністрів України від 08.08.12 р. № 766 затверджене *Технічне завдання та конфігурація створення системи відеоспостереження,* що містить вимоги, виконання яких дало змогу раціонально та ефективно реалізувати всі складові системи відеоспостереження на звичайних виборчих дільницях під час виборів народних депутатів України у 2012 році з використанням сучасних ІКТ[3]. Система відеоспостереження створювалася відповідно до взаємопов’язаних вимог нормативно-правових актів шляхом здійснення організаційно-розпорядчих заходів з використанням програмно-технічних і телекомунікаційних засобів, що

[3] Система відеоспостереження діяла на 32192 звичайних виборчих дільницях на території України і транслювала зображення з роздільною здатністю не менш як 320 х 240 (не більше 50 відсотків загальної кількості точок підключення), забезпечуючи реєстрацію і підключення не менш як 5 млн. користувачів з можливістю здійснення не менше 10 тис. одночасних переглядів з кожної камери (із забезпеченням одночасного ведення не менш як 300 тис. одночасних трансляцій).

забезпечують процеси збирання, передавання, накопичення, зберігання, архівування, трансляції відеоінформації щодо організації проведення голосування та підрахунку голосів виборців на звичайних виборчих дільницях під час проведення виборів народних депутатів України в день голосування 28 жовтня 2012 року.

Реалізацію завдань інформатизації у фінансово-банківській системі забезпечуватиме *Закон України “Про внесення змін до деяких законодавчих актів України щодо функціонування платіжних систем та розвитку безготівкових розрахунків”* від 18.09.12 р. № 5284-VI [5], яким внесено зміни до наступних законів України: 1) “Про Національний банк України” (уточнення функцій НБУ щодо регулювання платіжних систем); 2) “Про платіжні системи та переказ коштів в Україні” (введення нових термінів, уточнення змісту тих, що раніше використовувалися, зокрема – “еквайринг”, “електронний платіжний засіб”, “моніторинг”, “користувач платіжної системи”, “маршрутизація”, “мобільний платіжний інструмент”, “оператор послуг платіжної інфраструктури”, “платіжна організація”, “платіжний інструмент”, “платіжний пристрій”, “процесинг”, “система розрахунків” тощо, та уточнення деяких засад функціонування платіжних систем в Україні); 3) “Про фінансові послуги та державне регулювання ринків фінансових послуг”; 4) Цивільного кодексу України; 5) Кодексу України про адміністративні правопорушення (щодо введення відповідальності за порушення порядку приймання готівки для подальшого її переказу та здійснення операцій з електронними грошима); 6) Кримінального кодексу України; 7) “Про захист прав споживачів”; 8) “Про державну податкову службу в Україні”; 9) “Про електронний цифровий підпис”.

Прийнято низку нормативно-правових актів із створення державних автоматизованих систем.

Найважливішим нормативно-правовим актом з питань міграційної політики, ухваленим у 2012 р., стала *Концепція створення єдиної інформаційно-аналітичної системи управління міграційними процессами* [6], яка визначає шляхи та етапи створення єдиної інформаційно-аналітичної системи управління міграційними процесами, застосування якої спрямоване на автоматизацію діяльності ДМС і приведення з урахуванням кращого досвіду Європейського Союзу системи державного управління міграційними процесами у відповідність із стандартами Європейського Союзу; визначення підходів до формування та створення інформаційно-аналітичної системи, яка дасть можливість автоматизувати процеси діяльності ДМС, здійснювати обмін інформацією з іншими органами державної влади з метою забезпечення реалізації ними державної політики у сфері міграції (імміграції та еміграції), у тому числі протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших категорій мігрантів, а також сприятиме удосконаленню системи державного управління міграційними процесами відповідно до міжнародних стандартів у сфері реалізації прав людини.

Положення про автоматизовану інформаційно-аналітичну систему ресурсного забезпечення закладів охорони здоров’я державної форми власності, затверджене наказом Міністерства охорони здоров’я України від 20.11.12 р. № 933, визначає механізм функціонування автоматизованої інформаційно-аналітичної системи, створеної для забезпечення моніторингу медико-технічних ресурсів та їх технічного стану у закладах охорони здоров’я, а також виявлення потреб закладів у цих ресурсах.

Положення про інформаційно-пошукову систему “Скорпіон” Головного управління по боротьбі з організованою злочинністю МВС України, затверджене наказом Міністерства внутрішніх справ України від 24.09.12 р. № 825, визначає метою діяльності цієї системи об’єднання існуючих у Головному управлінні по боротьбі з

організованою злочинністю МВС України та управліннях по боротьбі з організованою злочинністю в Автономній Республіці Крим, областях, містах Києві та Севастополі інформаційних ресурсів у єдиний інформаційно-аналітичний комплекс із використанням сучасних інформаційних технологій, комп’ютерного та телекомунікаційного обладнання для забезпечення оперативно-службової діяльності спеціальних підрозділів по боротьбі з організованою злочинністю органів внутрішніх справ України, зміцнення їх спроможності до протидії та профілактики злочинності.

Постановою Кабінету Міністрів України від 08.04.13 р. № 257 затверджений *Порядок використання у 2013 році коштів, передбачених у Державному бюджеті для здійснення заходів з легалізації комп’ютерних програм, які використовуються в органах виконавчої влади.*

Порядок використання коштів, передбачених у Державному бюджеті для створення багатофункціональної комплексної системи “Електронна митниця”, затверджений постановою Кабінету Міністрів України від 22.08.12 р. № 776 з метою забезпечення: розвитку системи автоматизованого аналізу і управління ризиками; переходу на новий рівень автоматизації процедур митного контролю та митного оформлення; впровадження інформаційного обміну документами, необхідними для здійснення митного контролю та митного оформлення, між митними та іншими державними органами; підвищення ефективності здійснення митними органами попереднього документального контролю в пунктах пропуску; розвитку та автоматизації системи захисту прав інтелектуальної власності, класифікації товарів і проведення досліджень (аналізу, експертизи) проб (зразків) товару; автоматизації процесу справляння митних платежів та визначення митної вартості.

Порядок використання коштів, передбачених у Державному бюджеті для здійснення заходів щодо створення єдиних регіональних оперативно-диспетчерських служб з використанням сучасних GPS-технологій, затверджений постановою Кабінету Міністрів України від 03.10.12 р. № 943.

На покращення міжнародного співробітництва у цій сфері спрямовано: 1) постанову Кабінету Міністрів України від 19.12.12 р. № 1210 *“Про приєднання до Рішення Ради глав урядів Співдружності Незалежних Держав про Положення про Координаційну раду держав-учасниць СНД з питань інформатизації при Регіональній співдружності у галузі зв’язку від 7 жовтня 2002 року”*; 2) *Меморандум про взаєморозуміння між Урядом України та Урядом Сполучених Штатів Америки щодо основних напрямів та цілей програми допомоги з боку Агентства США з міжнародного розвитку* визначив підтримку продовження процесу інформатизації судів в Україні.

2.2. Державна політика щодо розвитку інформаційного суспільства

У 2012 – 2013 рр. основними нормативно-правовими актами, які формували національну політику у сфері розвитку інформаційного суспільства, стали *Стратегія розвитку інформаційного суспільства в Україні*, схвалена розпорядженням Кабінету Міністрів України від 15.05.13 р. № 386-р, та *Стратегія співробітництва держав-учасників СНД у побудові та розвитку інформаційного суспільства та План дій щодо її реалізації на період до 2015 року,* затверджені рішенням Ради глав урядів СНД 28 вересня 2012 р. (м. Ялта, Україна). Окрім того, органами державної влади у цій сфері було прийнято низку нормативно-правових актів. Так, постановою Кабінету Міністрів України від 28.11.12 р. № 1134 затверджена *Національна система індикаторів розвитку інформаційного суспільства,* що включає 31 індикатор.

Продовжено розвиток правової бази захисту персональних даних. Прийнято наступні закони України:

1. “*Про внесення змін до Закону України “Про захист персональних даних”* [7], який уточнює механізм регулювання правових відносин, пов’язаних із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних. В законі введено деякі нові терміни, зокрема – “володілець персональних даних” (замість – “володілець бази персональних даних”) і “розпорядник персональних даних” (замість – “розпорядник бази персональних даних”), “згода суб’єкта персональних даних”, “обробка персональних даних”, “картотека”, “одержувач”.

2. *“Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних”* [8], вносить зміни до механізму системи захисту персональних даних, зокрема до Кодексу України про адміністративні правопорушення та законів України: “Про захист персональних даних” та “Про ратифікацію Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних”. Даним Законом Уповноважений Верховної Ради України з прав людини наділяється статусом уповноваженого органу у сфері захисту персональних даних, з наданням відповідних повноважень.

Модернізовано також підзаконну законодавчу базу регулювання відносин у цій сфері. Наказом Міністерства юстиції України від 22.07.13 р. № 1466/5 [9] внесено зміни до деяких наказів Міністерства юстиції України щодо удосконалення правового регулювання у сфері захисту персональних даних, зокрема – Типового порядку обробки персональних даних у базах персональних даних, затвердженого наказом Міністерства юстиції України від 30.12.11 р. № 3659/5, а також до наказу Міністерства юстиції України від 08.07.11 р. № 1824/5 “Про затвердження форм заяв про реєстрацію бази персональних даних та про внесення змін до відомостей Державного реєстру баз персональних даних і порядку їх подання”.

Порядок обробки персональних даних у базі персональних даних Національної комісії, що здійснює державне регулювання у сфері енергетики, затверджений постановою Національної комісії, що здійснює регулювання у сфері енергетики, від 17.01.13 р. № 20.

Порядок обробки персональних даних у сфері забезпечення функціонування системи гарантування вкладів фізичних осіб затверджений Рішенням Виконавчої дирекції Фонду гарантування вкладів фізичних осіб від 12.07.12 р. № 9.

Вживалися заходи з модернізації окремих сфер діяльності: освіти, науки, культури, охорони здоров’я, інформаційної безпеки та активізації участі громадян у формуванні та реалізації управління державою.

Так, розпорядженням Кабінету Міністрів України від 27.03.13 р. № 168-р з метою забезпечення стабільно високого рівня усвідомленої підтримки населенням України євроінтеграційного курсу як одного з пріоритетів внутрішньої та зовнішньої політики нашої держави, реформ, які проводяться та проводитимуться владою з метою підготовки України до майбутнього членства в ЄС, пропонується, зокрема, орієнтуватися на використання сучасних методів донесення інформації (Інтернет-конференції, чати, ток-шоу, телевікторини, електронні видання, брендинг), у тому числі з використанням новітніх технологій, Схвалено *Концепцію реалізації державної політики у сфері інформування та налагодження комунікації з громадськістю з актуальних питань європейської інтеграції України на період до 2017 року.*

Пріоритетом економічного розвитку України визначено стимулювання розвитку індустрії програмної продукції, випуск високотехнологічної продукції.

Закон України “Про державну підтримку розвитку індустрії програмної продукції” [10], спрямований на формування сприятливих умов розвитку індустрії програмної продукції України для створення високопродуктивних робочих місць, залучення інвестицій, збільшення обсягів випуску високотехнологічної продукції, стимулювання наукомісткого експорту та імпортозаміщення, реалізацію науково-технічного потенціалу України. Законом визначено, що державна підтримка розвитку індустрії програмної продукції спрямована на: 1) удосконалення способів забезпечення розвитку індустрії програмної продукції в Україні; 2) стимулювання розвитку системи управління в індустрії програмної продукції, у тому числі на поліпшення управління якістю продукції на основі стандартизації; 3) формування ефективного механізму взаємодії юридичних та фізичних осіб, зайнятих у сферах фундаментальної і прикладної науки, виробничому та інших секторах економіки, з учасниками індустрії програмної продукції; 4) стимулювання переходу до моделі інноваційного розвитку індустрії програмної продукції; 5) удосконалення податкового, митного, валютного, трудового та пенсійного законодавства в частині, що регулює діяльність індустрії програмної продукції; 6) збільшення кількості високопродуктивних робочих місць в індустрії програмної продукції; 7) підвищення конкурентоспроможності учасників індустрії програмної продукції на зовнішніх ринках; 8) створення сприятливих умов для залучення вітчизняних та іноземних інвестицій для розвитку індустрії програмної продукції; 9) сприяння здійсненню фундаментальних та прикладних наукових досліджень у сфері інформаційних технологій; 10) активізацію міжнародного співробітництва та покращення іміджу України на міжнародному ринку як країни, що має розвинену і висококонкурентну індустрію програмної продукції; 11) сприяння пріоритетному запровадженню комп’ютерних програм, створених учасниками індустрії програмної продукції України, на державних підприємствах, в наукових установах, органах державної влади та органах місцевого самоврядування, у тому числі з метою зниження витрат замовників; 12) сприяння запровадженню комп’ютерних програм, створених учасниками індустрії програмної продукції України, у тому числі з метою зниження витрат вітчизняних товаровиробників.

Закон України “Про внесення змін до розділу XX “Перехідні положення” Податкового кодексу України щодо особливостей оподаткування суб’єктів індустрії програмної продукції” від 05.07.12 р. № 5091-VI встановлює правовий механізм оподаткування суб’єктів індустрії програмної продукції на період з 1 січня 2013 р. до 1 січня 2023 р.

Закон України “Про внесення змін до Закону України “Про державне регулювання діяльності у сфері трансферу технологій” від 02.10.12 р. № 5407-VI [11] – нова редакція Закону України “Про державне регулювання діяльності у сфері трансферу технологій”, що визначає правові, економічні, організаційні та фінансові засади державного регулювання діяльності у сфері трансферу технологій і спрямований на забезпечення ефективного використання науково-технічного та інтелектуального потенціалу України, технологічності виробництва продукції, охорони майнових прав на вітчизняні технології та/або їх складові на території держав, де планується або здійснюється їх використання, розширення міжнародного науково-технічного співробітництва у цій сфері, зокрема – регулювання діяльності з обігу комп’ютерних програм та інформаційно-комунікаційних технологій.

Державна програма активізації розвитку економіки на 2013 – 2014 роки, затверджена постановою Кабінету Міністрів України від 27.02.13 р. № 187 серед стимулюючих заходів передбачає: “удосконалення законодавства щодо стимулювання розвитку вітчизняної ІТ-індустрії, зокрема оподаткування суб’єктів індустрії програмної продукції”, що забезпечить “створення вітчизняної імпортозамінної програмної продукції або збільшення обсягу експорту не менше ніж на 3 млрд. гривень; збільшення обсягу

надходжень із сплати єдиного внеску на загальнообов’язкове державне соціальне страхування протягом першого року на 120 млн. гривень, наступних п’яти років – на 4274 млн. гривень; пришвидшення темпів розвитку індустрії програмної продукції до 40-45 відсотків на рік; збільшення щороку кількості робочих місць на 35-40 відсотків (більше ніж 20 тис. на рік)”.

З метою стимулювання розвитку високих технологій з пріоритетних галузевих спеціалізацій (інформаційні та комунікаційні технології, біотехнології та фармацевтика, енергозбереження та енергоефективність, нанотехнології, аерокосмічна індустрія, мікроелектроніка) прийнята постанова Кабінету Міністрів України *“Деякі питання підготовки до реалізації національного проекту “Технополіс”* від 31.10.12 р. № 1014 – створення інфраструктури інноваційного розвитку та високих технологій і їх складових.

2.3. Державна політика щодо розвитку електронного урядування

Державна політика щодо розвитку електронного урядування у 2012 – 2013 рр. у першу чергу була спрямована на подальше реформування системи державного управління, перехід до моделі держави, орієнтованої на обслуговування потреб громадян шляхом запровадження правового регулювання: 1) сучасних систем електронної взаємодії; 2) надання адміністративних послуг в електронній формі; 3) електронного документа та електронного підпису; 4) формування та використання державних електронних ресурсів тощо.

2.3.1. Правове регулювання електронної взаємодії

У Посланні Президента України зазначається, що “Суттєві зрушення спостерігаються і в упровадженні сучасних форм ведення електронного документообігу. Майже всі відомства до кінця 2012 р. вже були підключені до системи електронної взаємодії, також було створено технологічні умови для роботи держчиновників із листами, електронними документами, постановами та розпорядженнями КМУ, які не містять інформації з обмеженим доступом” [1, с. 216].

Концепція створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів [12], затверджена розпорядженням Кабінету Міністрів України від 05.09.12 р. № 634-р, визначила в якості проблеми, яка потребує розв’язання, – те, що єдина інфраструктура міжвідомчої інформаційної взаємодії державних органів та суб’єктів господарювання із застосуванням інформаційних технологій не створена, при цьому Єдиний веб-портал органів виконавчої влади, який повинен бути основою інтегрованої системи “Електронний Уряд”, виконує переважно презентаційну та інформаційну функції. Головною причиною такого стану справ є невизначеність правових засад та організаційно-технічних рішень щодо забезпечення впровадження електронного урядування, відсутність єдиного підходу до застосування інструментів і механізмів організації та координації діяльності державних органів у сфері інформатизації. Визначено, що впровадження інформаційних технологій, рівень якого є незначним, у більшості випадків не має системного характеру. Державними органами проводиться робота з опрацювання документів переважно у паперовому вигляді, що значно ускладнює оперативне вжиття заходів для вирішення проблемних питань, своєчасне надання адміністративних послуг та довідкової інформації з питань діяльності державних органів. Основними причинами виникнення проблеми є: 1) використання державними органами подібної інформації, що міститься в різних базах даних і не пов'язана між собою; 2) відсутність ідентифікаторів, які пов’язують інформаційні об'єкти в різних базах даних; 3) використання електронних інформаційних систем та баз

даних державних органів, взаємодія яких з ресурсами інших державних органів не була передбачена під час їх проектування; 4) відсутність системи електронної взаємодії державних електронних інформаційних ресурсів, впровадження та функціонування якої забезпечує створення, використання, обмін та збереження інформації, що належить державі, відповідно до запитів і повноважень державних органів.

Метою концепції визначено формування підходів до створення, впровадження та функціонування системи електронної взаємодії державних електронних інформаційних ресурсів, що забезпечує передачу необхідних даних за запитами в автоматичному режимі, оновлення первинних даних у разі їх зміни, пошук та узагальнення необхідної інформації під час взаємодії державних органів. Основним завданням створення системи електронної взаємодії державних електронних інформаційних ресурсів визначено забезпечення: 1) автоматизованої інформаційної взаємодії електронних інформаційних систем та баз даних державних органів, у тому числі прямого автоматичного обміну інформацією та взаємоузгодження логічно пов’язаних та інформаційно залежних реєстрів; 2) автоматизованої міжвідомчої електронної взаємодії державних органів у процесі роботи, що проводиться із фізичними та юридичними особами з використанням єдиної, достовірної та несуперечливої інформації, що розміщена в електронних інформаційних системах та базах даних державних органів; 3) електронного обслуговування фізичних та юридичних осіб за принципом “єдиного вікна” із застосуванням електронного цифрового підпису; 4) безпеки інформації відповідно до вимог законодавства про захист інформації та персональних даних.

Прийнято *План заходів щодо реалізації Концепції створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів* (розпорядження Кабінету Міністрів України від 11.07.13 р. № 517-р.).

Положення про систему електронної взаємодії органів виконавчої влади, затверджено постановою Кабінету Міністрів України від 18.07.12 р. № 670, визначає загальні засади створення, впровадження та забезпечення функціонування системи електронної взаємодії органів виконавчої влади. Система призначена для автоматизації процесів створення, відправлення, передавання, одержання, оброблення, використання, зберігання, знищення електронних документів та копій паперових документів в електронному вигляді з використанням електронного цифрового підпису, які не містять інформацію з обмеженим доступом, та контролю за виконанням актів, протокольних рішень Кабінету Міністрів України та інших документів. До складу системи входять програмно-технічні комплекси (основний та резервний) та інші технічні засоби, що забезпечують створення, відправлення, передавання, одержання, обробка, використання, контроль за виконанням і зберіганням електронних документів, технологічне об’єднання функціонально пов’язаних складових системи, у тому числі систем автоматизації діловодства, що належать органам виконавчої влади, та комплексна система захисту інформації. Користувачами системи є відповідальні посадові особи Секретаріату Кабінету Міністрів України, міністерств, інших центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, місцевих органів виконавчої влади.

Порядок інформаційної взаємодії між кадастрами та інформаційними системами, затверджений постановою Кабінету Міністрів України від 03.06.13 р. № 483, визначає механізм обміну інформацією між кадастрами та інформаційними системами і перелік відомостей, обмін якими може здійснюватись у процесі такої взаємодії, та спрямований на: 1) формування єдиної картографічної основи для геоінформаційних систем; 2) забезпечення взаємного поповнення даними інформаційних систем; 3) забезпечення обов’язковості передачі геопросторових даних

до Державного земельного кадастру у випадках, передбачених законодавством; 4) забезпечення об’єктивності, достовірності та повноти відомостей у Державному земельному кадастрі; 5) визначення переліку відомостей, обмін якими може здійснюватись у процесі взаємодії між інформаційними системами; 6) запобігання дублюванню робіт з наповнення інформаційних систем; 7) уніфікацію інформаційних систем; 8) забезпечення геопросторовими даними органів державної влади, органів місцевого самоврядування, юридичних і фізичних осіб.

Прийнято низку відомчих нормативно-правових актів, що регулюють питання електронної взаємодії.

Порядок роботи з електронними документами через систему електронної взаємодії органів виконавчої влади з використанням електронного цифрового підпису, затверджений наказом Міністерства юстиції України від 01.11.12 р. № 1600/5, встановлює загальні правила створення, відправлення, передавання, одержання, оброблення, використання та зберігання електронних документів та електронних копій паперових документів, на які накладено електронний цифровий підпис, які не містять інформацію з обмеженим доступом, Секретаріатом Кабінету Міністрів України, міністерствами, іншими центральними органами виконавчої влади, Радою міністрів Автономної Республіки Крим, місцевими органами виконавчої влади через систему електронної взаємодії органів виконавчої влади.

Порядок передачі даних про юридичних осіб, зареєстрованих (легалізованих) відповідно до частини четвертої статті 3 Закону України “Про державну реєстрацію юридичних осіб та фізичних осіб-підприємців”, затверджений наказом Міністерства юстиції України від 01.07.13 р. № 1302/5, установлює механізм, форми та строки передачі даних, необхідних для державної реєстрації юридичних осіб та їх структурних підрозділів, зареєстрованих (легалізованих) відповідно до частини четвертої статті 3 Закону України “Про державну реєстрацію юридичних осіб та фізичних осіб-підприємців” крім громадських об’єднань, від Державної реєстраційної служби України, структурних підрозділів головних управлінь юстиції Міністерства юстиції України в Автономній Республіці Крим, в областях, містах Києві та Севастополі, районних, районних у містах, міських (міст обласного значення), міськрайонних, міжрайонних управлінь юстиції, що забезпечують реалізацію повноважень з питань реєстрації (легалізації) об'єднань громадян, інших громадських формувань, статутів, до державного реєстратора юридичних осіб та фізичних осіб-підприємців.

Наказом Міністерства юстиції України, Міністерства аграрної політики та продовольства України від 03.12.12 р. № 1779/5/748 затверджено деякі *питання забезпечення інформаційної взаємодії органу, що здійснює ведення Державного земельного кадастру, та органу державної реєстрації прав,* зокрема – Регламент надання інформації про зареєстровані земельні ділянки органу державної реєстрації прав та про зареєстровані права на земельні ділянки органу, що здійснює ведення Державного земельного кадастру, що визначає порядок та процедуру інформаційної взаємодії при наданні Укрдержреєстром інформації про зареєстровані речові права на земельні ділянки Держземагентству України та наданні Держземагентством України до Укрдержреєстру інформації про зареєстровані земельні ділянки, форми журналів обліку переданих та отриманих інформаційних файлів та Регламент надання на запити державного реєстратора прав на нерухоме майно інформації про земельні ділянки, який визначає порядок та процедуру надання Держземагентством України до Укрдержреєстру інформації про земельні ділянки на запити державного реєстратора прав на нерухоме майно, форми журналів обліку переданих та отриманих інформаційних файлів.

Порядок електронної взаємодії суб’єктів первинного фінансового моніторингу та Державної служби фінансового моніторингу України, затверджений наказом Міністерства фінансів України від 01.04.13 р. № 436, визначає механізми взаємодії між суб’єктами первинного фінансового моніторингу та Державною службою фінансового моніторингу України, а також вимоги та формати повідомлень електронного обміну щодо фінансового моніторингу.

Рішення Національної комісії з цінних паперів та фондового ринку *“Про внесення змін до Положення про подання адміністративних даних та інформації у вигляді електронних документів до Національної комісії з цінних паперів та фондового ринку”* від 19.03.13 р. № 367 щодо використання електронного цифрового підпису.

Нова редакція *Порядку надання послуг конфіденційного зв’язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям,* затверджена постановою Кабінету Міністрів України від 29.04.13 р. № 328, визначає механізм та умови надання операторами телекомунікацій послуг конфіденційного зв’язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам, організаціям у Національній системі конфіденційного зв’язку.

2.3.2. Правове регулювання надання адміністративних послуг в електронній формі

У Посланні Президента України зазначалося, що *“Одним із головних завдань модернізації державного управління в Україні є вдосконалення системи надання адміністративних послуг населенню. Створення ефективної системи надання фізичним і юридичним особам адміністративних послуг є головним напрямом реалізації в Україні принципу “сервісної” держави – держави для громадян. Втілення в життя ідеї “сервісної” держави насамперед вимагає кардинального перегляду відносин між управлінським апаратом і громадянином. Пріоритетом для державного службовця мають стати інтереси й потреби пересічного громадянина”* [1, с. 215].

Базовим документом, що регулює діяльність у сфері надання адміністративних послуг є *Закон України “Про адміністративні послуги”* [13], який визначає правові засади реалізації прав, свобод і законних інтересів фізичних та юридичних осіб у сфері надання адміністративних послуг.

На виконання зазначеного закону України органами державної влади розпочато формування законодавчої бази з надання адміністративних послуг, зокрема – в електронній формі.

Порядок ведення Реєстру адміністративних послуг [14], затверджений постановою Кабінету Міністрів України від 30.01.13 р. № 57, визначає механізм ведення Реєстру адміністративних послуг як єдиної інформаційної комп’ютерної бази даних про адміністративні послуги, що надаються відповідно до закону суб’єктами надання адміністративних послуг. До Реєстру вносяться відомості про: 1) суб’єкта надання адміністративної послуги; 2) назву адміністративної послуги; 3) розмір плати (адміністративний збір) за надання адміністративної послуги (у разі її надання на платній основі); 4) результат надання адміністративної послуги; 5) правові підстави для надання адміністративної послуги та встановлення розміру плати за її надання.

Порядок ведення Єдиного державного порталу адміністративних послуг [15], затверджений постановою Кабінету Міністрів України від 03.01.13 р. № 13, встановлює механізм ведення Єдиного державного порталу адміністративних послуг, що ведеться з метою забезпечення доступу суб’єктів звернення до інформації про адміністративні послуги з використанням Інтернету і є офіційним джерелом інформації про надання

адміністративних послуг. Визначається зміст інформаційної взаємодії суб’єктів надання адміністративних послуг. Портал забезпечує: 1) доступ суб’єктів звернення до інформації про адміністративні послуги, суб’єктів надання адміністративних послуг та центри надання адміністративних послуг; 2) доступність для завантаження і заповнення в електронній формі заяв та інших документів, необхідних для отримання адміністративних послуг; 3) можливість подання суб’єктами звернення заяв за допомогою засобів телекомунікаційного зв’язку; 4) можливість отримання суб’єктами звернення інформації про хід розгляду їх заяв; 5) можливість отримання суб’єктами звернення за допомогою засобів телекомунікаційного зв’язку результатів надання адміністративних послуг; 6) можливість здійснення суб’єктами звернення оплати за надання адміністративної послуги дистанційно, в електронній формі. На порталі розміщуються: 1) інформація про суб’єктів надання адміністративних послуг та центри надання адміністративних послуг; 2) Реєстр адміністративних послуг; 3) реквізити нормативно-правових актів з питань надання адміністративних послуг; 4) електронні форми заяв та інших документів, необхідних для отримання адміністративних послуг; 5) адреси електронної пошти суб’єктів надання адміністративних послуг для подання суб’єктами звернення заяв щодо надання адміністративних послуг за допомогою засобів телекомунікаційного зв’язку.

Вимоги до підготовки технологічної картки адміністративної послуги [16], затверджені постановою Кабінету Міністрів України від 30.01.13 р. № 44, якими визначено, що технологічна картка адміністративної послуги, які містять інформацію про порядок надання адміністративної послуги суб’єктом надання такої послуги, затверджується зазначеним суб’єктом для кожної адміністративної послуги, яку він надає. У технологічній картці зазначаються: 1) етапи опрацювання звернення про надання адміністративної послуги; 2) відповідальна посадова особа суб’єкта надання адміністративної послуги; 3) структурні підрозділи суб’єкта надання адміністративної послуги, відповідальні за етапи (дію, рішення); 4) строки виконання етапів (дії, рішення).

Примірне положення про центр надання адміністративних послуг [17], затверджене постановою Кабінету Міністрів України від 20.02.13 р. № 118, уточнює правовий статус центру надання адміністративних послуг та адміністраторів центрів.

Типовий порядок проведення конкурсу для надання супутніх послуг, пов’язаних з наданням адміністративних послуг, затверджений постановою Кабінету Міністрів України від 29.05.13 р. № 379, визначає загальну процедуру проведення конкурсу для надання супутніх послуг у приміщеннях, у яких розміщуються центри надання адміністративних послуг, та інших приміщеннях, у яких надаються адміністративні послуги.

Порядок та умови надання у 2013 році субвенції з державного бюджету місцевим бюджетам на фінансування заходів з реформування системи надання адміністративних послуг [18], затверджені постановою Кабінету Міністрів України від 27.03.13 р. № 204, спрямовані на здійснення заходів з реформування системи надання адміністративних послуг шляхом забезпечення функціонування у мм. Вінниці, Кіровограді, Києві, Луганську, Львові, Полтаві, Харкові та Хмельницькому центрів надання адміністративних послуг.

Порядок використання у 2013 році коштів державного бюджету, передбачених на утворення центрів надання адміністративних послуг [19], затверджений наказом Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України від 21.06.13 р. № 256, визначає механізм використання у 2013 році коштів державного бюджету (50000 тис. грн.), передбачених на утворення 676 центрів надання адміністративних послуг.

Концепція створення електронного сервісу “Електронний кабінет платника податків” [20] схвалена розпорядженням Кабінету Міністрів України від 05.12.12 р. № 1007-р з метою розширення переліку послуг, що надаються органами державної податкової служби платникам податків з використанням електронного сервісу, поліпшення якості обслуговування платників податків, забезпечення достовірності інформації, що подається платниками податків до органів державної податкової служби, підвищення рівня прозорості та відкритості діяльності органів державної податкової служби. Електронний сервіс створюється з метою надання платникам податків можливості працювати з органами державної податкової служби у режимі реального часу з використанням електронного цифрового підпису на безоплатній основі. Робота з електронним сервісом здійснюється з персонального комп’ютера платника податків, підключеного до Інтернету, шляхом автентифікації з використанням електронного цифрового підпису та авторизації такого платника.

Порядок надання органами Пенсійного фонду України послуг в електронному вигляді, затверджений постановою правління Пенсійного фонду України від 07.09.12 р. № 16-1, визначає механізм надання територіальними органами Пенсійного фонду України послуг в електронному вигляді, заснований на технологіях віддаленого доступу (веб-технологіях) та автоматизованої передачі і обробки інформації.

Передбачено, що надаються такі електронні послуги:

1. Реєстрація користувачів на веб-порталі.

2. Доступ до розміщеної на веб-порталі інформації:

а) для громадян та застрахованих осіб: 1) про порядок реєстрації громадян у базі даних веб-порталу; 2) про права, обов’язки та відповідальність одержувачів пенсійних та інших виплат, що здійснюються Пенсійним фондом України; 3) про порядок одержання та використання пенсійного посвідчення; 4) про умови, порядок призначення, перерахунку та виплати пенсій тощо; 5) зразки заяв, скарг, запитів на інформацію, інших документів, необхідних для призначення та перерахунку пенсій, переведення з одного виду пенсії на інший, зміни способу виплати пенсій, виплати допомоги на поховання тощо, включаючи можливість роздрукування або заповнення таких документів в електронному вигляді; 6) про права, обов’язки та відповідальність застрахованих осіб; 7) про порядок одержання та використання свідоцтва про загальнообов’язкове державне соціальне страхування; 8) про порядок організації прийому громадян у територіальних органах Пенсійного фонду України, у тому числі за принципом “єдиного вікна”;

б) для страхувальників, у тому числі фізичних осіб-підприємців та осіб, які забезпечують себе роботою самостійно: 1) про порядок реєстрації в базі даних веб-порталу; 2) про взяття на облік страхувальників у територіальних органах Пенсійного фонду України, їх права та обов’язки; 3) про умови нарахування та сплати єдиного внеску на загальнообов’язкове державне соціальне страхування та інших обов’язкових платежів; 4) про умови та порядок складення і подання звітності; 5) про порядок проведення територіальними органами Пенсійного фонду України перевірок, а також досудового оскарження рішень територіальних органів Пенсійного фонду України; 6) про іншу інформацію, пов’язану з регулюванням правових і фінансових відносин між територіальними органами Пенсійного фонду України, страхувальниками, у тому числі фізичними особами-підприємцями та особами, які забезпечують себе роботою самостійно; 7) зразки бланків, заяв, інших документів, необхідних для взяття на облік (зняття з обліку), складення та подання звітності, призначення та перерахунку пенсій тощо, включаючи можливість роздрукування або зчитування таких документів в електронному вигляді.

3. Доступ для громадян, застрахованих осіб та страхувальників, у тому числі фізичних осіб-підприємців та осіб, які забезпечують себе роботою самостійно, до інформації про стан відомостей про застраховану особу, пенсійних виплат, обробки звіту, поданого в електронному вигляді, стан взаєморозрахунків за зобов’язаннями платника (за умови підтвердження автентичності особи, що одержує доступ, шляхом реєстрації особи в базі даних веб-порталу).

4. Взаємодія громадян, застрахованих осіб та страхувальників, у тому числі фізичних осіб-підприємців та осіб, які забезпечують себе роботою самостійно, з територіальними органами Пенсійного фонду України з питань: 1) заповнення бланків заяви, скарги, запитів у електронному вигляді; 2) стану розгляду заяв, скарг, запитів, поданих в електронному вигляді; 3) подання запитів для підготовки в паперовому вигляді довідок, інших документів, які заявник одержує під час особистого звернення до територіальних органів Пенсійного фонду України; 4) попереднього запису на прийом у територіальному органі Пенсійного фонду України.

5. Одержання іншої необхідної довідкової інформації (місцезнаходження, телефони територіальних органів Пенсійного фонду України, новини тощо).

У Посланні Президента України зазначалося, що *“Пріоритетом подальшого реформування системи адміністративних послуг має стати запровадження механізму надання адміністративних послуг в електронній формі. Це створить для громадян можливість одержувати якісні послуги в будь-який час, максимально швидко і в зручний для них спосіб. Належне урядування на нинішньому етапі розвитку державного управління та сучасних інформаційних технологій неможливе без ефективних і дієвих інструментів електронного урядування, що не лише автоматизують класичні державні послуги, а й суттєво трансформують саму систему державного управління, сприяють посиленню його прозорості, зменшують потенційний корупційний складник”* [1, с. 216].

2.3.3. Правове регулювання електронного документа та електронного підпису

Постановою Кабінету Міністрів України від 27.05.13 р. № 371 внесено зміни до *Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу щодо послуг фіксування часу.*

Концепція реформування законодавства у сфері використання інфраструктури відкритих ключів та надання електронних довірчих послуг [21], затверджена наказом Міністерства юстиції України від 10.04.13 р. № 668/5, визначає сучасний стан системи електронного цифрового підпису в Україні, цілі, пріоритетні завдання та стратегічні напрями її розвитку, окреслює механізми реалізації концепції та очікувані результати. Реалізація концепції забезпечить: 1) визнання юридичної значимості отриманих кваліфікованих електронних довірчих послуг та забезпечення належної довіри фізичних та юридичних осіб до таких послуг, і, як наслідок, їх активне впровадження та використання; 2) використання всіх можливостей інфраструктури відкритих ключів, її стандартизацію та розбудову електронних довірчих послуг для здійснення ефективного електронного урядування, у тому числі надання адміністративних послуг в електронному вигляді, запровадження електронного нотаріату, масове використання електронного документообігу, подальший інтенсивний розвиток електронного судочинства, електронних закупівель, електронного архіву тощо; 3) визнання в Україні іноземних кваліфікованих сертифікатів відкритих ключів та кваліфікованого електронного підпису, що забезпечить активний розвиток транскордонного співробітництва та інтеграцію України у світовий електронний інформаційний простір.

Регламент роботи центрального засвідчувального органу, затверджений наказом Міністерства юстиції України від 29.01.13 р. № 183/5, визначає організаційно-методологічні та технологічні умови діяльності центрального засвідчувального органу під час обслуговування посилених сертифікатів відкритих ключів засвідчувальних центрів органів виконавчої влади або інших державних органів, центрів сертифікації ключів, акредитованих центрів сертифікації ключів, реєстрації, акредитації засвідчувальних центрів та центрів сертифікації ключів.

Вимоги до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису, затверджені наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 20.08.12 р. № 1236/5/453 та включають: 1. Вимоги до формату посиленого сертифіката відкритого ключа; 2. Вимоги до структури об’єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами; 3. Вимоги до формату списку відкликаних сертифікатів; 4. Вимоги до формату підписаних даних; 5. Вимоги до протоколу фіксування часу; 6. Вимоги до протоколу визначення статусу сертифіката.

2.3.4. Правове регулювання формування та використання державних електронних ресурсів

Завданням формування та використання державних електронних ресурсів у 2012 – 2013 рр. приділялася значна увага з боку органів державної влади. Достатньо потужно розвивалася у цей час система законодавчого забезпечення цих процесів.

Особлива увага приділялася правовому забезпеченню діяльності із створення державних інформаційних ресурсів у вигляді кадастрів, реєстрів, баз даних тощо. Так, прийнято низку нормативно-правових актів з формування:

Єдиного державного демографічного реєстру – 1) Закон України “Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус” від 20.11.12 р. № 5492-VI; 2) Постанова Кабінету Міністрів України “Деякі питання виконання Закону України “Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус” від 13.03.13 р. № 185 (дію постанови зупинено на підставі постанови Кабінету Міністрів України від 12.06.13 р. № 415);

Державного земельного кадастру: 1) Закон України “Про Державний земельний кадастр” від 07.07.11 р. № 3613-VI; 2) Порядок ведення Державного земельного кадастру, затверджений постановою Кабінету Міністрів України від 17.10.12 р. № 1051; 3) Порядок інформаційної взаємодії між кадастрами та інформаційними системами, затверджений постановою Кабінету Міністрів України від 03.06.13 р. № 483 (визначає механізм обміну інформацією між кадастрами та інформаційними системами і перелік відомостей, обмін якими може здійснюватись у процесі такої взаємодії, та спрямований на: формування єдиної картографічної основи для геоінформаційних систем; забезпечення взаємного поповнення даними інформаційних систем; забезпечення обов’язковості передачі геопросторових даних до Державного земельного кадастру у випадках, передбачених законодавством; забезпечення об’єктивності, достовірності та повноти відомостей у Державному земельному кадастрі; визначення переліку відомостей, обмін якими може здійснюватись у процесі взаємодії між інформаційними системами; запобігання дублюванню робіт з інформаційного наповнення інформаційних систем; уніфікацію інформаційних систем; забезпечення актуальними геопросторовими даними органів державної влади, органів місцевого самоврядування, юридичних і фізичних осіб); 4) постанову Кабінету Міністрів України “Про інформаційну взаємодію

органу, що здійснює ведення Державного земельного кадастру, та органу державної реєстрації прав” від 22.02.12 р. № 118, що затверджує: Порядок надання інформації про зареєстровані земельні ділянки органу державної реєстрації прав та про зареєстровані речові права на земельні ділянки органу, що здійснює ведення Державного земельного кадастру; Порядок надання органом, що здійснює ведення Державного земельного кадастру, органу державної реєстрації прав доступу до перегляду кадастрових карт (планів); 5) Порядок адміністрування Державного земельного кадастру, затверджений наказом Міністерства аграрної політики та продовольства України від 27.12.12 р. № 836 (визначає зміст та загальні вимоги до адміністрування Державного земельного кадастру – здійснення заходів щодо створення та супроводження програмного забезпечення Державного земельного кадастру; технічне й технологічне забезпечення Державного земельного кадастру; збереження та захист відомостей Державного земельного кадастру); 6) Вимоги до технічного і технологічного забезпечення виконавців (розробників) робіт із землеустрою, затверджені наказом Міністерства аграрної політики та продовольства України від 11.04.13 р. № 255; 7) наказ Міністерства юстиції України, Міністерства аграрної політики та продовольства України “Про деякі питання забезпечення інформаційної взаємодії органу, що здійснює ведення Державного земельного кадастру, та органу державної реєстрації прав” від 03.12.12 р. № 1779/5/748 (визначає порядок та процедуру інформаційної взаємодії при наданні Укрдержреєстром інформації про зареєстровані речові права на земельні ділянки Держземагентству України та наданні Держземагентством України до Укрдержреєстру інформації про зареєстровані земельні ділянки, форми журналів обліку переданих та отриманих інформаційних файлів); 8) Порядок проведення інвентаризації земель, затверджений постановою Кабінету Міністрів України від 23.05.12 р. № 513, що установлює вимоги до проведення інвентаризації земель під час здійснення землеустрою та складення за її результатами технічної документації із землеустрою щодо проведення інвентаризації земель, яка проводиться з метою: забезпечення ведення Державного земельного кадастру, здійснення контролю за використанням і охороною земель; визначення якісного стану земельних ділянок, їх меж, розміру, складу угідь; узгодження даних, отриманих у результаті проведення інвентаризації земель, з інформацією, що міститься у документах, які посвідчують право на земельну ділянку, та у Державному земельному кадастрі; прийняття за результатами інвентаризації земель Кабінетом Міністрів України, Радою міністрів Автономної Республіки Крим, місцевими держадміністраціями та органами місцевого самоврядування відповідних рішень; здійснення землеустрою тощо;

Центрального депозитарію цінних паперів – Положення про провадження депозитарної діяльності, затверджене Рішенням Національної комісії з цінних паперів та фондового ринку від 23.04.13 р. № 735);

єдиних державних реєстрів: 1) інститутів спільного інвестування (Положення про реєстрацію регламенту інститутів спільного інвестування та ведення Єдиного державного реєстру інститутів спільного інвестування, затверджене рішенням Національної комісії з цінних паперів та фондового ринку від 18.06.13 р. № 1047); 2) виробників спирту етилового, коньячного і плодового, спирту етилового ректифікованого виноградного, спирту етилового ректифікованого плодового, спирту-сирцю виноградного, спирту-сирцю плодового, алкогольних напоїв та тютюнових виробів (Інструкція з ведення Єдиного державного реєстру виробників спирту етилового, коньячного і плодового, спирту етилового ректифікованого виноградного, спирту етилового ректифікованого плодового, спирту-сирцю виноградного, спирту-

сирцю плодового, алкогольних напоїв та тютюнових виробів затверджена наказом Міністерства фінансів України від 30.11.12 р. № 1246); 3) тварин (Положення про Єдиний державний реєстр тварин, затверджене наказом Міністерства аграрної політики та продовольства України від 25.09.12 р. № 578);

державних реєстрів: 1) інвестиційних проектів та проектних (інвестиційних) пропозицій (Порядок ведення Державного реєстру інвестиційних проектів та проектних (інвестиційних) пропозицій, затверджений постановою Кабінету Міністрів України від 18.07.12 р. № 650); 2) технологій (Порядок реєстрації технологій та їх складових, що створені чи придбані за бюджетні кошти або створені чи придбані підприємствами державної форми власності, затверджений постановою Кабінету Міністрів України від 03.07.13 р. № 472); 3) виробників насіння і садивного матеріалу (Положення про Державний реєстр виробників насіння і садивного матеріалу затверджено наказом Міністерства аграрної політики та продовольства України від 20.02.13 р. № 115); 4) сертифікованих інженерів-землевпорядників (Форми документів, необхідних для видачі Держземагентством України кваліфікаційних сертифікатів інженерів-землевпорядників та включення інформації про них до Державного реєстру сертифікованих інженерів-землевпорядників затверджено наказом Міністерства аграрної політики та продовольства України від 28.11.12 р. № 738); 5) фізичних осіб-платників податків (Положення про реєстрацію фізичних осіб у Державному реєстрі фізичних осіб-платників податків, затверджене наказом Міністерства фінансів України від 06.11.12 р. № 1147); 6) речових прав на нерухоме майно (Закон України “Про внесення змін до деяких законодавчих актів України у зв’язку із запровадженням державної реєстрації речових прав на нерухоме майно та їх обтяжень” від 04.07.13 р. № 402-VII); 7) оцінювачів та суб’єктів оціночної діяльності (Порядок ведення Державного реєстру оцінювачів та суб’єктів оціночної діяльності, затверджений наказом Фонду державного майна України від 10.06.13 р. № 796); 8) нерухомих пам’яток України (Порядок обліку об’єктів культурної спадщини, затверджений наказом Міністерства культури України від 11.03.13 р. № 158); 9) медичної техніки та виробів медичного призначення (Порядок ведення Державного реєстру медичної техніки та виробів медичного призначення, затверджений наказом Міністерства охорони здоров’я України від 16.07.12 р. № 533); 10) селекційних досягнень у тваринництві (Положення про Державний реєстр селекційних досягнень у тваринництві, затверджене наказом Міністерства аграрної політики та продовольства України від 02.07.12 р. № 385);

єдиних реєстрів: 1) арбітражних керуючих (розпорядників майна, керуючих санацією, ліквідаторів) України (Порядок формування і ведення Єдиного реєстру арбітражних керуючих (розпорядників майна, керуючих санацією, ліквідаторів) України, затверджений наказом Міністерства юстиції України від 26.03.13 р. № 541/5); 2) для ведення автоматизованого обліку тракторів, самохідних шасі, самохідних сільськогосподарських, дорожньо-будівельних і меліоративних машин, техніки, інших механізмів (Положення про Єдиний реєстр для ведення автоматизованого обліку тракторів, самохідних шасі, самохідних сільськогосподарських, дорожньо-будівельних і меліоративних машин, сільськогосподарської техніки, інших механізмів затверджено наказом Міністерства аграрної політики та продовольства України від 22.01.13 р. № 29); 3) виданих ліцензій на провадження діяльності у сфері використання ядерної енергії (Порядок формування, ведення Єдиного реєстру виданих ліцензій на провадження діяльності у сфері використання ядерної енергії, затверджений наказом Державної інспекції ядерного регулювання України від 14.06.13 р. № 64-од); 4) електронний реєстр автобусних маршрутів (Порядок формування, затвердження та ведення реєстру

міжнародних, міжміських та приміських автобусних маршрутів загального користування, затверджений наказом Міністерства інфраструктури України від 20.05.13 р. № 305); 5) проектів, що реалізуються в Україні з використанням ресурсів міжнародних фінансових організацій та міжнародної технічної допомоги (Порядок ведення єдиного реєстру проектів, що реалізуються в Україні з використанням ресурсів міжнародних фінансових організацій та міжнародної технічної допомоги затверджений наказом Міністерства економічного розвитку і торгівлі України від 03.12.12 р. № 1378); 6) підприємств, щодо яких порушено провадження у справі про банкрутство (Положення про Єдиний реєстр підприємств, щодо яких порушено провадження у справі про банкрутство, затверджене наказом Міністерства юстиції України від 15.09.11 р.№ 3018/5 (в редакції наказу Міністерства юстиції України від 18.01.13 р. № 31/5));

реєстрів: 1) громадських об’єднань (Порядок ведення Реєстру громадських об’єднань та обміну відомостями між зазначеним Реєстром і Єдиним державним реєстром юридичних осіб та фізичних осіб-підприємців, затверджений постановою Кабінету Міністрів України від 19.12.12 р. № 1212); 2) символіки громадських об’єднань (Порядок реєстрації символіки громадського об’єднання, затверджений постановою Кабінету Міністрів України від 19.12.12 р. № 1209); 3) сертифікатів якості зерна та продуктів його переробки (Порядок ведення Реєстру сертифікатів якості зерна та продуктів його переробки, затверджений наказом Міністерства аграрної політики та продовольства України від 11.06.13 р. № 362); 4) сертифікатів відповідності послуг із зберігання зерна та продуктів його переробки (Порядок ведення Реєстру сертифікатів відповідності послуг із зберігання зерна та продуктів його переробки та надання відомостей з нього, затверджений наказом Міністерства аграрної політики та продовольства України від 11.06.13 р. № 361); 5) сертифікатів на насіння та/або садивний матеріал (Порядок ведення Реєстру сертифікатів на насіння та/або садивний матеріал затверджений наказом Міністерства аграрної політики та продовольства України від 26.03.13 р. № 222); 6) великих платників податків (Порядок формування Реєстру великих платників податків та Зміни до Порядку обліку платників податків і зборів затверджено наказом Міністерства фінансів України від 11.09.12 р. № 986); 7) неприбуткових установ та організацій (Положення про Реєстр неприбуткових установ та організацій, затверджений наказом Міністерства фінансів України від 24.01.13 р. № 37); 8) суб’єктів індустрії програмної продукції, які застосовують особливості оподаткування (Порядок ведення реєстру, форм реєстраційної заяви, заяви про анулювання реєстрації та свідоцтва про реєстрацію суб’єктів індустрії програмної продукції, які застосовують особливості оподаткування затверджений наказом Міністерства фінансів України від 14.01.13 р. № 12); 9) виданих та отриманих податкових накладних (Форма Реєстру виданих та отриманих податкових накладних та порядку його ведення, затверджено наказом Міністерства фінансів України від 17.12.12 р. № 1340); 10) місцевих запозичень та місцевих гарантій (Порядок ведення Реєстру місцевих запозичень та місцевих гарантій, затверджений наказом Міністерства фінансів України від 25.07.12 р. № 866); 11) морських портів України (Порядок ведення Реєстру морських портів України затверджений постановою Кабінету Міністрів України від 11.07.13 р. № 496); 12) гідротехнічних споруд морських портів України (Порядок ведення Реєстру гідротехнічних споруд морських портів України затверджений наказом Міністерства інфраструктури України від 18.02.13 р. № 91); 13) фінансових векселів (Закон України “Про внесення змін до Податкового кодексу України та деяких інших законів України щодо фінансових векселів” від 04.07.13 р. № 407-VII); 14) адміністративних послуг (Порядок ведення Реєстру адміністративних послуг, затверджений постановою Кабінету Міністрів України від 30.01.13 р. № 57); 15) учасників Фонду гарантування вкладів

фізичних осіб (Положення про порядок ведення реєстру учасників Фонду гарантування вкладів фізичних осіб затверджене рішенням виконавчої дирекції Фонду гарантування вкладів фізичних осіб від 12.07.12 р. № 7); 16) власників іменних цінних паперів (Ліцензійні умови провадження професійної діяльності на фондовому ринку (ринку цінних паперів) – депозитарної діяльності, а саме діяльності з ведення реєстру власників іменних цінних паперів, затверджені рішенням Національної комісії з цінних паперів та фондового ринку від 14.05.13 р. № 815; Положення про порядок дематеріалізації іменних цінних паперів, затверджене рішенням Національної комісії з цінних паперів та фондового ринку від 30.05.13 р. № 932); 17) аудиторських фірм та аудиторів, які можуть проводити аудиторські перевірки фінансових установ (Порядок ведення реєстру аудиторських фірм та аудиторів, які можуть проводити аудиторські перевірки фінансових установ, та визнання такими, що втратили чинність, деяких розпоряджень Державної комісії з регулювання ринків фінансових послуг України, затверджений розпорядженням Національної комісії, що здійснює державне регулювання у сфері ринків фінансових послуг від 26.02.13 р. № 640); 18) аудиторських фірм, які можуть проводити аудиторські перевірки професійних учасників ринку цінних паперів (Порядок ведення реєстру аудиторських фірм, які можуть проводити аудиторські перевірки професійних учасників ринку цінних паперів затверджений рішенням Національної комісії з цінних паперів та фондового ринку від 25.10.12 р. № 1519); 19) іпотечного покриття звичайних іпотечних облігацій (Положення про іпотечне покриття звичайних іпотечних облігацій, порядок ведення реєстру іпотечного покриття та управління іпотечним покриттям звичайних іпотечних облігацій, затверджене рішенням Національної комісії з цінних паперів та фондового ринку від 27.12.12 р. № 1902); 20) сертифікатів типу транспортних засобів та обладнання і виданих виробниками сертифікатів відповідності транспортних засобів або обладнання (Порядок ведення реєстру сертифікатів типу транспортних засобів та обладнання і виданих виробниками сертифікатів відповідності транспортних засобів або обладнання, затверджений наказом Міністерства інфраструктури України від 17.08.12 р. № 521); 21) страхових агентів, які мають право здійснювати посередницьку діяльність з обов’язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів (Порядок реєстрації страхових агентів, які мають право здійснювати посередницьку діяльність з обов’язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів, у Моторному (транспортному) страховому бюро України, затверджений розпорядженням Національної комісії, що здійснює державне регулювання у сфері ринків фінансових послуг, від 18.04.13 р. № 1270); 22) суб’єктів господарювання, які здійснюють операції з дорогоцінними металами і дорогоцінним камінням (Порядок обліку, створення та ведення реєстру суб'єктів господарювання, які здійснюють операції з дорогоцінними металами і дорогоцінним камінням, затверджений наказом Міністерства фінансів України від 08.04.13 р. № 465); 23) Довідково-інформаційний реєстр перекладачів (Порядок ведення Державною міграційною службою України Довідково-інформаційного реєстру перекладачів, затверджений наказом Міністерства внутрішніх справ України від 11.03.13 р. № 228); 24) індустріальних (промислових) парків (Порядок прийняття рішення про включення індустріального (промислового) парку до Реєстру індустріальних (промислових) парків, затверджений постановою Кабінету Міністрів України від 16.01.13 р. № 216); 25) проектів наукових парків, реалізація яких потребує державної підтримки (Порядок державної реєстрації проектів наукових парків, реалізація яких потребує державної підтримки, затверджений постановою Кабінету Міністрів України від 14.11.12 р. № 1101); 26) оптово-відпускних цін на лікарські засоби і вироби медичного

призначення (Положення про реєстр оптово-відпускних цін на лікарські засоби і вироби медичного призначення, порядок внесення до нього змін та форм заяв про декларування зміни оптово-відпускної ціни на лікарський засіб або виріб медичного призначення, затверджене наказом Міністерства охорони здоров’я України від 07.09.12 р. № 705); 27) Електронний реєстр пацієнтів (Положення про електронний реєстр пацієнтів, затверджене постановою Кабінету Міністрів України від 06.06.12 р. № 546); 28) Електронний реєстр пацієнтів Вінницької, Дніпропетровської, Донецької областей та м. Києва (Порядок ведення електронного реєстру пацієнтів Вінницької, Дніпропетровської, Донецької областей та м. Києва, затверджений наказом Міністерства охорони здоров’я України від 30.08.12 р. № 666); 29) хворих на туберкульоз (Порядок ведення реєстру хворих на туберкульоз, затверджений наказом Міністерства охорони здоров’я України від 19.10.12 р. № 818); 30) суб’єктів господарювання, які здійснюють оптову торгівлю спиртом коньячним і плодовим на підставі ліцензії на виробництво коньяку та алкогольних напоїв за коньячною технологією (Інструкція з ведення та використання даних Реєстру суб’єктів господарювання, які здійснюють оптову торгівлю спиртом коньячним і плодовим на підставі ліцензії на виробництво коньяку та алкогольних напоїв за коньячною технологією, затверджена наказом Міністерства фінансів України від 28.11.12 р. № 1231); 31) операторів, провайдерів телекомунікацій (Порядок ведення реєстру операторів, провайдерів телекомунікацій затверджено рішенням Національної комісії, що здійснює державне регулювання у сфері зв’язку та інформатизації від 01.11.12 р. № 560);

єдиної бази даних звітів про оцінку для цілей оподаткування та нарахування і сплати інших обов’язкових платежів, які справляються відповідно до законодавства (Порядок ведення єдиної бази даних звітів про оцінку для цілей оподаткування та нарахування і сплати інших обов’язкових платежів, які справляються відповідно до законодавства, затверджений наказом Фонду державного майна України від 10.06.13 р. № 795);

бази даних про вкладників (Правила формування та ведення баз даних про вкладників, затверджені рішенням виконавчої дирекції Фонду гарантування вкладів фізичних осіб від 09.07.12 р. № 3).

Висновки.

1. Протягом 2012 – 2013 рр. проведено суттєву модернізацію законодавчої бази з формування та реалізації національної політики з розвитку інформаційного суспільства, інформатизації та електронного урядування, що дозволяє реалізовувати значну кількість завдань подальшого соціально-економічного та політичного розвитку України, гармонійного входження до світового інформаційного співтовариства.

2. Разом з тим, зазначена законодавча база має значну кількість невизначеностей та протиріч. Це виражається, з одного боку, у неадекватно великій кількості регулюючих норм і інститутів, значному адміністративному і податковому тиску, неприйнятно високій кількості зобов’язань, покладених на суб’єкти діяльності у цих сферах. Численні обмеження перешкоджають реалізації прав приватної власності та підприємницької ініціативи, тобто саме тих правових норм, що визначають зростання добробуту. Держава, займаючи провідну позицію в регулюванні відносин з розвитку інформаційного суспільства, інформатизації та електронного урядування, демонструє сьогодні низьку спроможність ефективно справлятися з наданими повноваженнями.

3. Нормативні положення законодавства, які дуже часто коригуються, виявляються ще більш суперечливими, розмитими і неузгодженими з реальними потребами розвитку

інформаційного суспільства, інформатизації та електронного урядування, ніж правові норми, які діяли раніше. Деякі загальноекономічні і суспільно значущі правові акти розглядаються і приймаються без урахування специфіки ІКТ-діяльності. Це не тільки негативно впливає на розвиток інформаційного суспільства, інформатизації та електронного урядування, а й породжує необхідність створення значного масиву відомчих (таких, що роз’яснюють, уточнюють тощо), недостатньо узгоджених між собою документів. У багатьох соціально-економічних і загальногромадянських нормативних документах інформатизаційний блок просто відсутній. Це стосується навіть тих актів, які безпосередньо впливають на розвиток інформаційного суспільства, інформатизації та електронного урядування.

4. Для вітчизняного законодавства характерний значний розрив у часі між ухваленням нормативно-правових актів і подальшою розробкою конкретних нормативів, процедур, механізмів їх реалізації.

Перспективи щодо подальших досліджень. Подальші дослідження, на нашу думку, необхідно зосередити на приведення у відповідність наведених нормативно-правових актів положенням проекту Угоди про Асоціацію між Україною, з однієї сторони, та Європейським Союзом і його державами-членами, з іншої сторони.

Використана література

1. Про внутрішнє та зовнішнє становище України в 2013 році : щорічне Послання Президента України до Верховної Ради України. – К. : НІСД, 2013. – С. 50.

2. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Розпорядження Кабінету Міністрів України від 15.05.13 р. № 386-р // Офіційний вісник України. – 2013 р. – № 44. – Ст. 1581.

3. Програма економічних реформ на 2010 – 2014 роки “Заможне суспільство, конкурентоспроможна економіка, ефективна держава” : Указ Президента України від 12.03.13 р. № 128/2012 // Офіційний вісник України. – 2013 р. – № 21. – Ст. 700.

4. Про внесення змін до Закону України “Про особливості забезпечення відкритості, прозорості та демократичності виборів народних депутатів України 28 жовтня 2012 року”: Закон України від 02.10.12 р. № 5401-VI // Офіційний вісник України. – 2012 р. – № 77. – Ст. 3099.

5. Про внесення змін до деяких законодавчих актів України щодо функціонування платіжних систем та розвитку безготівкових розрахунків : Закон України від 18.09.12 р. № 5284-VI // Офіційний вісник України. – 2012 р. – № 79. – Ст. 3191.

6. Про схвалення Концепції створення єдиної інформаційно-аналітичної системи управління міграційними процесами : Розпорядження Кабінету Міністрів України від 07.11.12 р. № 870-р // Офіційний вісник України. – 2012 р. – № 85. – Ст. 3469.

7. Про внесення змін до Закону України “Про захист персональних даних” : Закон України від 20.11.12 р. № 5491-VI // Офіційний вісник України. – 2012 р. – № 97. – Ст. 3899.

8. Про внесення змін до Закону України “Про захист персональних даних” : Закон України від 20.11.12 р. № 5491-VI // Офіційний вісник України. – 2012 р. – № 97. – Ст. 2046.

9. Про внесення змін до деяких наказів Міністерства юстиції України щодо удосконалення правового регулювання у сфері захисту персональних даних : наказ Міністерства юстиції України від 22.07.13 р. № 1466/5 // Офіційний вісник України. – 2013 р. – № 58. – Ст. 2105.

10. Про державну підтримку розвитку індустрії програмної продукції : Закон України від 16.10.12 р. № 5450-VI // Офіційний вісник України. – 2012 р. – № 85. – Ст. 3448.

11. Про внесення змін до Закону України “Про державне регулювання діяльності у сфері трансферу технологій” : Закон України від 02.10.12 р. № 5407-VI // Офіційний вісник України. – 2012 р. – № 85. – Ст. 3431.

12. Про схвалення Концепції створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів : Розпорядження Кабінету Міністрів України від 05.09.12 р. № 634-р // Офіційний вісник України. – 2012 р. – № 67. – Ст. 2753.

13. Про адміністративні послуги : Закон України від 06.11.12 р. № 5203-VI // Офіційний вісник України. – 2012 р. – № 76. – Ст. 3067.

14. Про затвердження Порядку ведення Реєстру адміністративних послуг : Постанова Кабінету Міністрів України від 30.01.13 р. № 57 // Офіційний вісник України. – 2013 р. – № 9. – Ст. 339.

15. Про затвердження Порядку ведення Єдиного державного порталу адміністративних послуг : Постанова Кабінету Міністрів України від 03.01.13 р. № 13 // Офіційний вісник України. – 2013 р. – № 4. – Ст. 109.

16. Про затвердження вимог до підготовки технологічної картки адміністративної послуги : Постанова Кабінету Міністрів України від 30 січня 2013 р. № 44 // Офіційний вісник України. – 2013 р. – № 9. – Ст. 333.

17. Про затвердження Примірного положення про центр надання адміністративних послуг : Постанова Кабінету Міністрів України від 20.02.13 р. № 118 // Офіційний вісник України. – 2013 р. – № 16. – Ст. 557.

18. Про затвердження Порядку та умов надання у 2013 році субвенції з державного бюджету місцевим бюджетам на фінансування заходів з реформування системи надання адміністративних послуг : Постанова Кабінету Міністрів України від 27.03.13 р. № 204 // Офіційний вісник України. – 2013 р. – № 26. – Ст. 864.

19. Про затвердження Порядку використання у 2013 році коштів державного бюджету, передбачених на утворення центрів надання адміністративних послуг : наказ Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України від 21.06.13 р. № 256 // Офіційний вісник України. – 2013 р. – № 53. – Ст. 1955.

20. Питання створення та запровадження електронного сервісу “Електронний кабінет платника податків” : Розпорядження Кабінету Міністрів України від 05.12.12 р. № 1007-р // Офіційний вісник України. – 2012 р. – № 93. – Ст. 3797.

21. Про затвердження Концепції реформування законодавства у сфері використання інфраструктури відкритих ключів та надання електронних довірчих послуг : наказ Міністерства юстиції України від 10.04.13 р. № 668/5. – Режим доступу : //www.minjust.gov.ua

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 339.1:342.721:681.302

БРИЖКО В.М., *кандидат юридичних наук (Doctor of Philosophy), с.н.с.,*
Заслужений винахідник республіки,
співавтор Законів України “Про захист персональних даних”
від 13 травня 2006 р. № 2618 та від 1 червня 2010 р. № 2297-VI.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ: РЕАЛІЇ ТА ПРАКТИКА СУЧАСНОСТІ[1]

Анотація. *Про історію, хронологію розробки та узгодження, а також про питання до застосування Закону України “Про захист персональних даних”. Пропозиції щодо створення національної цілісної системи захисту персональних даних.*

Ключові слова: *інформаційне право, персональні дані, захист персональних даних.*

Аннотация. *Об истории, хронологии разработки и согласования, а также о вопросах применения Закона Украины “О защите персональных данных”. Предложения по созданию национальной целостной системы защиты персональных данных.*

Ключевые слова: *информационное право, персональные данные, защита персональных данных.*

Summary. *About history and chronology of development and mutual approval, as well as about the questions of application of Law of Ukraine “About the personal data protection”. Suggestions on creation of the national integral system of personal data protection.*

Keywords: *information law, personal data, personal data protection.*

Вступ. Нормативне вирішення проблеми захисту прав людини починає свою історію у 1215 році, коли англійський король Іоанн Безземельний під тиском баронів підписав Велику хартію вільностей (“Magna Carta”) [1, с. 13-19]. Значення Хартії полягає у тому, що вона була першим прецедентом обмеження деспотичної влади монарха, щоправда лише відносно феодалів і рицарства; про права простих людей мови не було.

Через 50 років Генріх ІІІ, після чергової доповіді міністрів про безлади на вулицях Лондона, промовив: *“Ну-ка, давайте сюда главных крикунов. Пусть дерутся они сами, у меня на глазах, а не стравливают толпы”*. У результаті монарх був вимушений присягнути першому парламенту (від фр. – “базікати”, “говорити”), хоча діяльність останнього довгий час мало сприяла забезпеченню прав людини. Про продуктивність та робочу атмосферу англійського парламенту тих часів красномовно свідчить виказана депутатом Ісаком Ньютоном лише єдина за п’ять років фраза: *“Закройте окно, дует”*. Потрібно було ще декілька століть, щоб від декларативних тверджень перейти до конкретних нормативних актів, що регламентують недоторканність особи.

В цьому аспекті історія ХХ сторіччя характерна активнішим просуванням по шляху досягнення індивідуальних свобод. Зараз немає такої демократичної конституції в світі, яка б не мала в своєму законодавстві природних, невід’ємних прав на особисту свободу людини.

Важливим при цьому є те, що особиста свобода невід’ємна від небезпеки. І справа по обмеженню свободи є справою зміцнення безпеки людини, суспільства та держави. Захист, хочемо ми цього чи ні, це обмеження, встановлені законом. Обмеження з боку правової держави мають сенс лише тоді, коли цими обмеженнями переслідується мета поставити перешкоди на шляху довільного поводження з правами людини.

[1] До матеріалів виступу на “круглому столі” на тему: *“Особливості захисту персональних даних у сучасному кіберпросторі: правові та техніко-технологічні аспекти” (Київ, 10 жовтня 2013 р.).* – Національний інститут стратегічних досліджень.

Міжнародне визнання права на захист приватної сфери особистого і сімейного життя, що передбачає захист особистих відомостей про людину, вперше увійшло до переліку фундаментальних прав і свобод у Загальній декларації прав людини, прийнятій Генеральною Асамблею ООН 10 грудня 1948 року. Стаття 12 Декларації проголосила: *“Ніхто не може зазнавати безпідставного втручання у його особисте життя, безпідставного посягання на недоторканність його житла, тайну його кореспонденції або на його честь і репутацію. Кожна людина має право на захист законом від такого втручання або таких посягань”* [1, с. 22-25] .

У 1970-х відбувся початок активного застосування інформаційно-комп’ютерних технологій, телекомунікаційних мереж та формування різних за напрямами електронних накопичувачів інформації – баз даних. Це поступово трансформувало європейське розуміння поняття “право на недоторканність особистого та сімейного життя” у бік застосування заходів “захисту права на інформаційний суверенітет особи”, зокрема, права людини визначати ким, коли, з якою метою та яким чином інформація про неї буде використовуватися іншими особами. Ця трансформація визначила зародження так званого “Інформаційного суспільства”, а у класичному праві – появу нової юридичної галузі під назвою “Інформаційне право”[2]. При цьому, забезпечення прав людини, зокрема у телекомунікація, отримало визначення у вигляді терміну “захист персональних даних”. Причини зазначеного полягають в тому, що з початку застосування новітніх технологій та мереж розпорошені по різних відомчих “відсіках” та у багатьох випадках анонімні інформаційні сліди життя людини стали отримувати електронну персоналізацію. Комп’ютери, програми, телекомунікації, бази даних перетворили тривалий і трудомісткий процес пошуку відомостей у високотехнологічну індустрію збирання особистої інформації з різних джерел, її обробки та поширення у визначених цілях – політичних, економічних, фінансових, кримінальних тощо. Інформація про особу, її здібності, наміри та вчинки, особисте чи сімейне життя, зміст розмов та стосунків, майновий стан, медичні відомості, особисте теле- чи відеоменю, результати вибору книг у бібліотеці, газет чи журналів, зміст файлів на комп’ютерах та на автовідповідачах, відомості щодо спілкування за допомогою засобів нового електронного середовища (е-середовища) – всі ці та багато інших даних за бажанням можна поєднати, проаналізувати та інтерпретувати (створити навіть бажаний “негативний портрет” особи) так, що людина, модель її поведінки виглядатиме “прозорою” в усіх своїх якостях та проявах.

У зв’язку з вищезазначеним у європейських країнах почали приймати закони про захист персональних даних (див. Таблицю 1). Головна їх мета бачилася у вирішенні проблеми забезпечення приватного життя людини згідно з принципами Європейської конвенції “Про захист прав людини та основоположних свобод” (Рим, 04.XI.1950 р.) [1, с. 34-44]. Відповідно до статті 8 Європейської конвенції від 1950 р.: *“Кожен має право на повагу до його приватного і сімейного життя, до житла і до таємниці кореспонденції. Органи державної влади не можуть втручатися у здійснення цього права інакше ніж згідно із законом і коли це необхідно в демократичному суспільстві в інтересах національної і громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням чи злочинам, для захисту здоров’я чи моралі або з метою захисту прав і свобод інших осіб”*.

[2] У 1994 році група фахівців під керівництвом Мартина Бангемана – *Комісара Ради Європи із захисту персональних даних* (на той час), здійснила аналіз розвитку ринкових відносин. Звіт групи є, так мовити, маніфестом побудови Інформаційного суспільства і мав назву: *“Європа і глобальне Інформаційне суспільство. Рекомендації Європейській Раді”* [2, с. 189-192].

Наприкінці 1970-х років суперечність між все більш активним впровадженням засобів автоматизованої обробки даних та їх поширенням у телекомунікаційних мережах, зловживання при використанні персональних даних, потреба у впорядкуванні експортно-імпортних операцій призвели до необхідності розробки міжнародно-правового акту, який мав забезпечити уніфіковане впорядкування інформаційних відносин у сфері захисту персональних даних. Комітетом Ради Європи з питань захисту даних були сформульовані принципи захисту від неправомірного збирання, обробки, зберігання та поширення персональних даних. Ці основоположні принципи 28 січня 1981 року отримали закріплення у першій міжнародній угоді світового рівня – Конвенції Ради Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” (відома як Конвенція РЄ № 108, згідно з порядком у серії Європейських договорів)[3].

З того часу захист персональних даних остаточно виокремився у самостійний вид діяльності та сферу нормативно-правового упорядкування інформаційних відносин.

Таблиця 1

Країна	**Дата підписання Конвенції РЄ № 108**	**Назва базового закону**	**Дата прийняття закону**	**Реєстрація баз персональних даних**	**Реєстрація ручної обробки даних**	**Ліцензування діяльності щодо даних**
Австрія	28.01.81 р.	Про захист даних	01.01.80 р. дод. 2000 р.	усі дані	так	деякі дані
Бельгія	07.05.82 р.	Про захист даних	08.12.92 р.	усі дані	так	деякі дані
Болгарія	02.06.98 р.	+				
Великобританія	14.05.81 р.	Про захист даних	12.07.84 р.	усі дані	так	деякі дані
Греція	17.02.83 р.	Про захист осіб у зв’язку з обробкою даних	09.11.87 р. дод. 1997 р.	усі дані	так	деякі дані
Данія	28.01.81 р.	Про захист даних Про реєстри даних	08.06.82 р. 2000 р.	деякі дані	так	деякі дані
Ірландія	18.12.86 р.	Про захист даних	13.07.88 р.	деякі дані	ні	ні
Ісландія	27.09.82 р.	Про захист персональних даних	05.06.81 р. дод. 2000 р.	усі дані	так	усі дані
Іспанія	28.01.82 р.	Про регулювання автоматизованої обробки персональних даних	29.10.92 р.	усі дані	ні	деякі дані
Італія	02.02.83 р.	Про захист осіб у зв’язку з обробкою персональних даних	01.02.92 р.	деякі дані	так	деякі дані
Латвія	31.10.00 р.	Про охорону даних фізичних осіб	2000 р.			

[3] Матеріали Конвенції РЄ № 108 та Додаткового до неї протоколу див. у розділі журналу “Європейські правові стандарти”. Переклад з англ. укр. мовою здійснений авторами Закону України “Про захист персональних даних”, і офіційно засвідчений МЗС України від 01.07.02 р.

Литва	+	Про правовий захист особистих даних	11.06.96 р.			
Люксембург	28.01.81 р.	Про використання персональних даних, які обробляються у комп’ютері	31.03.79 р.	усі дані	ні	ні
Молдова	04.05.98 р.	+	2000 р.			
Нідерланди	21.01.88 р.	Про захист даних	28.12.88 р. дод. 2000 р.	деякі дані	так	ні
Німеччина	28.01.81 р.	Про подальший розвиток обробки даних	20.12.90 р. дод. 1997 р.	усі дані	так	деякі дані
Норвегія	13.03.81 р.	Про реєстраторів персональних даних	09.06.82 р.	деякі дані	так	деякі дані
Польща	21.04.99 р.	+	+			
Португалія	14.05.81 р.	Про захист персональних даних	29.04.91 р.	усі дані	ні	усі дані
Росія	+	Про персональні дані	27.06.07 р.	усі дані	так	
Румунія	18.03.97 р.	+	+			
Словаччина	14.04.00 р.	+	+			
Словенія	23.11.93 р.	+	+			
Туреччина	28.01.81 р.	+	+			
Угорщина	13.05.93 р.	Про захист даних та доступ до інформації, яка має суспільний інтерес	11.1992 р.	усі дані	так	деякі дані
Фінляндія	10.04.91 р.	Про файли персональних даних	04.02.87 р., дод. 1999 р.	деякі дані	так	деякі дані
Франція	28.01.81 р.	Про інформатику, картотеки та свободи	06.01.78 р.	деякі дані	так	деякі дані
Швеція	28.01.81 р.	Про захист даних	13.05.73 р. дод. 1988 та 1999 рр.	деякі дані	ні	деякі дані
Швейцарія	02.10.97 р.	Про захист даних	19.06.92 р.	деякі дані	так	ні
Естонія	24.01.00 р.	Про особисті документи	2002 р.			

Примітка: + – базовий закон про захист персональних даних, що відповідає положенням європейських стандартів, прийнятий. Інших відомостей не визначено.

Згідно з Конвенцією РЄ № 108 держави, які підписали цей документ, зобов’язуються керуватися її положеннями стосовно персональних даних, що підлягають чи не підлягають автоматизованій обробці, як у суспільному, так і приватному секторах.

Кожна держава-член Ради Європи коригує національне законодавство у частині втілення її основних принципів та поставленої мети – забезпечення на її території поваги до прав та свобод кожної людини незалежно від її громадянства або місця проживання.

Конвенція РЄ № 108 допускає обмеження у правах фізичних осіб, якщо це стосується державної чи громадської безпеки, фінансових інтересів, боротьби зі злочинністю, захисту прав та основоположних свобод інших людей.

Згідно з Конвенцією РЄ № 108 кожна держава-член зобов’язана призначити Уповноважений орган нагляду та направити відповідне повідомлення Генеральному секретарю Ради Європи. Завдання Уповноваженого передбачають створення належного організаційно-правового упорядкування відносин для захисту персональних даних у країні.

Десятиріччя, що минули з часу прийняття Конвенції РЄ № 108, показали, що інститут Уповноваженого з питань захисту персональних даних не лише зберігся, а й дістав поширення у всіх західноєвропейських країнах. Нині уповноважені органи з питань захисту персональних даних діють більше ніж у двадцяти країнах Європи. Їх діяльність свідчить, що вони є ефективним засобом, здатним забезпечити баланс інтересів людини, суспільства і держави. У Німеччині, наприклад, за участі цього інституту вдалося оформити право на захист персональних даних як основне право фізичних осіб і розглядати його як конституційну норму.

В інтересах подальшої деталізації та уніфікації національних законодавств Консультативний комітет Ради Європи у питаннях захисту персональних даних заохочує секторний (галузевий) підхід, наполегливо дотримується та намагається розвивати загальні правила щодо окремих аспектів їх обробки, продовжує удосконалювати положення Конвенції РЄ № 108 стосовно проблем європейської інтеграції. У цьому плані Кабінет Міністрів Ради Європи затвердив Поправки від 15.06.99 р. щодо приєднання до неї держав Європейського Союзу. Вони передбачають застосування положень Конвенції РЄ № 108 до даних, які стосуються груп осіб, асоціацій, фундацій, компаній, корпорацій та будь-яких інших установ, що безпосередньо чи опосередковано формуються з окремих осіб, незалежно від того, мають такі установи правосуб’єктність чи ні.

Щоб процеси торгівлі не потерпали від європейських вимог щодо захисту даних, країни Сходу (Австралія, Гонконг, Нова Зеландія), Південної Африки, Америки (Канада) стали також приймати відповідні закони з питань захисту даних. Близько 40 країн світу мають закони з питань персональних даних. Але інформаційне законодавство багатьох з них має суттєві недоліки. Навіть у найбільш демократичних країнах поширеним є несанкціоноване прослуховування та інші порушення законів, що визначають порядок доступу до даних, що розповсюджуються за допомогою електронних каналів зв’язку [3].

Як раніше зазначалося, Конвенція РЄ № 108 є першим та головним документом, який визначає основоположні, уніфіковані принципи створення національного законодавства країн світу у сфері захисту персональних даних.

Через 14 років, у 1995 р., Європейський парламент та Рада Європейського Союзу запровадили першу в ЄС законодавчу ініціативу щодо персональних даних – Директиву 95/46/ЄС “Про захист осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних” від 24.10.95 р.[4] Згідно з директивою зміст європейської моделі захисту персональних даних можна визначити як “забезпечення єдиними механізмами виконання”.

Європейський Союз визначає, що прагне до того, щоб суб’єкти персональних даних мали визначені права і реальну можливість звернутися до посадової особи або органу, що зобов’язаний вжити дії для їх захисту. Кожній країні, що є учасником Євросоюзу, також як і в Конвенції РЄ № 108, рекомендовано створити уповноважений орган (або органи) із захисту персональних даних. Зазначене має на меті створення умов уніфікованого рівня організації та контролю за діяльністю у сфері захисту персональних даних.

[4] Матеріали Директиви 95/46/ЄС див. у розділі журналу “Європейські правові стандарти”.

У 1997 році був затверджений наступний документ – Директива 97/66/ЄС Європарламенту і Ради Євросоюзу від 15.12.97 р. “Про обробку персональних даних і захист прав людини в телекомунікаційному секторі” [1, с. 337-344]. Проте, після подій у Нью-Йорку 11.09.01 р. у рамках антитерористичної кампанії Європейський парламент 30.05.02 р. скасував її положення.

Стосовно Інтернет-відносин, то у листопаді 2003 р. Європейський суд дав чітке пояснення: *“згадування конкретних людей у розташовуваних на Інтернет-сайтах матеріалах, публікація їх імен чи будь-якої іншої конкретної інформації про них, є операцією з персональними даними. Стосовно подібних дій повинна застосовуватися Директива 95/46/ЄС із захисту персональних даних”.*

У плані основних напрямів та тенденцій із забезпечення інформаційної безпеки спостерігається наступне:

- вводяться е-паспорти, за допомогою яких (завдяки чипам) стає можливим відслідковувати (із супутника) будь-кого і будь-де;
- обмежуються (у багатьох країнах) можливості самозахисту за допомогою криптографії. Вводиться обов’язковість надання “ключів” дешифрування відповідним службам;
- має місце широка практика об’єднання БД на основі ідентифікаційних номерів: податкової, медичної, соціальної інформації, відомостей про майно, родинний стан, особисті таємниці, засіб життя тощо дозволяє створити вичерпне досьє (навіть негативне), доступне необмеженому колу осіб;
- активно використовуються системи відео спостереження в умовах відсутності зацікавленості урядів у прийнятті конкретних законів. Системи щодо порядку оповіщення громадян про спостереження, збереження записів і доступу до них не створено.
- обмежується можливість анонімності при використанні коштів комунікації (якщо не можна ідентифікувати суб’єкта відправленої транзакції);
- застосовуються технологій перегляду змісту е-пошти під час відсутності законодавчих обмежень. Хоча вважається, що е-пошта і дані, що містяться у комп’ютері, така ж особиста недоторканна сфера, як житло;
- ведуться генетичні дослідження. Тестування і створення БД ДНК вже є реалією. Небезпека – можливість робити генні висновки про риси особи і складання характеристики. При цьому медичні дані дорого коштують (щодо діагнозів захворювань, відомості про аналізи, запропоновані рецепти тощо, навіть про лікарів, що обслуговують);
- практично боротьба зі “спамом”, “сокетом” (рекламні розсилання) і “троянським конем” (викачуванням інформації) має номінальний зміст. Продаж персональних даних за допомогою “спаму” – звичайна практика. Програми-шпигуни запитують анкетні дані та створюють досьє користувачів Інтернету, а потім це несанкціоновано використовується в особистих, політичних чи економічних інтересах.

Постановка проблеми. Відповідно до статті 32 Конституції України 1996 р.: *“Ніхто не може зазнавати втручання в його особисте життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини”.*

У 2010 році Президент України Віктор Янукович підписав Закон “Про захист персональних даних” (№ 2297-VI), який Верховна Рада прийняла 1 червня [4].

Аналіз багатьох публікацій (див. наведену літературу, посилання на джерела та Інтернет за ключовими словами) свідчить про те, що проблематика захисту персональних даних викликає занепокоєння у значної кількості людей у зв’язку з наявністю загальновизнаного європейськими правовими стандартами права на недоторканність приватного життя, з одного боку, а з іншого –поширенню у житті реалій несанкціонованого використання персональних даних не уповноваженими на це особами. Іншими словами, міжнародне право та світові стандарти – є, Конституція – є, закон про захист персональних даних – є, а захист практично існує “на папері”. Об’єктивно це може визначатися труднощами політичної та соціально-економічної реформації, яка, на превеликий жаль, йде в Україні досить повільно.

З іншого боку, побутує думка, що проблема захисту персональних даних у наш час не актуальна у зв’язку з нерозвиненістю громадянського суспільства, наявністю менталітету примата держави і низьким рівнем інформатизації. При цьому зрозуміло, що немає жодної області життєдіяльності людини, суспільства та держави, де не застосовувалися б персональні дані. Парадоксальність ситуації у тому, що потреба в захисті персональних даних громадян об’єктивно існує, але вона серйозно не сприймається.

Є три основні причини для руху в напрямі удосконалення нормативно-правового упорядкування відносин у сфері захисту персональних даних, із яких виходять європейські та інші країни:

- усунення передумов та порушень прав людини на її персональні дані;
- розвиток е-комерції (е-бізнесу, е-торгівлі);
- гармонізація національних законодавств відповідно до приписів континентального права та норм європейських правових стандартів.

Для України актуальність і об’єктивна необхідність захисту прав громадян в інформаційній сфері визначається:

- розвитком інформаційних технологій і розповсюдження автоматизованих засобів і засобів збору, обробки, зберігання і поширення персональних даних;
- значною активністю у формуванні баз даних (соціального, фінансового, маркетингового, медичного, екологічного, адміністративного, правоохоронного та ін. змісту) та несанкціонованим поширенням персональних даних;
- використанням інформаційних технологій кримінальними структурами, що підривають зусилля з розвитку і зміцнення демократичної, правової держави.
- потребою у приведенні норм вітчизняного законодавства до приписів європейських правових стандартів в аспекті участі України в міжнародному процесі обміну інформацією, в міжнародних проектах, що засновані на використанні інформаційних технологій у різних секторах соціальної, економічної, наукової та науково-технічної діяльності.

Таким чином, проблема, що розглядається, не може не викликати стурбованості та нарікань щодо існуючого стану та потреби у створенні в державі цілісного та ефективного механізму захисту людиною своїх прав стосовно її персональних даних.

Метою статті є підсумок стану та формулювання пропозицій щодо створення цілісної системи у сфері захисту персональних даних в Україні.

Виклад основних положень. Сьогодні Україна перебуває на порозі доленосного рішення. Мова йде про підписання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом і його державами-членами, з іншої сторони [5] (далі – Угода про асоціацію), проект якої було схвалено Урядом України 18 вересня 2013 року [6].

У проекті Угоди про асоціацію, у статті 15 “Захист персональних даних” (Розділ ІІІ “Юстиція, Свобода та Безпека”), визначено: *“Сторони погоджуються співпрацювати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи. Співробітництво у сфері захисту персональних даних може включати, inter alia* (“в тому числі” – *Авт.*)*, обмін інформацією та експертами”.* Надалі Угода про асоціацію згадує поняття “захист персональних даних” ще чотири рази (ст.ст. 80, 123, 129 та 141) і лише у декларативному значенні повтору його необхідності. Про інструменти чи механізми реалізації правового захисту персональних даних мови у документі не йде, на противагу детальному розкриттю упорядкування відносин щодо економічних аспектів.

Звернемо увагу на те, що *Європейський Союз має економіко-правову спрямованість діяльності,* яка передбачає об’єднання європейських держав, націлене на їх інтеграцію *з метою формування спільного ринку*, що передбачає вільний рух товарів, капіталу і послуг, включаючи скасування паспортного контролю в межах Шенгенської зони, а також виробляє спільну політику в області торгівлі, сільського господарства, рибальства і регіонального розвитку. У складі інститутів ЄС е посада *Інспектора із захисту даних.*

Одночасно, *Рада Європи має соціально-правову спрямованість діяльності,* яка передбачає сприяння співпраці між всіма країнами світу *з метою впровадження стандартів права, демократичного розвитку, законності і культурної взаємодії.* Ця міжнародна організація є повністю самостійною, яка не входить в систему інститутів ЄС.

Україна у 2006 році ратифікувала Конвенцію Ради Європи № 108 “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” від 28.01.81 р. та “Додатковий протокол до Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних” від 08.11.01 р. Раніше зазначалося, Конвенція РЄ № 108 є першим та головним документом у сфері правового захисту персональних даних, який був прийнятий на розвиток положень Конвенції Ради Європи “Про захист прав та основоположних свобод” 1950 р.

Головними у Раді Європи вважаються два окремих інститути, які очолюють:

- Омбудсмен (від швец. – “захисник народу”) – загальні питання прав і свобод;
- *Комісар із захисту персональних даних* – усі питання щодо персональних даних.

Кожний з інститутів підпорядкований особисто Генеральному секретарю Ради Європи.

Якщо неупереджено порівняти функціональне призначення зазначених міжнародних організацій та деякі їх акти (див. Таблицю 2), кожен з яких спрямований на уніфікацію національних законодавств, може виникнути дилема у виборі рішень стосовно пріоритетів захисту прав людини у сфері персональних даних.

Економіка як сукупність виробничих відносин не може існувати без наявності певних відомостей, зокрема персональних даних. Держава також потребує персональних даних у контексті необхідності зворотного зв’язку в управлінні і забезпечення інформаційної безпеки, яка є складовою національної безпеки. Звідси й потреба в отриманні різноманітних даних та відповідному нормативному упорядкуванні відносин.

З іншого боку – присутній соціально-правовий аспект та міжнародне визнане право людини на *повагу до її приватного і сімейного життя, до недоторканості житла і таємниці кореспонденції*. В Україні статтею 32 Конституції встановлено – *“…Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом”*. Це визначає необхідність обмеження в поширенні персональних даних.

Відзначене, на наш погляд, й обумовлює складнощі у нормативно-правовому та організаційному вирішенні проблем, які існують у сфері захисту персональних даних.

Таблиця 2

Рада Європи	Європейський Союз
Основні акти	
Конвенція РЄ № 108 “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” від 28.01.81 р. Протокол до Конвенції РЄ № 108 щодо органів нагляду та транскордонних потоків даних від 08.11.01 р.	Директива 95/46/ЄС “Про захист осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних” від 24.10.95 р. Регламент ЄС № 45/2001 “Про захист фізичних осіб щодо обробки персональних даних установами і органами ЄС та вільного переміщення таких даних”
Деякі інші документи на розвиток основних актів	
Рекомендації РЄ № R (81)1 “Про захист персональних даних у автоматизованих базах медичних даних” Рекомендації РЄ № R (81)19 “Про доступ до інформації, що знаходиться у розпорядженні державних органів” Рекомендації РЄ № R (91)10 “Про передачу третім особам персональних даних, які знаходяться в розпорядженні державних органів” Рекомендації РЄ № R (87)15 “Про регулювання використання персональних даних у секторі поліції” Рекомендації РЄ № R (99)5 “Про захист осіб у зв’язку з обробкою даних у інформаційних магістралях” Рекомендації РЄ № R (2000)13 “Про європейську політику доступу до архівів” Рекомендації РЄ № R (95)13 “Про кримінально-процесуальні принципи, пов’язані з інформаційними технологіями” Рекомендації РЄ № R (99)15 “Про висвітлення у засобах масової інформації виборчих компаній” Рекомендації РЄ № R (2000)7 “Про права журналістів не розголошувати їх джерела інформації” Рекомендації РЄ № R (89)9 “Про злочини, пов’язані з комп’ютерами”	Директива 96/9/ЄС “Про правовий захист баз даних” Директива 97/13/ЄС “Про спільну базу для загальних дозволів та індивідуальних ліцензій в сфері телекомунікаційних послуг” Директива 96/19/ЄС ЄС “Про внесення поправок до Директиви 90/388/ЄЕС “Про забезпечення повної конкуренції на ринках телекомунікацій” Резолюція Ради ЄС від 20.06.01 р. “Про оперативні запити правоохоронних органів щодо громадських телекомунікаційних мереж та послуг” Директива 97/66/ЄС “Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі” (скасована) Директива 97/7/ЄС “Про захист прав споживачів у дистанційних контрактах” Резолюція Ради ЄС від 17.01.95 р. “Про законне перехоплення телекомунікаційних повідомлень” Директива 99/93/ЄС “Про систему електронних підписів, що застосовується в межах Співтовариства” Директива 2000/31/ЄС “Про правові аспекти інформаційних послуг щодо електронної комерції на внутрішньому ринку” Директива 2002/58/ЄС “Про обробку персональних даних та захист таємниці у секторі телекомунікацій”

Сьогодні, виходячи з європейських і світових уявлень про права і свободи журналісти борються за свободу слова. Віруючі – відстоюють свободу віросповідання і виступають проти заміни імені людини на ідентифікаційний номер. Мусульмани – заперечують будь-яке втручання в тіло людини (біометрія, чипи). Іудеї – проти того, щоб рахували євреїв. Правозахисники – стурбовані проблемами у реалізації права на

приватність персональних даних, поширеним несанкціонованим прослуховуванням телефонних розмов тощо. Підприємці – не бажають щоб інформація про їх і їхню діяльність (угоди, доходи, нерухомість, автомобілі, їхня родина тощо) потрапляла до рук злочинців (хоча саме в цьому середовищі спостерігається найактивніша діяльність із збору в БД персональних даних; як запевняють – в комерційних інтересах[5]). Пенсіонери – намагаються захистити свої права від бандитів, які завдяки “наведенню” з існуючих баз персональних даних шахрайськими способами заволодівають їх квартирами, майном тощо.

При цьому, процес отримання персональних даних перетворюється на окремий бізнес, метою якого є тільки збір, обробка та поширення персональних даних на комерційних засадах. Раніше персональні дані накопичувалися в картотеках і державних реєстрах. Тепер вони активно обробляються в комп’ютерах у приватних інтересах. Роблячи покупки в Інтернет-магазинах та отримуючи дисконтні картки, споживач змушений повідомляти свої персональні дані. Власники зазначених магазінів, з одного боку, зацікавлені у відомостях про стан попиту на ринку, який може бути оцінений завдяки відомостям про покупців та потенційних споживачів їх продукції, а з іншого – не завжди забезпечують захист персональних даних людини, навіть можуть збирати та пропонувати зазначені дані для продажу й отримання іншого виду прибутку, без диверсифікації номенклатури продукції. Останнє в умовах ринку – значний важіль у конкурентній боротьбі, гарант від розорення при змінах кон’юнктури.

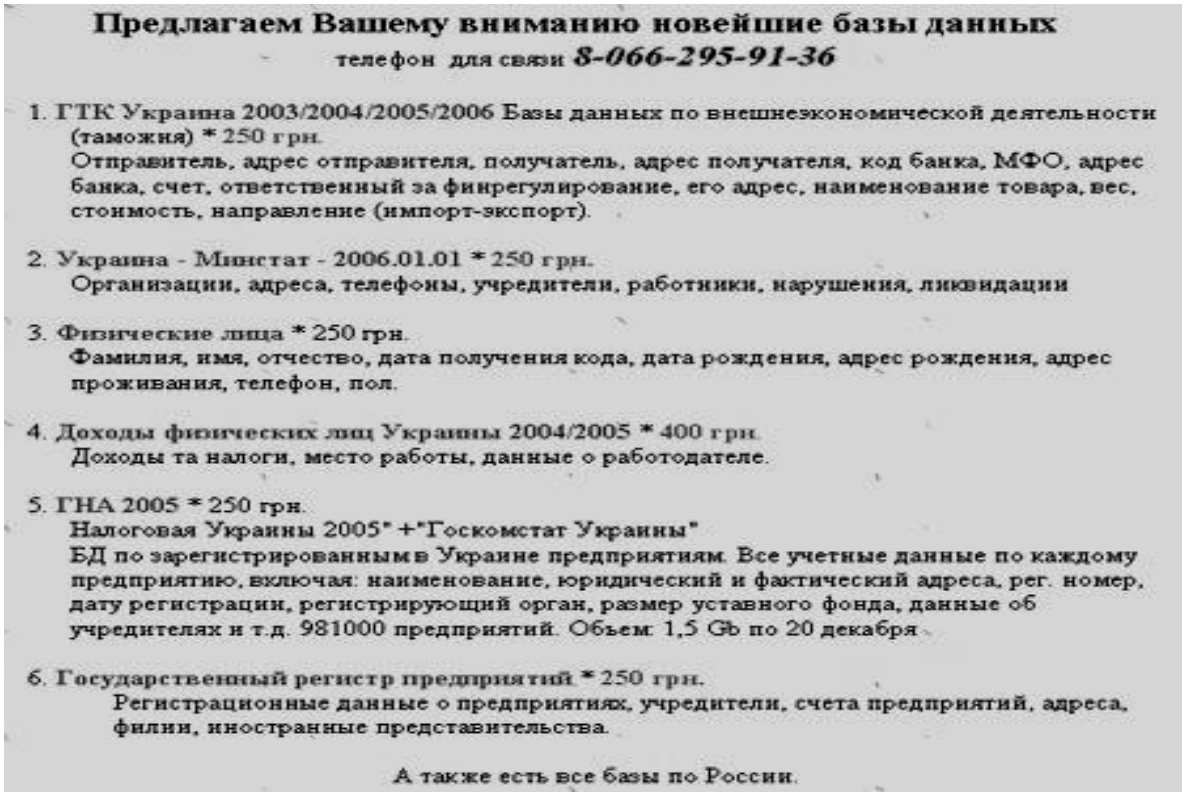
Природно, там, де “пахне” грошима, відразу виникає й активно розвивається відповідна злочинність. Збір та продаж персональних даних – звичайно не виняток. Відомості про паспортні та медичні дані, звички, коло знайомих, матеріальний стан, особисте життя, маршрути подорожей та багато ін. збираються у БД та реалізуються на дисках або розміщуються в Інтернеті. Коштує така БД від 10 (дрібний продаж) – до 1500 (через Інтернет) дол. Інформація мобільного зв’язку потрапляє на чорний ринок (номер коштує 50 дол., прослуховування – 150 дол. на рік). Як зазначалося у [8]: *“…світовий ринок персональних даних досягає 3 млрд. доларів у рік”,* у Росії – 20 - 24 млн. дол., а деякі експерти вважають, що він становить 100 млн. дол. на рік [9, 10]. У [11] повідомлялося, що збиток, завданий британській економіці розкраданнями ідентифікаційних даних у 2006 р., становив 1,8 млрд. ф. ст., а на кінець десятиріччя ця цифра могла досягти 3,8 млрд. ф. ст. завдяки росту злочинності у е-середовищі.

Окремі приклади комерційного поширення персональних даних див. на Рис. 1, 2.

Ті, хто займається маркетингом, продовжують вишукувати нові шляхи для збору будь-яких відомостей про своїх конкурентів та потенційних покупців: їх діяльність, оточення, стосунки, погляди, інтереси, характер, поведінка та багато ін. Для бізнесу персональні дані – зручне, а тепер і необхідне доповнення із усього того, що надає Інтернет або інші мережі. Уже цілком чітко усвідомлено, що за допомогою засобів е-середовища набагато легше збирати величезні обсяги різної інформації, а аналіз і взаємне ув’язування відомостей забезпечує істотні прибутки і лідерство в бізнесі. Критерії, відповідно до яких відомості про людину включаються до списку, призначеного для маркетингових заходів, очевидні. Так дані про людину, що має машину, вносять до

[5] Перша картотека персональних даних та комерційне поширення відомостей із неї з’явилися у 1886 році, коли шовкоторговець Л’юіс Тепен із Нью-Йорка створив агентство збору та аналізу інформації про кредитоспроможність підприємців, які зверталися до нього за позикою. Накопичивши декілька томів кредитних звітів, він став продавати інформацію. Клієнти платили від 100 до 200 дол. на рік [7].

списку її відповідної моделі; дані про власників моторних човнів – до списку відповідних моделей володарів човнів, і так далі.



Предлагаем Вашему вниманию новейшие базы данных

телефон для связи *8-066-295-91-36*

1. ГТК Украина 2003/2004/2005/2006 Базы данных по внешнеэкономической деятельности (таможня) * 250 грн.
   Отправитель, адрес отправителя, получатель, адрес получателя, код банка, МФО, адрес банка, счет, ответственный за финрегулирование, его адрес, наименование товара, вес, стоимость, направление (импорт-экспорт).

2. Украина - Минстат - 2006.01.01 * 250 грн.
   Организации, адреса, телефоны, учредители, работники, нарушения, ликвидации

3. Физические лица * 250 грн.
   Фамилия, имя, отчество, дата получения кода, дата рождения, адрес рождения, адрес проживания, телефон, пол.

4. Доходы физических лиц Украины 2004/2005 * 400 грн.
   Доходы та налоги, место работы, данные о работодателе.

5. ГНА 2005 * 250 грн.
   Налоговая Украины 2005" +"Госкомстат Украины"
   БД по зарегистрированным в Украине предприятиям. Все учетные данные по каждому предприятию, включая: наименование, юридический и фактический адреса, рег. номер, дату регистрации, регистрирующий орган, размер уставного фонда, данные об учредителях и т.д. 981000 предприятий. Объем: 1,5 Gb по 20 декабря

6. Государственный регистр предприятий * 250 грн.
   Регистрационные данные о предприятиях, учредители, счета предприятий, адреса, филии, иностранные представительства.

А также есть все базы по России.

Рис. 1. Комерційна пропозиція персональних даних в Україні [12].

Назва баз персональних даних	**Ціна** (руб)
“Приватні особи м. Москви та Московської області”	$ 150
“Приватні особи Росії та СНД” (включає е-адресу)	$ 200
“Фізичні особи Московської області”	1000
“Жителі Московського регіону” (повні відомості щодо паспорта)	400
“Прописка у м. Москві”	500
“Прописка у Московській області”	400
“Квартири та їх власники м. Москви”	1000
“Приватизовані квартири м. Москви”	400
“Експортно-імпортні операції” (товар, вартість, постачальник, споживач тощо)	1400
“Московська ліцензійна палата” (про ліцензії)	400
“Московська реєстраційна палата” (про юридичних осіб і приватних підприємців)	500
“Московський земельний комітет”	200
“ДАІ м. Москви” (повні відомості про автомобілі та їх власників)	500
“Посвідчення водія у м. Москва та Московській області”	500
“Мобільні телефони Московського регіону”	500
“Єдина міська телефонна мережа м. Москви”	500
“МТС 2003” (усі телефонні номери, реквізити та адреса абонентів)	500
“Банки Росії” (усі реквізити)	300

Рис. 2. Комерційна пропозиція персональних даних в Росії [13].

В основу прямого маркетингу покладене створення списків людей, поєднуваних загальними демографічними даними. І для цих цілей зовсім не потрібна конфіденційна інформація. Головне, щоб її було якомога більше.

Реальність така, що за відсутності в державі ефективного механізму та цілісної системи захисту персональних даних структури та окремі особи, що збирають, обробляють та поширюють персональні дані, заробляють як їм заманеться, з порушенням прав тих, чиї дані обробляються. Від такої “комерції” бюджет держави взагалі нічого не одержує[6].

І все це на тлі ілюзорності і ефемерності абсолютного захисту та нарікань щодо недоліків законодавства України у сфері персональних даних.

Про деякі проблемні аспекти, пов’язані з законом.

Історично при укладанні національних правових систем захисту персональних даних дотримуються двох принципів, які передбачають:

- створення всеохоплюючого закону про захист приватного життя, який спрямований на упорядкування інформаційних відносин, пов’язаних з визначеними даними. Цей підхід веде до необхідності коригування положень закону при появі нових загроз;
- створення спеціальних законів для кожного типу зазіхань на приватне життя або для кожної сфери, яка є потенційним джерелом загрози та порушень (наприклад, для мас-медіа, банків, телекомунікацій та ін.). Але при виникненні нових загроз такий підхід призводить до безсистемності, дублювання та суперечливості окремих норм.

У практичному застосуванні обидва підходи виявили свою низьку ефективність.

Набутий досвід враховується законодавцями – при створенні національного закону застосовують змішаний підхід. Він полягає у створенні рамкового (базового, системоутворювального) закону про захист персональних даних, а вже на його основі розробляються окремі галузеві нормативно-правові акти. При виникненні нових загроз та видів порушень прав особи на її персональні дані система захисту залишається незмінною, а до галузевих актів вносяться необхідні доповнення та зміни.

Саме в цьому і полягала основна ідея при розробці Закону України, яка так й не була сприйнята повною мірою. Створити “закон-панацею” для персональних даних на всі випадки життя не є можливим. Звідси і нарікання до окремих правових конструкцій, які є до нашого часу. Але в кожного свій погляд і свій інтерес, які, нерідко, не узгоджуються з прагненнями інших, що взагалі не сприяє створенню єдиній системи.

Розробку проекту Закону України “Про захист персональних даних” було ініційовано в 1996 році у Національному агентстві з питань інформатизації при Президенті України, після публікації статті за назвою “*Персональные данные: есть проблемы?*” [14].

Перша версія законопроекту була підготовлена до середини 1998 року. Вона неодноразово розглядалася в таких міністерствах і комітетах як: Мінекономіки, Мінфінансів, Мін’юстиції, МВС, СБУ, Комітет з питань державних секретів, Державна податкова адміністрація, Рада національної безпеки і оборони, Уповноважений ВР України з прав людини.

---

[6] Якось після демонстрації дослідів з електрикою, Майкла Фарадея запитали: “*Яка користь від електрики?* .”

Він відповів: *“Коли-небудь ви будете мати можливість обкласти її податком”.*

Наведемо тільки деякі відомості щодо кількості експертиз (розглядів) та зауважень в органах влади.

Мін’юстиції: перший розгляд – 25 зауважень; другій – 10 зауважень; третій – 11 зауважень; четвертий – 6 зауважень; п’ятий – 3 зауваження.

Мінекономіка: при першому і другому розгляді було одне і те ж зауваження щодо ліцензування діяльності на персональні дані, на третій – вже 5 інших зауважень, у четвертий – законопроект був узгоджений, у п’ятий розгляд виникло нове зауваження: *“…необхідним є обґрунтований прогноз про очікувані соціально-економічних наслідки закону”.*

Мінфінансів: після першого розгляду законопроект був узгоджений без зауважень. При другому розгляді було вже 3 зауваження. При третьому і четвертому розглядах зауважень не було – узгоджений. При п’ятому розгляді – 2 зауваження.

Державна податкова адміністрація: при першому розгляді було 6 зауважень, при другому, третьому і четвертому розгляді зауважень не було – узгоджений, при п’ятому розгляді з’явилося 8 зауважень.

МВС: перший розгляд – 18 зауважень, другій – 4, третій – 1, четвертий і п’ятий – законопроект узгоджено.

СБУ: перший розгляд –19 зауважень, другій – 4, третій – 3, четвертий – 7, п’ятий – 23 зауваження.

На кінець 1999 р. було враховано понад 250 зауважень та пропозицій і законопроект, погоджений з усіма державними органами влади, за винятком Мінюсту і СБУ, був 27 грудня спрямований до Кабінету Міністрів України (вих. № 5555 Держкомзв’язку).

Після внесення поправок профільними відділами секретаріату КМУ законопроект в котре був розісланий на узгодження до тих самих органів влади, а також до Міністерства освіти і науки та Міністерства закордонних справ.

До окремих особливостей експертизи в міністерствах і комітетах можна віднести:

- відсутність системності і послідовності в організації роботи по проведенню експертизи. Це полягало в тому, що у зв’язку із змінами керівництва органів та виконавців експертиза виконувалася різними особами і зауваження часто повторювалися;
- нерідко виконавці мали туманне уявлення про предмет експертизи, що було зрозуміло з формулювань зауважень, а також запитань у процесі телефонних розмов;
- заперечення Мін’юстом можливості введення в законодавство нової юридичної категорії – “права власності фізичної особи на свої персональні дані”[7], не зважаючи на розвиток комерції з персональними даними. Іншими словами, нами пропонувалося додати людині повноваження на її персональні дані, властиві праву власності, та в межах визначених Конституцією. Проте, в висновках Мін’юсту (зокрема, вих. № 23-9-4450 від 27.06.00 і № 23-9-7900 від 2.11.00 р.) наголошувалося те, що вказана пропозиція *“…свідчить про недостатній рівень опрацьованості проекту та суперечливе розуміння авторами проекту поняття власності”.*

Зазначимо при цьому, що не так давно **(!)** Єврокомісія визнала за доречне дослідити цю нашу юридичну новацію на предмет введення до законодавства ЄС.

[7] Див. книгу *“Защита персональных данных”,* видану у 1998 році [15], в якій представлено першу версію законопроекту (С. 81-96) та надано відповідну аргументацію механізмів його реалізації, зокрема щодо власності на персональні дані (С. 41-42). У подальшому процес удосконалення рішень розглядався та доводився нами до громадськості у наукових статтях, зокрема [16 – 23] та книгах [2, 24 – 29].

До липня 2000 р. законопроект “Про захист персональних даних” в Україні підписали керівники наступних органів влади: Мінфінансів, Мінекономіки, Міносвіти і науки, Державної податкової адміністрації, МВС, СБУ, МЗС, Держкомзв’язку, після чого знову було спрямовано до Кабінету Міністрів України.

Через шість років, після того як законопроект пройшов додаткову експертизу юристів інших міністерств, комітетів та громадських організацій, був підтриманий спеціалістами у сферах інформаційного та адміністративного права, інформатизації, та інформаційної безпеки, які мають наукові ступені та звання (академіки та члени-кореспонденти НАН України та НАПрН України – 9; доктора наук – 18; кандидати наук – 24), врахував понад 600 зауважень та пропозицій, отримав позитивний висновок Головного науково-експертного управління Апарату ВР України, 16 березня 2006 р. він був прийнятий у другому читанні та в цілому абсолютною більшістю народних депутатів України (згідно поіменного голосування: За – 287; Проти – 0; Утрималися – 1; Не голосували – 108. Всього – 396 депутатів), але потім Закон… зник.

Зауважимо, за роки розробки проект Закону України “Про захист персональних даних” обговорювався на численних конференціях, семінарах, “круглих столах” тощо (за загальним підсумком – понад 40). Про першу версію автори проекту (В. Брижко та О. Баранов) доповідали на засіданні експертів *“Впровадження міжнародних стандартів із захисту приватності інформації персонального характеру в Україні”* у присутності Комісара Ради Європи із захисту даних, виконавчого члена Комісії Австрії у питаннях захисту даних пані Вольтраут Кочі.

Лише у 2010 році проект закону без суттєвих змін знову внесено на розгляд та голосування депутатів. Згідно з поіменним голосуванням у другому читанні та в цілому проголосувало народних депутатів України: За – 355; Проти – 0; Утрим. – 0; Не голосували – 61. Всього – 416 депутатів. Підписаний Президентом України Закон № 297-VI від 01.06.10 р. набрав чинності з 01.01.11 р.

Висновки та окремі пропозиції.

1. Законодавство про захист персональних даних практично в жодній країні світу не отримало своєї зрілості, навіть на термінологічному рівні. Повна адекватність національних законодавств про захист персональних даних ще не досягнуто.

Основною проблемою нормативно-правового упорядкування відносин у сфері захисту персональних даних є протиріччя між прагненням максимального використання персональних даних у державних та корпоративних інтересах й, одночасно, особисте бажання кожної людини максимально захистити свої права.

Теоретично ідея захисту персональних даних виходить з необхідності захисту індивідуума і гарантій верховенства його інтересів над “державними та суспільними інтересами”. Зазначені інтереси, звичайно, можуть бути спрямовані на виконання волі одного керівника (лідера) із силою і невідворотністю натовпу. Проте будь-яке насильство повинне застосовуватися процедурно, згідно загальносвітових принципів визначених Конвенцією Ради Європи № 108 “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” від 28.01.81 р.

2. Можна стверджувати, що Закон України “Про захист персональних даних” відповідає принципам, закладеним у Конвенції Ради Європи № 108 від 28.01.81 р.

Головна проблема на національному рівні полягає у відсутності ефективного правового механізму щодо адміністративно-організаційного регулювання відносин (який детально надавався у [30]) та відповідальності у сфері захисту персональних даних. Незважаючи на санкції, введені Законом України “Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення

законодавства про захист персональних даних” (набрав чинності 01.01.12 р.), практична відповідальність за порушення закону продовжує носити декларативний характер.

Щодо бажань максимальної деталізації у забезпеченні захисту персональних даних, то є сенс мати на увазі, що, по-перше, ідеальну модель захисту створити можна, але реалізувати її практично неможливо – абсолютного захисту не існує, життя не в змозі перемогти смерть. По-друге, зайва деталізація упорядкування відносин у цій сфері в умовах розвитку інформаційного суспільства може знижувати попит на розробку нових інформаційно-комп’ютерних технологій. Це обумовлена мотивація для “бізнес-софт-індустрії”, яка не буде зацікавленою у технологіях, здатних забезпечити сильний захист.

3. У повсякденному житті фізична особа виступає у двох іпостасях: як “людина” та як “громадянин” (як зауважував Ш. Монтеське: *“Свобода личности и свобода гражданина не всегда совпадают”)*. У принципі, для створення умов більш сильного захисту персональних даних у законодавстві це потребує їх розмежування.

Захист прав “людини” від несанкціонованої комерційної діяльності з її даними має здійснюватися завдяки засобам потужного “інституту власності” (через тріаду повноважень – користування, володіння, розпорядження). Це надає можливість безпосереднього залучення людини до процесу захисту своїх персональних даних на визначених законом умовах.

Підкреслимо, зазначений захист має стосуватися лише того аспекту, коли мова йде про “людину” персональні дані якої використовують з комерційною метою: збирання даних з різних джерел, створення баз персональних даних та їх поширення на комерційних засадах, здійснення чого в обов’язковому порядку повинно враховувати добре відоме оголошення: *Стій! Приватна власність. Вхід заборонено.*

Діяльність органів державної влади, зокрема функціонування її силових структур, не є можливою без персональних даних. Для органів влади фізична особа виступає як “громадянин”, використання даних якого повинно здійснюватися у межах повноважень наданих Конституцією та галузевими законами.

Така постановка справи, з одного боку, надає законодавству в сфері захисту персональних даних нову якість, системність та перспективність, про що детально йдеться у [15, с. 40-42; 23, с. 169-176; 24, с. 38-42; 22, с. 45-54; 24, с. 12-25; 25, с. 66-68; 29, с. 65-69].

З іншого – ця новація у повному обсязі відповідає положенню статті 11 Конвенції РЄ № 108 “*Жодне з положень цієї глави* (Глава II – Основоположні принципи захисту даних – *від Авт.*) *не тлумачиться як таке, що обмежує або іншим чином перешкоджає можливості Сторони забезпечувати суб’єктам даних більший ступінь захисту, ніж передбачений цією Конвенцією*” [1, с. 68].

До вказаного додамо наступне.

До теперішнього часу законодавство не дає відповідь на питання – кому належать майнові блага від використання персональних даних будь-якої конкретної особи?

Згідно зі статтею 8 Закону України “Про захист персональних даних” від 01.06.10 *суб’єкт персональних даних має <u>особисті</u> <u>немайнові права</u> на <u>персональні дані</u>.* Й це у той час, коли їх *<u>не санкціоновано</u>* збирають та *<u>продають</u>*.

Зазначимо, що поняття “особисті немайнові права” залучено з Цивільного кодексу України і запроваджено лише у нашій країні. У міжнародному праві, праві Європейської Спільноти, а також у законодавстві європейських країн його і не існує. При цьому, ані в Конституції України, ані в ЦКУ поняття “персональні дані” не вживається. А слово “особистих”, що пристосовано у ЦКУ до “немайнових прав”, взагалі зайве. Зазначене поняття сприймається як “масло-масляне” та сприяє підтримці “системи”, яка в умовах е-середовища може працювати лише формально та адміністративно-суб’єктивно.

4. Проблема реєстрації баз персональних даних в Україні потребує додаткових досліджень та врахування практичного досвіду, який мають провідні європейські держави, наприклад, *Великобританія.*

Інститут Уповноваженого з питань захисту персональних даних у Великобританії функціонує на основі Закону “Про захист даних ” від 12.07.84 р. Він визначив посади Міністра по захисту даних, Реєстратора по захисту даних і утворив Суд по захисту даних.

Міністр вправі змінити чи доповнити положення закону, з метою надання додаткових гарантій по захисту персональних даних. Проект розпорядження, правила чи наказу повинен бути схвалений постановою кожної палати парламенту.

Реєстратор призначається грамотою Її Величності королеви й має обов’язки:

- ведення реєстру осіб, які збирають і зберігають персональні дані, а також мають комп’ютерні бюро і надають послуги щодо персональних даних;
- вручення повідомлень про порушення закону, про скасування реєстрації або про заборону передачі даних;
- розгляд скарг про порушення закону.

Будь-яка особа вправі звернутися з апеляцією до *Суду по захисту даних* у разі відмови Реєстратора розглянути скаргу про порушення закону.

Основними елементами системи захисту персональних даних у Великобританії є:

- ведення реєстру баз персональних даних та осіб, які надають послуги щодо персональних даних;
- перевірка і контроль діяльності з персональними даними;
- вручення повідомлення про порушення, про скасування реєстрації, про заборону передачі даних;
- адміністративне і судове оскарження у зв’язку із захистом даних.

5. Виходячи з практики розділення повноважень та функцій структур Уповноваженого з прав людини (Омбудсмена) та Уповноваженого з питань захисту персональних даних (Комісара із захисту персональних даних), які існують в адміністрації Ради Європи і європейських країнах, є необхідність оцінки такої підходу, шляхом практичного ознайомлення та вивчення відповідного досвіду, наприклад у *Німеччині.*

У цій країні Інститут Комісара почав формуватися в 1970 році, коли в Землі Гессен вперше у світі був прийнятий Закон “Про захист даних ”. Закон установив державну посаду Комісара із захисту даних на правах єдиноначальності. Цьому виборному державному службовцю закон надав і забезпечив право повної незалежності від владних структур, а також надав право спостереження за діяльністю щодо персональних даних.

Сьогодні захист персональних даних у країні визначається положеннями Федерального Закону “Про подальший розвиток обробки і захисту даних” від 20.12.90 р. Згідно із законом за поданням Федерального уряду Бундестаг на строк 5 років обирає Федерального уповноваженого з питань захисту даних, який потім призначається на посаду Президентом.

6. Через те, що законодавство відстає від розвитку технологій та можливостей Інтернету, а корпоративні засоби захисту персональних даних не завжди відповідають принципам європейських правових стандартів, захист прав людини у сфері персональних даних вимагає визначення особливих повноважень та можливостей із контролю та регуляції інформаційних відносин різних суб’єктів незалежним від владних структур Уповноваженим із захисту персональних даних в Україні (можливо на прикладі Німеччини – подвійне підпорядкування: Бундестагу (щорічний звіт та отримання завдань) та Міністру внутрішніх справ (нагляд за діяльністю та допомога у перевірках).

Щодо України, то однією з важливих функцій Уповноваженого має стати постійне відстеження змін в розвитку нових інформаційно-комп’ютерних технологій та оперативне вживання заходів захисту персональних даних.

7. Вирішення завдання створення в Україні цілісної системи ефективного захисту персональних даних є однією з головних складових загальної соціально-політичної та економічної проблеми, пов’язаною з побудовою інформаційного суспільства. У правовій, соціальній державі це визначається потребою в узгоджені суперечливих але взаємопов’язаних аспектів упорядкування соціальних та економічних інформаційних відносин за умов забезпечення інформаційної безпеки. Зазначене регулювання не можна обмежувати тільки нормами Конституції та окремими не дуже пов’язаними між собою статтями деяких чинних законів.

Для сфери захисту персональних даних в Україні необхідними є додаткові галузеві закони, у яких принципи рамкового Закону України “Про захист персональних даних” мають бути деталізовані, не порушуючи при цьому юридичні рамки його цільового та функціонального призначення.

8. У загальному плані для створення в Україні цілісної системи ефективного захисту персональних даних слід запровадити Судову палату з питань захисту персональних даних та почати підготовку кваліфікованих фахівців для цієї сфери.

Використана література

1. Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв’язку з автоматизованою обробкою даних у правоохоронній діяльності : посібник. – Кн. 2 / [В. Брижко, М. Швець та ін.] ; за ред. д.е.н., професора М. Швеця. – К. : ТОВ “Пан Тот”, 2006 р. – 509 с.

2. е-майбутнє та інформаційне право / [В. Брижко, Ю. Базанов та ін.] ; за ред. д.е.н., професора М. Швеця. – [2-е вид., доп.]. – К. : ТОВ “Пан Тот”, 2006. – 234 с.

3. Прослушивание телефонов в международном праве и законодательстве одиннадцати европейских стран ; сост. Е.Е. Захаров. – Х. : “Фолио”, 1999. – 152 с. – (Харьковская правозащитная группа).

4. – Режим доступу : //www.domik.kontrakty.ua

5. – Режим доступу : //www.kmu.gov.ua/kmu/control/uk/publish/article?art_id=246581344&cat_id=223223535

6. – Режим доступу //www.dengi.ua/news/123868_Associaciya_s_ES_ne_grozit_Ukraine_poterej_ekonomicheskoj_nezavisimosti_-_evrokomissar.html

7. Расколотая база. – Режим доступу : //www.aferizm.ru/bb_bd.htm

8. Цена персональных данных. – Режим доступу : //www.i2r.ru/article.shtml?id=1384

9. Проблема правовой защиты персональных данных. – Режим доступу : //www.kiev-security.org.ua/box /4/136.shtml

10. Законспирированный оборот. – Режим доступу : //www.privasi.hro.org/risk/data/index

11. Киберпреступность сильнее полиции // Обзор. – 2006. – № 103(128). – С. 6.

12. – Режим доступу : //www.khpg.org/index.php?id=1186147137

13. – Режим доступу : //www.khpg.org/index.php?id=1186147137

14. Баранов А.. Персональные данные : есть проблемы? / Зеркало недели, 15.06.96 г.

15. Брыжко В.М. Защита персональных данных / [А.А. Баранов, В.М. Брыжко, Ю.К. Базанов]. – К. : Национальное агентство по вопросам информатизации при Президенте Украины, 1998. – 128 с.

16. Баранов А.А., Брыжко В.М. Защита персональных данных / Деловая Украина, 08.10.97 г.

17. Персональні дані та право власності // Українське право. – 2002. – № 1. – С. 152-157. – (Українська правнича фундація).

18. Про приєднання України до Конвенції № 108 Ради Європи // Право України. – 2003. – № 1. – С. 34-37.

19. Організаційно-правовий захист персональних даних // Бюлетень з обміну досвідом роботи. – 2003. – № 144. – С. 27-33. – (Міністерство внутрішніх справ України).

20. Перспективи приєднання України до Конвенції Ради Європи про захист осіб у зв’язку з автоматизованою обробкою персональних даних // Проблеми пенітенціарної теорії і практики. – 2003. – № 8. – С. 136-140. – (Бюлетень МВС України та КІВС).

21. Упорядкування суспільних відносин у сфері захисту персональних даних // Правова інформатика. – 1/2003. – С. 43-47.

22. Про економічний аспект захисту персональних даних у контексті права власності на інформацію // Правова інформатика. – № 1(9)/2006. – С. 45-48.

23. До питання е-торгівлі та захисту персональних даних // Правова інформатика. – № 1(13)/2007. – С. 12-25.

24. Права человека и защита персональных данных / [А.А. Баранов, В.М. Брыжко, Ю.К. Базанов]. – Харьков: ХПГ-Фолио, 2000. – 280 с. – (Издана при содействии Харьковской правозащитной группы и Национального фонда поддержки демократии США).

25. Правовий механізм захисту персональних даних / В.М. Брижко : монографія ; за заг. ред. д.е.н., професора М.Я. Швеця та д.ю.н., професора Р.А. Калюжного. – К. : Парламентське видавництво, 2003. – 120 с.

26. Інформаційне право та правова інформатика у сфері захисту персональних даних : монографія / [В. Брижко, М. Гуцалюк, М. Швець та ін.] ; за ред. д.е.н., професора М. Швеця. – К. : ТОВ “Пан Тот”, 2005. – 333 с.

27. Електронний банкінг у контексті захисту персональних даних : монографія / [В. Брижко, Ю Базанов та ін.] ; за ред. д.е.н., професора М. Швеця. – К. : ТОВ “ПанТот”, 2008 р. – 141 с.

28. Методологічні та правові засади упорядкування інформаційних відносин : монографія / В.М. Брижко. – К.: ТОВ “ПанТот”, 2009. – 418 с.

29. Основи систематизації інформаційного законодавства : теоретичні та правові засади : монографія / В.М. Брижко. – К. : ТОВ “ПанТот”, 2012 р. – 304 с.

30. Організаційно-правові питання захисту персональних даних : дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.07 – теорія управління; адміністративне право і процес; фінансове право; інформаційне право / Брижко Валерій Михайлович ; Національна академія державної податкової служби України. – К., 2004. – 251 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.721: 681.3.02

МЕЛЬНИК К.С., здобувач наукового ступеня кандидата юридичних наук,
начальник управління юридичного забезпечення
Державної служби України з питань захисту персональних даних

ТЕОРЕТИКО-ПРАВОВИЙ ЗМІСТ ТЕРМІНА “ПЕРСОНАЛЬНІ ДАНІ”

Анотація. *У статті проведено комплексний аналіз терміна “персональні дані” згідно європейським підходом до формування та визначення його правового змісту. Запропоновані оптимальні шляхи його удосконалення в законодавстві України.*

Ключові слова: *персональні дані, захист персональних даних, ідентифікація, удосконалення законодавства.*

Аннотация. *В статье проведен комплексный анализ термина “персональные данные” в соответствии с европейским подходом к формированию и определению его правового содержания. Предложены оптимальные пути его усовершенствования в законодательстве Украины.*

Ключевые слова: *персональные данные, защита персональных данных, идентификация, усовершенствование законодательства.*

Summary. *The law nature of the term “personal data” according to European way of formation and determination of its law context is analyzed in the article. The optimal ways for improvement of Ukrainian legislation are proposed.*

Key words: *personal data, personal data protection, identification, improvement of legislation.*

Постановка проблеми. Інститут захисту персональних даних пройшов динамічний та тривалий шлях свого становлення, однак є достатньо молодим у правовому значенні. Його формування значною мірою пов’язано з розвитком конституційних прав і свобод людини і громадянина, зокрема з правом особи на недоторканність приватного життя, що є одним із основоположних принципів світових демократій та знайшло своє відображення у багатьох міжнародно-правових актах. Це право як юридична категорія зародилося в США. В англійській мові всі сторони приватного життя позначаються єдиним терміном “privacy” (з англ. – приватне життя, приватність), який не має буквального перекладу українською мовою.

Починаючи з 90-х років XX століття в документах Європейського Союзу активно використовується термін “право на захист даних” (з англ. – *right to data protection*). На своєму засіданні 4 липня 1999 року у Кельні Рада Європейського Союзу ухвалила рішення про підготовку проекту Хартії основних прав Європейського Союзу. У зв’язку з цим Робоча група Статті 29 Директиви ЄС 95/46/ЄС, підтримуючи рішення Ради ЄС, ухвалила 7 вересня 1999 року рекомендацію, якою запропонувала включити право на захист персональних даних до європейського “каталогу фундаментальних прав” [1].

Україна, прагнучи дотримуватись європейських стандартів у частині захисту права людини на недоторканність її приватного життя, ратифікувала у 2010 році Конвенцію Ради Європи № 108 про захист осіб у зв’язку з автоматизованою обробкою персональних даних 1981 року [2] та Додатковий протокол до неї щодо органів нагляду та транскордонних потоків даних 2001 року [3]. З метою належної імплементації норм зазначених міжнародних договорів цього ж року прийнято Закон України “Про захист персональних даних” від 1 червня 2010 року № 2297-VI [4], який, зокрема, у статті 2 містить визначення терміна “персональні дані”.

Правовий зміст терміна “персональні дані” є вихідним у формуванні підходів щодо законодавчого регулювання захисту персональних даних в Україні відповідно до європейських стандартів. Необхідність комплексного дослідження правової природи терміна “персональні дані” на основі європейського досвіду його формування та визначення й зумовлюють актуальність даного дослідження.

У вітчизняній юридичній літературі дослідженню окремих питань цієї проблематики приділяли увагу такі учені, як О. Баранов, В. Брижко, І. Жиляєв, Є. Захаров, Р. Романов, Ю. Базанов та ін. Розгляд цього питання здійснюється і зарубіжними вченими, як Л. Брейдейс, М. Важорова, Р. Валєєв, І. Вельдер, В. Гаврилов, В. Копилов, М. Рассолов, С. Уоррен та ін. Наукові пошуки з даного питання знаходяться у стадії свого розвитку, що потребує подальших досліджень.

Метою статті є визначення правової природи та змісту терміну “персональні дані” відповідно до європейського підходу формування, а також пошук оптимальних шляхів його удосконалення в законодавстві України.

Виклад основного матеріалу. Ключовим у сфері захисту персональних даних в Україні є термін “персональні дані”, який характеризує названу сферу загалом і є похідним для формування інших концептуальних термінів. Цей термін не тільки надає назву відповідній галузі, а й утворює інші спеціалізовані терміни, такі як: “обробка персональних даних”, “суб’єкт персональних даних”, “згода суб’єкта персональних даних”, “володілець персональних даних”, “розпорядник персональних даних”, “обробка персональних даних”, “знеособлення персональних даних” тощо. Термін “персональні дані” має вкрай важливе значення для суб’єктів відносин, пов’язаних із персональними даними, зокрема для кваліфікації, які саме персональні дані, що обробляються, потребують захисту. Саме цим обумовлюється необхідність чіткого законодавчого визначення терміна “персональні дані” в українському законодавстві. Оскільки Україна прагне дотримуватись найкращих європейських підходів та практик у побудові дієвої системи захисту персональних даних, варто звернути увагу на європейський досвід формування та визначення терміна “персональні дані”.

Європейська юридична теорія та практика виробила достатньо узагальнене юридичне визначення поняття “персональні дані”.

Конвенція Ради Європи № 108 про захист осіб у зв’язку з автоматизованою обробкою персональних даних 1981 року визначає персональні дані як *будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною*.

Відповідно до статті 2 Директиви Європейського Парламенту і Ради № 95/46/ЄС про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних 1995 року (далі – Директива № 95/46/ЄС) [5] “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, яку може бути встановлено прямо чи непрямо, зокрема, за допомогою ідентифікаційного коду або одного чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості.

Більш змістовно термін “персональні дані” розкривається в документах Європейського Союзу та Ради Європи рекомендаційно-роз’яснювального характеру. Так, у Повідомленні Європейської комісії від 4 листопада 2010 року № COM (2010) 609 Європарламенту, Раді ЄС, Економічно-соціальному комітету та Комітету регіонів ЄС “Комплексний підхід до захисту персональних даних в Європейському Союзі” [6]

зазначено, що термін “персональні дані” має на меті охопити всю інформацію, пов’язану з ідентифікацією або можливістю ідентифікувати особу прямо чи не прямо. З метою встановлення, чи особа може бути ідентифікована, мають враховуватися *всі засоби, якими може скористатися володілець персональних даних або будь-яка інша особа для ідентифікації згаданої людини*.

У свою чергу, варто звернути увагу на рекомендацію Комітету міністрів Ради Європи державам-членам № CM/Rec (2010) щодо захисту осіб у зв’язку з автоматизованою обробкою персональних даних у контексті їх профілювання [7, с. 42-51]. Відповідно до пункту 1 Додатка до зазначеної рекомендації *особа не вважається такою, що підлягає ідентифікації, якщо ідентифікація вимагає необґрунтованих часу та зусиль.*

Отже, термін “персональні дані” повинен охоплювати всю інформацію про фізичну особу, яка ідентифікована або може бути ідентифікована у будь-який можливий спосіб. Для визначення факту ідентифікації особи необхідно враховувати всі можливі засоби для ідентифікації вказаної особи. Такий широкий підхід до визначення персональних даних надає змогу досягти достатньої гнучкості, що дозволяє використовувати вказаний термін у різноманітних ситуаціях, які існують або можуть виникнути у майбутньому. Проте, якщо ідентифікувати фізичну особу неможливо або ідентифікація особи вимагає необґрунтованих часу та зусиль, рекомендується не відносити інформацію до категорії персональних даних.

Наведене вище визначення персональних даних у статті 2 Директиви № 95/46/ЄС відображає намір європейського законодавця надати якомога більш широкі правові можливості його застосування. У початковій пропозиції Європейської комісії, що передувала ухваленню Директиви № 95/46/ЄС, зазначається, що, *як і в Конвенції 108, широке визначення прийнято з метою охопити всю інформацію, яка може бути пов’язана з людиною* [8]. У подальшому Європейська комісія у оновленій пропозиції зазначає, що *зміни до пропозиції враховують бажання парламенту дати якомога більш загальне визначення терміна* “*персональні дані*”*, з тим щоб включити всю інформацію, яка стосується особи, яку можна ідентифікувати* [9].

Досить детальний аналіз терміна “персональні дані” міститься у Висновку Робочої групи із захисту даних, утвореної відповідно до статті 29 Директиви № 95/46/ЄС**,** № 4/2007 (WP 136) від 20 червня 2007 року щодо концепції персональних даних (далі – Висновок WP 136) [10, с. 515-541]. У Висновку WP 136 наведений аналіз терміну “персональні дані”, визначеного статтею 2 Директиви № 95/46/ЄС. Експерти Робочої групи при ґрунтовному аналізі терміна “персональні дані” виходили з наступних міркувань:

- кінцевою метою застосування правил, що містяться в Директиві № 95/46/ЄС, є захист основоположних прав і свобод фізичних осіб, зокрема права на недоторканність приватного життя людині в контексті обробки її персональних даних;

- сфера застосування Директиви № 95/46/ЄС включає ряд заходів, а її текст є “гнучким” для забезпечення належного правового реагування на різні життєво важливі обставини;

- сфера застосування Директиви № 95/46/ЄС має чіткі рамки та обмеження, які необхідно враховувати в процесі аналізу;

- слід уникати надмірного обмеження тлумачення терміна “персональні дані”.

Термін “персональні дані”, на думку експертів Робочої групи, варто поділити на 4 основні змістовні блоки, кожен з яких несе в собі певний правовий зміст. У поєднанні ці змістовні блоки утворюють термін “персональні дані” та визначають, чи слід вважати певну інформацію “персональними даними”.

Блок 1 – “Будь-яка інформація”.

Перший блок передбачає широке тлумачення поняття, незважаючи на природу чи зміст інформації і технічний формат, в якому вона представлена. Це означає, що як об’єктивна, так і суб’єктивна інформація про особу у будь-якому обсязі може вважатися “персональними даними” незалежно від технічного носія, на якому вона зберігається. У висновку також обговорюються біометричні дані та юридичні відмінності разом з прикладами, з яких вони можуть бути взяті.

З точки зору природи інформації поняття персональних даних включає в себе будь-які формулювання про людину. Воно охоплює “об’єктивну” інформацію, таку як вміст речовин у крові. Вона також включає “суб’єктивну” інформацію – думки чи оцінки. Останній вид формулювань складає значну частку обробки персональних даних в таких сферах, як банківська справа для оцінки надійності позичальників (“Тит – надійний позичальник”), страхування (“Тит начебто не помре скоро”) або зайнятість (“Тит – гарний працівник і гідний підвищення”). Для того щоб інформацію віднести до категорії “персональних даних”, немає необхідності у перевірці її достовірності. Насправді, правила захисту даних уже передбачають, що інформація може бути недостовірною, і надають суб’єкту персональних даних право на доступ до цієї інформації і оскарження її недостовірності через відповідні засоби правового захисту, такі як механізми оскарження в суді.

З точки зору змісту інформації поняття персональних даних включає дані, які містять будь-яку інформацію. Це стосується як “конфіденційної інформації про особу”, так і “відкритої” інформації. Термін “персональні дані” включає інформацію, яка стосується приватного життя людини “в буквальному значенні слова”, а також інформацію про всі види діяльності, що здійснюються особою, як, наприклад, робочі відносини або економічна чи соціальна поведінка людини. Тому термін включає в себе інформацію про осіб незалежно від їх положень або можливостей (як споживача, пацієнта, найманого робітника, клієнта і т.д.).

Приклад № 1: Професійні звички та практика. Інформація, що міститься у рецепті на ліки (наприклад, ідентифікаційний номер препарату, назва препарату, дія ліків, виробник, ціна продажу, перше або подальше отримання ліків за одним рецептом, показання до застосування препарату, можливість заміни, ім’я та прізвище особи, яка виписала рецепт, його номер телефону тощо), незалежно від того, чи індивідуальна форма рецепта, чи він виписаний “за зразком”, може розглядатися як персональні дані про лікаря, який приписав дані ліки, навіть якщо пацієнт анонімний. Таким чином, надання інформації про рецепти, виписані ідентифікованими лікарями або лікарями, яких можна ідентифікувати, виробникам рецептурних препаратів, слід вважати передачею персональних даних третій особі.

Враховуючи формат інформації або носій, на якому ця інформація міститься, поняття персональних даних включає інформацію, доступну в будь-якій формі – наприклад, символьну, цифрову, графічну, фотографічну або акустичну. Воно включає інформацію на папері, а також інформацію, що зберігається в пам’яті комп’ютера у вигляді двійкового коду або, наприклад, на відеоплівці. Це є логічним наслідком охоплення автоматичної обробки персональних даних сферою її дії. Зокрема, дані про звук і зображення кваліфікуються як персональні дані з цієї точки зору, оскільки вони можуть представляти інформацію про особу. З іншого боку, інформація, що міститься в структурованій базі даних або файлі, не обов’язково має вважатися персональними даними. Крім того, інформація, що міститься у вигляді вільного тексту в електронному

документі, може бути віднесена до персональних даних за умови дотримання інших критеріїв у визначенні персональних даних.

Приклад № 2: Телефонний банкінг. В телефонному банкінгу, якщо голос клієнта, який дає вказівки банку, записується на плівку, ці записані вказівки повинні вважатися персональними даними.

Приклад № 3: Відеоспостереження. Зображення осіб, зафіксовані системою відеоспостереження, можуть бути персональними даними за умови, що осіб на плівці можна впізнати.

Приклад № 4: Дитячий малюнок. В результаті нейро-психіатричної експертизи, проведеної на дівчині в контексті судового розгляду по справі щодо її опіки, був представлений малюнок, зроблений нею, що характеризує її сім’ю. Малюнок містив інформацію про настрій дівчини і про те, що вона думає про членів своєї сім’ї. По суті, малюнок може вважатися “персональними даними”. Він дійсно розкриватиме інформацію про дитину (стан її здоров’я з психіатричної точки зору), а також про, наприклад, поведінку батька або матері. Внаслідок цього батьки можуть скористатися своїм правом доступу до цієї специфічної інформації.

Окремо необхідно розглянути біометричні дані. Ці дані можуть бути визначені як біологічні властивості, фізіологічні характеристики, життєві риси або повторювані дії, які є унікальними для даної людини і вимірюваними, навіть якщо шаблони, які використовуються на практиці для їх технічного вимірювання, містять певний ступінь ймовірності. Типовими прикладами таких біометричних даних є відбитки пальців, зображення сітківки ока, структури обличчя, голос, а також геометрія руки, конфігурація вен або навіть деякі глибоко вкорінені навички або інші характеристики поведінки (такі, як власноручний підпис, натиснення клавіш, певна хода або манера мовлення і т.д.). Особливістю біометричних даних є те, що вони можуть вважатися як змістом інформації про конкретну особу (“Тит має ці відбитки пальців”), так і елементом для встановлення зв’язку між частиною інформації та особою (“до цього об’єкта торкалася якась особа, залишивши відбитки пальців, і ці відбитки пальців належать Титу; таким чином, до цього об’єкта торкався Тит”). Завдяки їх унікальному зв’язку з конкретною особою, біометричні дані можуть використовуватися для ідентифікації особи. Двоїстий характер цих даних проявляється також і у випадку з даними ДНК, які містять інформацію про людське тіло і надають можливість конкретно ідентифікувати особу. Зразки людської тканини (наприклад, зразки крові) є джерелами вилучених біометричних даних, але самі по собі вони не є біометричними даними (як, наприклад, зразок для відбитків пальців є біометричними даними, але самі пальці – ні). Тому вилучення інформації зі зразків є збором персональних даних. Збір, зберігання і використання зразків тканини самі по собі можуть бути предметом окремого правового регулювання [11].

Блок 2 – “що стосується”.

Зазначений блок відіграє важливу роль у визначенні субстантивного обсягу поняття, особливо стосовно об’єктів та нових технологій. У Висновку WP 136 зазначаються три альтернативні елементи, тобто зміст або мета, або результат для визначення чи “стосується” інформація окремої особи. Зазначене також охоплює інформацію, яка може мати явний вплив на те, як відбувається оцінювання або обробка даних людини.

Загалом, інформація може вважатися такою, що “стосується” особи, якщо вона про цю людину. У багатьох випадках цей зв’язок можна легко встановити. Наприклад, дані, зареєстровані в особовій справі людини у відділі кадрів юридичної особи, явно “стосуються” цієї людини як працівника. Такими ж є дані за результатами медичного

обстеження пацієнта, що містяться в його медичній картці, або відеозображення людини, зняте під час відеоінтерв’ю з цією людиною. Можна навести ще ряд інших ситуацій, хоча, в них не завжди так очевидно, як у попередніх випадках, вдається визначити, що інформація “стосується” людини. У деяких випадках інформація, що передається за допомогою даних, стосується, насамперед об’єктів, а не окремих осіб. Такі об’єкти, як правило, належать якійсь особі, можуть бути предметом особливого впливу з боку або у відношенні осіб та можуть знаходитися у фізичній або географічній близькості з особами або з іншими об’єктами. В такому випадку лише опосередковано можна вважати, що інформація стосується тих осіб або тих об’єктів.

Приклад № 5: вартість будинку. Вартість конкретного будинку – це інформація про об’єкт. Правила захисту даних однозначно не застосовуються, якщо ця інформація буде використовуватися виключно для демонстрації рівня цін на нерухомість в певному районі. Тим не менш, за певних обставин така інформація повинна також розглядатися як персональні дані. Дійсно, будинок є майном власника і тому може використовуватися для визначення, наприклад, обсягу зобов’язань цієї людини по сплаті певних податків. У цьому контексті, безсумнівно, така інформація повинна вважатися персональними даними.

З огляду на вищезазначені випадки і за аналогією необхідно зазначити, що для того, щоб можна було вважати, що дані “стосуються” фізичної особи, має бути присутній елемент “змісту” або елемент “цілі”, або елемент “результату”.

Елемент “змісту” присутній в тих випадках, коли – відповідно до найбільш очевидного і загального розуміння в суспільстві слова “стосується” – інформація надається про конкретну людину, незалежно від цілей контролера даних (володільця персональних даних) або третіх осіб, або впливу цієї інформації на суб’єкта персональних даних. Інформація “стосується” людини, якщо вона є даними про цю людину, і це має оцінюватися у світлі всіх обставин справи. Наприклад, результати медичних аналізів безпосередньо стосуються пацієнта або інформація, що міститься у файлі певного клієнта якоїсь компанії, безпосередньо стосується цього клієнта.

Таким же чином елемент “цілі” може обумовлювати той факт, що інформація “стосується” певної людини. Можна вважати, що елемент “цілі” існує, якщо дані використовуються або можуть бути використані з урахуванням всіх обставин певної справи, для оцінки, певного ставлення або впливу на стан чи поведінку людини.

Третій вид “відношення” до конкретних осіб виникає за наявності елементу “результату”. Незважаючи на відсутність елементу “зміст” або “цілі”, можна вважати, що дані “стосуються” особи, коли їх використання може вплинути на права та інтереси певної особи з урахуванням усіх обставин певного випадку. Слід зазначити, що потенційний результат не обов’язково повинен чинити великий вплив. Достатньо, щоб інші особи могли ставитися по-іншому до конкретної особи в результаті обробки таких даних.

Ці три елементи (зміст, ціль, результат) повинні розглядатися як альтернативні (взаємовиключні) умови, а не в сукупності. Зокрема, якщо присутній елемент змісту, для того, щоб вважати, що інформація стосується особи, немає ніякої необхідності для присутності інших елементів. Наслідком цього є те, що одна й та сама інформація може стосуватися різних осіб одночасно залежно від того, який елемент присутній у відношенні до кожної з осіб.

Блок 3 – “фізична особа”.

Персональні дані стосуються лише живих людей. Право на захист персональних даних у цьому сенсі – універсальне право, яке не обмежується лише громадянами певної країни. Поняття фізичної особи зазначено у статті 6 Загальної декларації прав людини, відповідно до якої *кожен має право на визнання будь-де своєї правосуб’єктності* [12].

Законодавство різних держав (у тому числі і в Україні), зазвичай у царині цивільного права, більш точно окреслює поняття людини. Під цим поняттям розуміється здатність бути суб’єктом правовідносин, починаючи від народження особи і закінчуючи її смертю. Тому, в принципі, персональні дані – це дані, що стосуються ідентифікованих живих людей або які можуть бути ідентифіковані. Зазначене порушує низку інших питань в контексті цього аналізу.

Дані про померлих осіб. Інформація стосовно померлих людей в принципі не повинна вважатися персональними даними, оскільки померлі більше не є фізичними особами в сенсі цивільного права. Тим не менше, дані про покійних можуть опосередковано захищатися у певних випадках. З одного боку, контролер даних (володілець персональних даних) може не бути в змозі встановити, чи особа, до якої мають відношення дані, жива або вже померла. Або навіть якщо контролер даних зможе це зробити, інформація про померлих може оброблятися в такому ж режимі, як інформація про живих.

З іншого боку, інформація про померлих осіб може також стосуватися живих осіб, наприклад, інформація про те, що покійна Марія страждала на гемофілію, свідчить про те, що її син Джон також страждає на цю саму хворобу, адже вона пов’язана із генами, що знаходяться у Х-хромосомі. Таким чином, у деяких випадках інформація, що є даними про померлих осіб, може вважатися такою, що одночасно стосується і живих осіб та становить персональні дані. Отже, дані померлих можуть опосередковано підпадати під правила захисту даних.

Ненароджені діти. Міра, в якій правила захисту даних можуть застосовуватися до народження дитини, залежить від загальної позиції національних систем права стосовно захисту ненароджених дітей. Для того щоб, наприклад, врахувати права спадщини, деякі держави визнають принцип, що діти, котрі зачаті, але ще не народжені, вважаються такими, що начебто народилися, коли справа стосується вигод (і таким чином можуть отримати спадщину або прийняти пожертву), за умови, що вони зможуть бути успішно народжені. В інших державах спеціальний захист надається конкретними правовими нормами також з дотриманням цієї ж умови. Щоб визначити, чи положення національного законодавства про захист даних також захищають інформацію про ненароджених дітей, потрібно брати до уваги цей загальний підхід, разом з думкою, що призначення правил захисту даних – захищати дані про особу.

Юридичні особи. Оскільки визначення персональних даних стосується людей, тобто фізичних осіб, інформація стосовно юридичних осіб у принципі не розглядається як персональні дані. Однак, за цілого ряду обставин певні правила захисту персональних даних можуть все одно опосередковано застосовуватися до інформації стосовно юридичних осіб, наприклад, у контексті їх засновників, директорів тощо.

Блок 4 – “ідентифікована або яку можна ідентифікувати”.

В даному блоці зосереджується увага європейських експертів на умовах, за яких індивідуум повинен вважатися *таким, що може бути ідентифікований*, і особливо на *засобах, які ймовірно в розумній мірі будуть використані* контролером даних або будь-якою іншою особою для ідентифікації цієї особи. Конкретний контекст окремого випадку відіграє важливу роль у цьому аналізі. Висновок WP 136 також зачіпає проблему “псевдонімізованих даних” та використання “даних, закодованих ключем” у статичних та фармацевтичних дослідженнях.

Загальне правило зводиться до того, що фізична особа може бути “прямо” або “опосередковано” ідентифікована. Загалом, фізична особа може вважатися “ідентифікованою”, якщо в групі осіб вона “виділяється” з-поміж інших членів групи.

Відповідно, фізична особа є такою, яка “може бути ідентифікована”, якщо, незважаючи на те, що її ще не було ідентифіковано, це можливо зробити.

Додаткове роз’яснення з цього питання міститься в повідомленні Європейської комісії COM (92) 422 [13]. У повідомленні зазначається, що *людина може бути ідентифікована прямо за допомогою імені або опосередковано за допомогою номера телефону, номера автомобіля, номера соціального страхування, номера паспорта або поєднання важливих критеріїв, які дозволяють йому бути визнаним шляхом звуження групи, до якої він належить (вік, рід занять, місце проживання і т.д.).* Зазначене свідчить, що достатній ступінь деяких ідентифікаторів для досягнення ідентифікації людини залежить від контексту конкретної ситуації. Дуже поширеного імені та/або прізвища може бути недостатньо, щоб ідентифікувати особу, тобто виділити когось з усього населення країни. Проте, цього може бути достатньо для ідентифікації, наприклад, учня в класі. Навіть допоміжна інформація, наприклад, “людина в чорному костюмі” може ідентифікувати когось з перехожих, що стоять на світлофорі. Таким чином, питання про те, чи може бути ідентифікована особа, якої стосується певна інформація чи ні, залежить від обставин ситуації.

Запропонований європейський підхід до визначення терміна “персональні дані” є досить конструктивним. У цілому ж запропоноване українським законодавцем визначення терміна “персональні дані” у статті 2 Закону України “Про захист персональних даних” (“персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована”) змістовно відповідає зазначеним термінам, визначеним у Конвенції Ради Європи № 108 про захист осіб у зв’язку з автоматизованою обробкою персональних даних та в Директиві 95/46/ЄС. Проте, на думку автора статті, визначення терміна “персональні дані” в Законі України “Про захист персональних даних” потребує стилістичного доопрацювання.

Висновки.

Комплексний аналіз терміна “персональні дані” згідно з європейським підходом до формування та визначення його правового змісту свідчить про необхідність запровадження на рівні національного законодавства якомога більш загального його визначення, з тим щоб охопити всю інформацію, яка стосується фізичної особи, яку можна прямо або опосередковано ідентифікувати.

Термін “персональні дані”, визначений в українському законодавстві, змістовно відповідає європейському підходу до його визначення, проте потребує стилістичного перегляду з метою чіткого визначення його складових у контексті прямої або опосередкованої ідентифікації фізичної особи.

З огляду на зазначене пропонується викласти абзац десятий статті 2 Закону України “Про захист персональних даних” у такій редакції: *персональні дані – відомості чи сукупність відомостей про фізичну особу, яка може бути конкретно ідентифікована або ідентифікована у будь-який можливій спосіб.*

Варто зазначити, що даний термін потребує перегляду й у інших законах та підзаконних актах, які прямо чи опосередковано регулюють питання захисту персональних даних.

Використана література

1. Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights adopted on 7 September 1999. – The Working Party on the Protection of Individuals with regard to the Processing of Personal Data. – Brussels, 1999. – Режим доступу : //www.ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp26en.pdf

2. Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних // Офіційний вісник України. – 2011. – № 1. – С. 701.

3. Додатковий протокол до Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних // Офіційний вісник України. – 2011. – № 1. – С. 708.

4. Про захист персональних даних : Закон України від 01.06.10 р. № 2297-VI // Офіційний вісник України. – 2010. – № 49. – С. 199.

5. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних : Директива Європейського парламенту і Ради № 95/46/ЄС. – Режим доступу : //www.zakon.rada.gov.ua/laws/show/994_242

6. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the regions “A comprehensive approach on personal data protection in the European Union”. – Режим доступу : //www.ec.europa.eu/health/ data_collection/ docs/ com_2010_0609_en.pdf

7. Захист осіб у зв’язку з автоматизованою обробкою персональних даних в контексті їх профілювання : Рекомендації Комітету міністрів Ради Європи державам-членам № CM/Rec (2010) / Мервінський О.І., Козак В.Ф., Мельник К.С. – (Захист персональних даних : міжнародні стандарти : збірник нормативно-правових документів). – К. : Видавництво Подоліна І.В., 2013. – 812 с.

8. Commission Communication COM (90) 314 on the protection of individuals in relation to the processing of personal data in the Community and information security. Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data. – Режим доступу : //www.aei.pitt.edu/3768/1/3768.pdf

9. Commission Communication COM (92) 422: Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. – Режим доступу : //www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:1992: 311:0030:0061:EN:PDF

10. Про концепції персональних даних : Висновок Робочої групи із захисту даних, утвореної відповідно до статті 29 Директиви 95/46/ЄС (WP 136) від 20.06.07 р. / О.І. Мервінський, В.Ф. Козак, К.С. Мельник – (Захист персональних даних : міжнародні стандарти : збірник нормативно-правових документів). – К. : Видавництво Подоліна І.В., 2013. – 812 с.

11. Про дослідження біологічних матеріалів людського походження : Рекомендація Комітету міністрів Ради Європи державам-членам № Rec (2006) 4. – Режим доступу : //www.wcd.coe.int/ViewDoc.jsp?id=977859

12. Загальна декларація прав людини. – Режим доступу : //www.zakon4.rada.gov.ua/laws/show/995_015

13. Commission Communication COM (92) 422 : Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.. – Режим доступу : //www.eur-lex.europa.eu/LexUriServ/Lex UriServ.do?uri=OJ:C:1992 :311:0030:0061:EN:PDF

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342:007

БАРАНОВ О.А., *кандидат технічних наук,*
лауреат Державної премії України в галузі науки і техніки

ОБ’ЄКТ ПРАВОВІДНОСИН В ІНФОРМАЦІЙНОМУ ПРАВІ

Анотація. *До проблеми визначення об’єкту правовідносин в інформаційному праві.*
Ключові слова: *правовідносини, об’єкт, інформаційне право.*

Аннотация*. К проблеме определения объекта правоотношений в информационном праве.*
Ключевые слова: *правоотношения, объект, информационное право.*

Summary. *To the problem of decision of object of legal relationships in an informative right.*
Keywords: *legal relationships, object, informative right.*

Постановка проблеми. У теорії права проблематиці визначення об’єкта правовідносин завжди приділялася особлива увага. У результаті тривалої дискусії сформувалися дві основні теорії об’єкта правовідносини: моністичний (теорія єдиного об’єкта) і плюралістична (теорія множинності об'єктів).

Яскравими виразниками ідей моністичного підходу є О.С. Іоффе, який вважав, що об’єкт правовідносин – людська поведінка, діяльність або дії людей [4], а також Ю.К. Толстой [22, с.60], який стверджував, що об’єктом правовідносин можна визнавати лише майбутнє, тобто можливу поведінку суб’єкта.

На думку С.С. Алексєєва, об’єктами правовідносин виступають явища (предмети) матеріального і духовного світу, тобто різноманітні матеріальні та нематеріальні блага, здатні задовольняти потреби суб’єктів [1]. Це визначення, по суті, є квінтесенцією змісту плюралістичної теорії об’єкта правовідносин, яку розвивали С.Ф. Кечекьян [5], В.Н. Протасов [17], О.Ф. Скакун [19], Н.І. Матузов [20], Є.В. Єрмолаєва [3], А.Є. Юріцин [24], А,С. Бондарєв [2]. Слід визнати вірним висновок О.В. Зайчука та Н.М. Онищенко про те, що багато хто з авторів намагаючись знайти оптимальне і адекватне рішення та відповісти на загальне питання, що таке об’єкт правовідносин, висказують не тільки відмінні точки зору, а й ті, що доповнюють одна одну [21].

Особливої актуальності ця наукова дискусія набуває у зв’язку з визначенням теоретичних основ формування та розвитку нових галузей права тому, що саме це питання є засадничим при вивченні питання предмету та методу правового регулювання.

Метою статті є розгляд особливостей визначення об’єкту правовідносин в інформаційному праві, як нової галузі права.

Аналіз останніх досліджень і публікацій. М.І. Матузов вважаючи, що об’єктом правових відносин виступає те, на що спрямовані суб’єктивні права і юридичні обов’язки його учасників, іншими словами те, заради чого саме виникають правовідносини, дав розгорнуте визначення множинного об’єкта правовідносин, до якого він відносить [20]:

1. Матеріальні блага (речі, предмети, цінності).

2. Нематеріальні особисті блага (життя, честь, здоров’я, гідність, свобода, безпека, право на ім’я, недоторканність людини) .

3. Поведінка, дії суб’єктів, різного роду послуги та їх результати.

4. Продукти духовної творчості (твори літератури, мистецтва, живопису, музики, скульптури, а також наукові відкриття, винаходи, раціоналізаторські пропозиції – все те, що є результатом інтелектуальної праці).

5. Цінні папери, офіційні документи (облігації, акції, векселі, лотерейні квитки, гроші, приватизаційні чеки, паспорти, дипломи, атестати тощо).

До цього переліку А.Є. Юріциним додаються ще й результати поведінки учасників правовідносин (це наслідки, до яких призводить та чи інша дія) [24].

Досить широке визначення дають О.В. Зайчук і Н.М. Онищенко вважаючи, що об’єкти правовідносин настільки різноманітні, наскільки різноманітні правовідносини, що регулюються правом [21], при цьому вони погоджуються з конкретизацією об’єкта правовідносин, наданої М.І. Матузовим.

Раціонально підійшов до визначення Б.А. Кормич визначаючи в якості об’єкта інформаційних правовідносин документовану або публічно оголошену інформацію про події та явища у сфері політики, економіки, культури, охорони здоров’я, а також у соціальній, екологічній, міжнародній та інших сферах [9, с. 56]. По суті справи це дещо трансформована моністична позиція.

В.Н. Протасовим об’єкт правовідносини визначено як явище зовнішнього світу, здатне задовольнити інтерес правомочної особи, яке виступає у вигляді речі, послуги, продукту духовної творчості або особистого нематеріального блага, заради якого і діють суб’єкти правовідносин в рамках своїх юридичних прав та обов’язків [17].

Виклад основного матеріалу. Слід зауважити, що методологічно визначення, надане В.М. Протасовим, є більш змістовним і продуктивним для подальшого використання. Але при цьому необхідно уникати надмірної перевантаженості дефініції. Саме такий підхід буде використаний нами надалі при формулюванні відповідних дефініцій.

Звернемо увагу на іншу проблему у визначенні об’єкта правовідносин. Іноді правовідносини, об’єктом яких виступає, наприклад, режим доступу або використання інформації, відбуваються з метою задовольнити потреби або інтерес не тільки суб’єктів цих правовідносин, як про це, говорить А.В. Міцкевич [13], стверджуючи, що тільки суб’єкт правовідносин може бути зацікавленою стороною, але і з метою задоволення потреб або інтересів третіх осіб. Наприклад, вимоги перевіряючих органів про необхідність розміщення конкретної інформації про діяльність органу виконавчої влади на сторінках веб-сайту є правовідносинами, результати яких задовольняють інтереси третіх осіб. До подібних правовідносин можна віднести велику їх частину, яка регулюється нормами, що носять публічно-правовий характер.

У відповідності з класичною теорією правовідносин, яка базується на жорстко однозначному визначенні конкретних об’єкта, суб’єктів і суб’єктивних прав і обов’язків, без втрати її логічності, не можна визнати наявність якихось третіх невизначених суб’єктів. Тому в теорії права виникла дискусія про доцільність введення поняття абсолютних, статусних, базових, вихідних або первинних правовідносин, що покликані виконувати функцію загальнорегулятивних правовідносин [20]. Деякі дослідники не підтримували зазначену точку зору [22, 23, с. 30], проте сучасні реалії практики правового регулювання та розвитку правової науки призвели до ситуації поступового визнання правильності введення поняття загально регулятивних правовідносин. Щодо інформаційної сфери, то це виправдовується наявністю досить великої кількості правових норм, що носять публічно-правовий характер.

Прихильницею плюралістичного напряму в теорії правовідносин З.Г. Криловою справедливо стверджується, що в якості об’єкта правовідносин виступає поведінка його суб’єктів, спрямована на досягнення юридичних наслідків [15].

Цілком обґрунтовано В.К. Бабаєв робить висновок про те, що іноді метою правовідносин є результат поведінки – “багато правовідносин і встановлюються заради

того, щоб шляхом поведінки осіб домогтися певного результату, в цьому випадку не поведінка буде об’єктом правовідносини, а саме результат поведінки” [12]. Також В.В. Копейчиков крім дій суб’єктів правовідносин, також відносить до об’єкту правовідносин і результати цих дій [16].

У роботі присвяченій дослідженню об’єкта інформаційних правовідносин, Л.П. Коваленко стверджує, що до основних елементів таких правовідносин відноситься поведінка (дії, бездіяльність) суб’єктів при здійсненні ними інформаційних відносин (наприклад, придбання виключних прав, передача майнових прав, купівля-продаж інформаційних об’єктів, тиражування та розповсюдження інформаційних об’єктів та інші аналогічні дії) [6]. Крім того, що автор вводить до складу об’єкта правовідносин поведінку їх суб’єктів, вона показує, що ця поведінка стосується не тільки обороту інформації, а також стосується процесів, пов’язаних із забезпеченням цього обороту.

Об’єктивні дані свідчать про те, що реальна поведінка суб’єктів правовідносин не завжди відповідає змісту їх форми, тобто змісту правової норми. Пояснюючи це явище В.А. Кодавбовіч і В.А. Кучинський вважають, що найбільш вірно, теоретично обґрунтовано розглядати в якості форми правовідносини тільки суб’єктивні права та обов’язки його сторін, які чітко визначають рамки можливої та належної їх поведінки, що становить реальний зміст суспільних відносин між ними [7]. Цей висновок видається правильним, оскільки поведінка суб’єктів суспільних відносин є проявом волі конкретних індивідуумів, вільних в ухваленні рішень і у своїх вчинках. Вони можуть бути і протиправними в конкретних правовідносинах, коли суб’єктами цих правовідносин не будуть виконуватися відповідні права або обов’язки.

З іншого боку, О.П. Копиленко в якості об’єкта правовідносини визнає тільки: матеріальні – предмети матеріального світу, предмети споживання, нерухомість, предмети домашнього вжитку, твори мистецтва тощо; нематеріальні – духовні цінності, морально-психологічний стан людини тощо [8]. Аналогічну позицію займає О.Ф. Скакун вважаючи, що до об’єкта правовідносин можна віднести тільки предмети матеріального світу, послуги виробничого і невиробничого характеру, продукти духовної та інтелектуальної творчості, особисті немайнові блага [19].

Автор фундаментальної монографії з теорії правовідносин Р.О. Халфіна стверджує, що форма правовідносини (норма права – *Авт.*) впливає на зміст суспільних відносин не тільки закріплюючи певні акти, вчинки, дії або бездіяльність в якості прав і обов’язків, а й обумовлюючи відповідність, логічний зв’язок всього комплексу актів поведінки, всієї лінії поведінки з встановленими правами та обов’язками [23, с.213]. У цій же роботі Р.О. Халфіна більш однозначно сказала – оскільки все що стосується особистих благ, послуг, прав, складає зміст правовідносини, тому сюди відноситься все сказане з приводу включення в об’єкти права поведінки або матеріального змісту відносин [23, с. 215].

Дійсно, юридичний зміст правовідносин встановлює юридичні права та обов’язки, які можуть бути реалізовані тільки за допомогою певної поведінки їх суб’єктів або через певні дії цих суб’єктів. Більше того, юридичні права і обов’язки найчастіше можуть вважатися реалізованими тільки в тому випадку, якщо було досягнуто конкретний результат. Або іншими словами, абстрактна модель правомірної поведінки суб’єктів правовідносин, обумовлена конкретними юридичними правами та обов’язками може вважатися реалізованою в конкретному випадку тільки тоді, коли буде досягнуто результат, який може бути сприйнятий як належний та відповідний заданій абстрактної моделі.

Незважаючи на недостатність певної стрункості в теоретичних положеннях різних послідовників плюралістичного підходу, слід зазначити, що розділяючи думку багатьох авторів будемо вважати, що саме ця теорія найбільш близька до реалій правового регулювання. Ґрунтуючись на плюралістичному підході, сформулюємо наступне визначення: *об’єкт правовідносин – це матеріальні та нематеріальні блага, що задовольняють потреби та інтереси, як суб’єктів даного правовідношення, що діють в рамках своїх юридичних прав та обов’язків, так і інших суб’єктів, та виступають у вигляді: речей, документів, продуктів духовної творчості, особистого нематеріального блага, послуг або робіт та їх результатів, результатів поведінки та дії.*

В якості основи для теоретичної характеристики об’єкта правових відносин в інформаційній сфері, як частині загальної теорії правовідносин, доцільно також обрати плюралістичний підхід.

Дотримуючись зазначеного підходу Д.В. Огородов пропонує вважати об’єктом правових відносин в інформаційній сфері або певну інформацію, або безпосередньо пов’язаний з інформацією результат поведінки учасника правовідносини (надання, одержання, нерозголошення інформації та ін.) Або іншими словами, правовідносини в інформаційній сфері їм запропоновано визначати як врегульовані нормами права суспільні відносини, що виникають з приводу інформації або юридично значимих результатів дій (бездіяльності) з інформацією (передача, отримання, нерозголошення тощо) [14].

На думку Д.А. Ловцова особливі об’єкти інформаційних правовідносин дозволяють виділити їх в особливий рід правовідносин [11]. До таких особливих об’єктів він відносить: інформаційно-правовий режим та пов’язаною з ним інформаційною діяльністю в інформаційній сфері. Далі Д.А. Ловців наводить еклектично складену класифікацію інформаційних правовідносин, що складається з чотирьох підкласів у сфері: засобів забезпечення інформаційної безпеки особистості, суспільства і держави; ЗМІ; засобів автоматизації і ЕОТ; засобів телематики. Навіть при поверхневому аналізі видно, що ця класифікація, віддаючи деяку данину питанням інформаційної інфраструктури, не охоплює певні пласти реальних правовідносин в інформаційній сфері: наприклад, правовідносин, пов’язаних із створенням, розповсюдженням (передачею) і зберіганням інформації.

У той же час слід звернути увагу на позицію Д.А. Ловцова щодо інформаційно-правового режиму. Дійсно, на перший погляд, здається, що наприклад, встановлення правового режиму обмеження доступу до конкретних видів інформації не охоплюється класифікацією об’єктів правовідносин, що запропонована С.С. Алексєєвим (різноманітні матеріальні і нематеріальні блага, здатні задовольняти потреби суб’єктів), і тому представляє собою щось особливе. Але якщо простежити діалектичний зв’язок встановлення правового режиму обмеження доступу до інформації, то виявиться, що це робиться в інтересах конкретних суб’єктів з метою уникнути певної шкоди від несанкціонованого використання такої інформації.

Недостатньо стрункo і логічно визначають інформаційне правовідношення та його предмет М.А. Лапіна, А.Г. Ревін і В.І. Лапін. Відстоюючи начебто плюралістичний підхід, вони стверджують, що реалізація прав і обов’язків суб’єктів інформаційного правовідношення може бути пов’язана не тільки з їх поведінкою і діями (правомірними чи неправомірними), а і з речовими правами або продуктами творчої діяльності, а також з особистими нематеріальними благами, наприклад, при охороні честі і гідності громадян, захисті конфіденційної інформації тощо [10]. Але надалі непослідовно

заявляють, що об’єктом інформаційно-правових відносин є дії сторін (учасників правовідносин), а предметом правовідносин – інформація в різній формі та вигляді.

У рамках дослідження суб’єкта правовідносин у сфері засобів масової інформації Р.С. Свистовичем також була обрана плюралістична концепція об’єкта правовідносини [12]. Дотримуючись плюралістичного підходу В.М. Боєр і О.Г. Павельєва висловлюють досить дискусійну ідею про те, що в якості об’єкта інформаційних правовідносин інформація може виступати як [25]:

– товар у процесах її створення, зберігання та використання, передачі та розповсюдження;

– джерело для прийняття рішень;

– джерело отримання знань при освіті та вихованні в процесах здійснення конституційного права на освіту;

– засіб сповіщення суспільства про події та явища (через ЗМІ) у порядку здійснення конституційного права на інформацію;

– засіб звітності про діяльність юридичних і фізичних осіб (податкова звітність, бухгалтерська звітність, статистична звітність тощо);

– засіб реалізації прав і свобод особистості через надання відомостей про особу різним структурам (право на життя, право на житло, право на медичну освіту, право на виховання, право на працю тощо);

– засіб, за допомогою якого реалізуються певні цілі (отримання прибутку, залучення клієнтів тощо).

В інформаційній сфері до об’єкта правовідносини у відповідності з раніше сформульованим його визначенням доцільно віднести ті об’єкти правовідносини, з приводу яких вони виникають в процесі обороту інформації, тобто при створенні, поширенні, використанні, зберіганні та знищенні інформації, або в процесі забезпечення цього обороту, тобто в процесі функціонування елементів інформаційної інфраструктури. Тому для інформаційної сфери в якості об’єкта інформаційних правовідносин визначимо наступне.

1. Матеріальні блага – речі (інформаційні продукти, особисті папери і документи).

При цьому інформаційними продуктами можуть бути твори літератури, мистецтва, живопису, музики, книги, журнали, кіно-, відео- та фотоматеріали, аудіо твори, наукові відкриття, винаходи, раціоналізаторські пропозиції, результати інформаційних робіт і послуг, аналітичні звіти, звіти про проведені дослідження, у тому числі наукові, статистичні звіти тощо.

Слід зауважити, що визнання інформації (інформаційних продуктів) в якості речі, що відбулося в практичній діяльності де факто, вимагає і юридичного визнання шляхом зміни правової доктрини. Крім того, таке визнання також дозволяє уникнути такого штучного утворення як – “продукти духовної творчості”, як результату інтелектуальної праці. Це дозволить підійти до правового регулювання суспільних відносин, пов’язаних з інформацією будь-якого виду з єдиних доктринальних позицій.

Під особистими паперами розуміються документи, фотографії, щоденники, інші записи, особисті архівні матеріали тощо фізичної особи.

Документи – в їх якості можуть виступати цінні папери, векселі, розписки, сертифікати (грошові), розрахункові чеки, ліцензії, паспорта, дипломи, атестати тощо.

Більш предметно до визначення дефініцій термінів “інформаційний продукт” і “документ” слід звернутись в рамках обговорення проблеми термінології інформаційного права.

2. Нематеріальні особисті блага – право на свободу слова, право на інформацію, право на захист персональних даних, авторське право, право інтелектуальної власності тощо.

3. Поведінка та дії суб’єктів правовідносин в інформаційній сфері, а також результати поведінки та дій.

З урахуванням вищесказаного дамо таке визначення дефініції: *об’єкт інформаційних правовідносин – це матеріальні та нематеріальні блага, що задовольняють потреби та інтереси, як суб’єктів даного правовідношення, що діють в рамках своїх юридичних прав та обов’язків, так і інших суб’єктів, та виступають у вигляді: інформаційних продуктів, особистих паперів, документів, особистого нематеріального блага, послуг і робіт, а також їх результатів, результатів поведінки та дії в процесі обороту інформації або забезпечення цього обороту.*

Висновки.

Теоретичні питання в окремій галузі права повинно досліджувати в контексті положень загальної теорії права, тому дослідження визначення суб’єкту правовідношень в інформаційному праві базувались на результатах відповідних досліджень правовідношень в загальній теорії права. Отримані результати проведеного дослідження є дуже важливими з огляду на подальше вивчення питань предмету та методу правового регулювання в інформаційній сфері.

Використана література

1. Алексеев С.С. Общаятеория права : в 2-х т. – Т. 2 / С.С. Алексеев. – М. : “Юрид. лит.”, 1981. – 360 с. – Режим доступа : //www.kursach.com/biblio/0010003/030.html

2. Бондарев А.С. Два типа правоотношений в обществе : их единство и различия / А.С. Бондарев // Вестник Пермского университета. – 2011. – № 1. – С. 7-18. – (Серия “Юридические науки”).

3. Ермолаева Е.В. Объектправоотношения : историко-теоретическоеисследование / Е.В. Ермолаева : автореф. дис. на соискание учен. степ. канд. юрид. наук : спец. 12.00.01. – Казань, 2004. – 25 с. – Режим доступа : //www.dissercat.com/content/obekt-pravootnosheniya-istoriko-teoreticheskoe-issledovanie

4. Иоффе О.С. Правоотношение по советскому гражданскому праву / О.С. Иоффе. – Л. : Изд-во ЛГУ, 1949. – 143 с. – Режим доступа : //www.law.edu.ru/script/cntSource.asp?cntID=100083361

5. Кечекьян С.Ф. Правоотношения в социалистическом обществе / С.Ф. Кечекьян. – М. : Изд-во АН СССР, 1958. – Режим доступа : //www.pravo.vuzlib.net/book_z622_page_23.html

6. Коваленко Л.П. Об’єкт інформаційних правовідносин / Л.П. Коваленко // Право і безпека. – 2012. – № 5. – С. 78-83.

7. Кодавбович В.А. Содержание правоотношений : права и обязанности или поведение сторон? / В.А. Кодавбович, В.А. Кучинский // Юридический журнал. – 2007. – № 2. – С. 47-51. – Режим доступа : //www.media.miu.by/files/store/items/uj/10/urjournal_10_2007_10.pdf

8. Копиленко О.П. Правознавство / О.П. Копиленко, Л.І. Мозговий. – К. : Професіонал ВД, 2007. – 400 с. – Режим доступа : //www.pidruchniki.ws/15941024/pravo/pravovidnosini_pravomirna_povedinka_pravoporushennya

9. КормичБ. А. Информационное право / Б.А. Кормич. – Х. : БУРУН и К., 2011. – 334 с.

10. Лапина М.А. Информационное право : учеб. пособие ; под ред. И.Ш. Килясханова / М.А. Лапина, А. Г. Ревин, В. И. Лапин. – М. : Закон и право, 2004. – 335 с.

11. Ловцов Д.А. Информационные правоотношения : особенности и продуктивная классификация / Д.А. Ловцов // Информационное право. – 2009. – № 1. – С. 3-6. – Режим доступа : //www.recoveryfiles.ru/laws.php?ds=3089

12. Общая теория права : курс лекцій ; под общей редакцией профессора В.К. Бабаева. – Нижний Новгород : 1993. – 488 с. – Режим доступа : //www.kursach.com/biblio/0010004/1402.html

13. Общая теория права : учебник для юридических вузов / [Ю.А. Дмитриев, И.Ф. Казьмин, В.В. Лазарев и др.] ; под. общ. ред. А.С. Пиголкина. – [2-е изд., испр. и доп.]. – □ М. : Изд-во МГТУ им. Н.Э. Баумана, 1998. – 384 с.

14. Огородов Д.В. Правовые отношения в информационной сфере : автореф. дис. на соискание учен. степени канд. юрид. наук : спец. 12.00.14 – Административное право; финансовое право; информационное право / Д.В. Огородов. – М., 2002. – 25 с. – Режим доступа : //www.law.edu.ru/book/book.asp?bookID=117440

15. Основы права : учебник / [З.Г. Крылова, Э.П. Гаврилов, В.И. Гуреев и др.] ; под ред. З.Г. Крыловой. – М. : Высш. шк., 2000.□ – 400 с. – Режим доступа : //www.bibliotekar.ru/osnovy-prava-2/10.html

16. Правознавство : підручник ; за ред. В.В. Копєйчикова, А.М. Колодія. – К. : Юрінком Інтер, 2006. – 748 с.

17. Протасов В.Н. Теория права и государства. Проблемы теории права и государства : вопросы и ответы / В.Н. Протасов. – М. : Новый Юрист, 1999. – 240 с. – Режим доступа : //www.zipsites.ru/books/teor_gos_vop

18. Свистович Р.С. Правове регулювання інформаційних відносин у сфері масової інформації : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право / Р.С. Свистович. – К. : Нац. ун-т біоресурсів і природокористування України, 2011. – 24 с. – Режим доступа: //www.mydisser.com/ua/catalog/view/6/352/9514.html

19. Скакун О.Ф. Теорія держави і права : підручник ; [пер. з рос.] / О.Ф. Скакун. – Харків : Консум, 2001. – 656 с. – Режим доступу : //www.politics.ellib.org.ua/pages-1687.html

20. Теория государства и права : курс лекций ; под ред. Н.И. Матузова и А.В. Малько. – [2-е изд., перераб. и доп.]. М. : Юристъ, 2001. – 776 с. – Режим доступа : //www.alleng.ru/d/jur/jur052.html

21. Теорія держави і права. Академічний курс : підручник ; за ред. Зайчука О.В., Оніщенко Н.М. – К. : Юрінком Інтер, 2008. – 688 с. – Режим доступу : //www.ebk.net.ua/Book/law/zaychuk_tdp/part3/1805.html

22. Толстой Ю.К. К теории правоотношения / Ю.К. Толстой. – Ленинград : из-во Ленинградского ун-та, 1959. – 88 с. – Режим доступа : //www.pravo.vuzlib.org/book_z694_page_16.html

23. Халфина Р.О. Общее учение о правоотношении / Р.О. Халфина. – М. : Юридическая литература, 1974. – 340 с. – Режим доступа : //www.pravoznavec.com.ua/books/3/101/17/#chapter

24. Юрицин А.Е. Объекты правоотношений : монистический и плюралистический подходы исследования проблемы / [Н.В. Бондарчук, А.Е. Юрицин, А.Б. Лавров] : *материалы конф. [Кадровое обеспечение региональной экономики и управления : правовое поле, проблемы и перспективы]* / Сибирская Ассоциация непрерывного образования, 2007. – Режим доступа : //www.sano.ru/publik/Fev_konf/37.doc

25. Боер В.М. Информационное право : учеб.пособие. Ч. 1 / В.М. Боер, О.Г. Павельева. – СПб. : ГУАП, 2006. – 116 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 351.810:340.11:340.12

ЯРЕМЕНКО О.І., *кандидат наук з державного управління, доцент*

СУТНІСТЬ ТА СОЦІАЛЬНО-ПРАВОВА ПРИРОДА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Анотація. *Проаналізовано теоретичні проблеми соціально-правової сутності інформаційної діяльності, її місце та роль в системі соціальної діяльності людини, досліджено інформаційну діяльність в загальносоціальному та вузькоюридичному розумінні.*

Ключові слова: *соціальна діяльність, інформаційна діяльність, інформаційна сфера, правове регулювання інформаційної діяльності.*

Аннотация. *Проанализированы теоретические проблемы социально-правовой сущности информационной деятельности, ее место и роль в системе социальной деятельности человека, исследовано информационную деятельность в общесоциальном и узкоюридическом аспектах.*

Ключевые слова: *социальная деятельность, информационная деятельность, информационная сфера, правовое регулирование информационной деятельности.*

Summary. *The theoretical problems of social and legal essence of informational activity, its place and role, are analyzed in the system of social activity of human, informational activity is explored in the in general social and narrow legal understanding.*

Keywords: *social activity, informational activity, informational sphere, legal regulation of informational activity.*

Постановка проблеми. Соціальна сутність людини знаходить свій прояв в її зовнішній активності, одним з основних видів якої є діяльність. Саме завдяки діяльності розвиваються всі суспільні сфери і відбувається соціальний прогрес. При цьому, соціальна діяльність людини є явищем історичним, а процеси виникнення та трансформації її видів обумовлюється рівнем розвитку соціуму та динамікою індивідуальних і суспільних потреб.

Інформаційна діяльність як один із видів діяльності завжди мала особливе значення, оскільки інформаційна взаємодія є необхідною умовою існування як кожного суб’єкта окремо так і суспільства в цілому. На сучасному етапі розвитку суспільства відбувається активізація цього виду діяльності, що обумовлюється зростанням попиту на інформацію, інформаційні продукти та послуги. Як наслідок, набуває поширення тенденція перерозподілу співвідношення між діяльністю в матеріальній та нематеріальній сферах, а також посилюється їх взаємовплив. Ключове значення має той факт, що в умовах інформаційного суспільства інформація стає не тільки основою збагачення, а й найважливішою умовою суспільного виробництва, а її особливий статус полягає в її домінуючому впливі на результати виробництва [1, с. 296].

У процесі інформаційної діяльності виникають інформаційні відносини, які потребують правового регулювання, що призводить до виникнення нової комплексної галузі – інформаційного права. Упорядкування інформаційної діяльності правовими засобами ускладнює доволі широкий спектр її характеристик та вимірів, що передбачає використання юриспруденцією досліджень цього феномену іншими суспільними науками. Як зазначає Бачило І.Л., інформаційне право буде ефективним тільки тоді, коли у свою орбіту включить результати системних досліджень економіки, інформатики, соціології і психології та інших суміжних наук в цій галузі [2, с. 15]. Зазначене може свідчити про актуальність подальших досліджень сутності та соціально-правової природи інформаційної діяльності.

Аналіз останніх досліджень. Правові аспекти інформаційної діяльності є предметом дослідження у працях вітчизняних науковців Арістової І.В., Баранова О.А., Бєлякова К.І., Брижка В.М., Бєлєвцевої В.В., Гавловського В.Д., Калюжного Р.А., Кохановської О.В., Марущака А.І., Настюка В.Я., Пилипчука В.Г., Савінової Н.А., Святоцького О.Д., Сосніна О.В., Тихого В.П., Швеця М.Я. та інших.

Разом з тим, подальшого науково-теоретичного обґрунтування потребують окремі соціально-правові аспекти інформаційної діяльності.

Метою статті є дослідження теоретичних проблем соціально-правової сутності інформаційної діяльності, її місця та ролі в системі соціальної діяльності людини, аналіз інформаційної діяльності в загально-соціальному та вузькоюридичному розумінням та її класифікація.

Виклад основних положень. Розкриття соціально-правової природи інформаційної діяльності, передзусім передбачає попереднє з’ясування сутності діяльності як категорії суспільного буття.

Загальнотеоретичні дослідження соціальної діяльності активно розпочалися проводитися фахівцями в галузі суспільних наук ще в 70 – 80 роках ХХ-го століття та мають методологічне значення і до сьогодні. Як зазначає Маргуліс А.В., дослідження суспільства як системи діяльності дозволяє з’ясувати основні структурні елементи суспільного організму, проаналізувати стимули конкретного акту дії, зрозуміти процеси соціологізації особистості, весь комплекс взаємопов’язаних видів і сфер діяльності, і, врешті решт, дослідити внутрішню логіку суспільного розвитку [3, с. 3].

Болгарський дослідник Ніколов В. також розглядає соціальну діяльність в якості ключового методологічного аспекту пізнання суспільства та людини і виділяє три її основні риси: по-перше, діяльність – це особливий спосіб існування і розвитку людини; по-друге, діяльність – це спосіб взаємодії людини з оточуючим середовищем, суть якого полягає у створенні умов для свого існування; по-третє, діяльність – це особлива властивість і здатність людини, специфічний вид і форма її життєвої активності, яка суттєво відрізняється від всіх життєвих процесів тим, що змінює світ на основі засвоєння і розвитку форм культури [4, с. 8].

У загальнотеоретичному аспекті соціальну діяльність можна розглядати як різносторонній процес створення суспільним суб’єктом умов для свого існування і розвитку, як процес перетворення соціальної реальності у відповідності із суспільними потребами, метою і завданнями [5, с. 57].

Інформаційна діяльність в системі соціальної діяльності відіграє особливу роль. Насамперед, як зазначає ряд учених у галузі соціальної філософії, інформаційна складова наявна у всіх видах діяльності людини. Так, Маркарян Е.С. трактує діяльність як інформаційно скоректовану активність живих систем, яка виникає на основі їх ставлення до оточуючого середовища з метою самопідтримки [6, с. 13]. Дьомін М.В. кваліфікує діяльність як інформаційно спрямовану обґрунтовану активність людини, яка базується на знаннях і включає в себе сукупність інтелектуальних, оціночно-емоційних та практичних аспектів [7, с. 21]. Афанасьев В.Г. зазначає, що жоден з видів соціальної діяльності неможливий без теоретичної, пізнавальної діяльності щодо отримання і використання знань [8, с. 43].

Незважаючи на це, тривалий час у класифікаційних системах соціальної діяльності, запропонованих суспільними науками, інформаційна діяльність, як самостійних вид, не виокремлювалася, а розглядалася як елемент духовної діяльності. Аналіз духовної діяльності і виділення її в окремий вид здійснювався на основі методологічного принципу, згідно з яким конститутивною характеристикою будь-якої діяльності є її

предметність. Як зазначав Леонтьєв А.В., головним, що відрізняє одну діяльність від іншої, є відмінність їх предметів, адже саме предмет діяльності і надає їй певну спрямованість. При цьому, предмет діяльності може бути як матеріальним так і ідеальним, існуючим в об’єктивній формі чи у свідомості та уявленні людини [9, с. 84].

Саме на основі предмета науковці виділяли матеріальну (виробничу, практичну) та духовну діяльність. Згідно з таким підходом у результаті практичної діяльності виникають матеріальні блага, відбувається відновлення і перетворення соціальних умов, суспільних відносин та інститутів, а також відновлення і розвиток людини. Духовна ж діяльність розглядалася як процес цілеспрямованого систематичного відображення дійсності, що проявляється у формах наукового пізнання, прогнозування, програмування тощо. До предметів духовної діяльності відносили суспільні відносини, форми суспільного життя, різноманітні організації та інститути, системи управління, способи діяльності, норми її регулювання і всі складові суспільної свідомості, знання, ідеї тощо [5, с. 79].

Багатовимірність духовної сфери передбачає її функціональний зв’язок з усіма сферами суспільного життя, Як наслідок, вчені акцентували увагу на різних її аспектах. Так, Перфільєв М.Н. виділяв чотири види духовної діяльності:

по-перше, діяльність, в результаті якої виникають твори в самостійній формі, відособленій від виробника, – книги, картини інші твори мистецтва;

по-друге, діяльність, яка є невіддільною від процесу, в якому вона проводиться, – виконання усних, сценічних та інших творів;

по-третє, розумова діяльність в галузі матеріального виробництва – винахідництво, інженерія тощо;

по-четверте, управлінська діяльність в галузі матеріального і нематеріального виробництв [10, с. 85].

Така класифікація фактично ототожнює інформаційну діяльність з творчою діяльністю, яка юридично оформлена інститутами інтелектуальної власності, зокрема, авторськими, суміжними та патентними правами.

Інший радянський вчений Улєдов А.К. виділяв духовно-теоретичну діяльність, яка полягає у створенні ідей, поглядів, оцінок, уявлень, та духовно-практичну діяльність – інтеграцію створених духовних цінностей у свідомість людей [11, с. 68]. Таким чином, в цьому підході найбільш чітко прослідковується, що основні види інформаційної діяльності ототожнювалися з певними видами діяльності в духовній сфері.

Аналогічно, в концепції Кагана М.С. пізнавальна, ціннісноорієнтована та комунікаційна діяльності розглядаються як її специфічні види інформаційного характеру, хоча сам термін “інформаційна діяльність” ним також не застосовується [12, с. 85].

Тільки окремі вчені радянського періоду виділяли інформаційну діяльність в окремий вид суспільної духовної діяльності, розуміючи під ним процеси виробництва, розповсюдження, розподілу та споживання інформації [13, с. 114].

Трансформація наукових поглядів щодо сутності інформаційної діяльності, виокремлення її з духовної в самостійний вид відбулася під впливом розвитку інформаційної сфери, в т.ч. у зв’язку із виникненням комп’ютерних технологій. Як зазначає Ларцев В., у ході суспільного прогресу синтезувались якісно нові, неординарні і небачені раніше види суспільних відносин, які не можна з абсолютною впевненістю віднести ні до матеріальних відносин, ні до духовних – це сфера інформатизації та масових комунікацій [14, с. 69].

Авдєєв Р.Ф. підкреслює, що на межі третього тисячоліття відбулася зміна світогляду, який спричинила революція у сфері комунікацій та інформації, що досягла таких масштабів, яких не могли собі навіть уявити попередні покоління. Масова комп'ютеризація, впровадження і розвиток новітніх інформаційних технологій призвели до значного прориву у сферах освіти, бізнесу, промислового виробництва, наукових досліджень і соціального життя. Інформація перетворилася на глобальний, в принципі невичерпний ресурс людства, що вступило в нову епоху розвитку цивілізації – епоху інтенсивного освоєння цього інформаційного ресурсу [15, с. 81].

Високі темпи інформаційного розвитку обумовили інтерес до інформаційної діяльності суспільних наук, предметна сфера яких раніше не поширювалася на інформаційні явища. Повною мірою це стосується і юриспруденції. Так, Венгеров А.Б, який один із перших досліджував правові аспекти інформаційних відносин, зазначає, що важливе історичне значення має відокремлення процесу виробництва інформації від процесу використання інформації. У зв’язку з цим визрівають умови для того, щоб основоположна магістраль розвитку правової системи “економіка – політика – право” доповнилася таким напрямом як “інформація – політика – право” [16, с. 24].

У сучасній юридичній науці спостерігається декілька підходів до інформаційної діяльності. Так, Арістова І.В. та Чернадчук В.Д. цілком слушно зазначають, що існують відповідні підстави для введення у науковий обіг поняття “інтегративна інформаційна сфера”, яка за інформаційним критерієм (тобто за циркуляцією інформації) об’єднує усі сфери суспільного життя, у тому числі й інформаційну. При цьому, інформаційна сфера суспільного життя розглядається як сфера, в якій здійснюється суто інформаційна діяльність (збирання, виробництво, зберігання, використання, розповсюдження інформації) та відповідна діяльність, що забезпечує інформаційну діяльність. Суто інформаційна діяльність – це діяльність, в якій виробництво, розповсюдження, споживання інформації постає основною метою, а не засобом досягнення будь-якої мети [17, с. 48].

Бєляков К.І. визначає інформаційну діяльність як дії суб’єктів у галузі обігу інформаційних ресурсів та використання інформаційно-комунікаційних технологій (інформаційній сфері), які здійснюються в межах суспільних, корпоративних чи особистих інтересів або проти них [18, с. 69].

Брижко В.М. підкреслює, що до головних напрямів в упорядкуванні інформаційних відносин належить інформаційна діяльність державних органів, яка має управлінський, регулюючий зміст, що визначається адміністративним правом. Ця діяльність спрямована на забезпечення прав та інтересів суб’єктів інформаційної діяльності та взаємовигідного співробітництва України з іншими державами. Основними напрямами інформаційної діяльності держави є забезпечення інформаційних прав людини і основоположних свобод; забезпечення балансу інформаційних прав людини, суспільства і держави; створення, збереження, використання і поширення інформаційних ресурсів економічного, екологічного, фінансового, інформаційного й іншого призначення; охорона та захист інформаційних ресурсів і інформаційних послуг; підтримка інформаційної безпеки держави; експертиза проектів інформаційних систем і мереж; освітня робота, підготовка і підвищення кваліфікації кадрів [19, с. 251].

Бачило І.Л. під інформаційною діяльністю розуміє професійну діяльність в галузі створення, збору, пошуку, накопичення, обробки, зберігання, надання, представлення, розповсюдження, охорони та захисту інформаційних ресурсів, інформаційних технологій і використання засобів зв’язку, що здійснюється в рамках правового статусу організації (юридичної особи, органу державної влади та місцевого самоврядування), персоналу цих суб’єктів відповідно до їх прав і обов’язків, а також дії фізичних осіб по

задоволенню потреб в інформації і засобах інформатизації при дотриманні законодавства [20, с. 158].

Взявши за основу наведені вище концепції інформаційної діяльності вітчизняних та зарубіжних науковців, вважаємо за методологічно доцільне розглядати її під двома кутами зору: загально соціальним і вузько юридичним. Інформаційну діяльність в загально – соціальному розумінні слід трактувати виходячи з того, що суспільство є інтелектуалізованою, високоорганізованою системою з інформаційною взаємодією між його суб’єктами, яка виступає в якості необхідної умови його ефективного функціонування. При цьому, обіг інформації в соціальних підсистемах досить часто є стихійним, а значна група інформаційних процесів є елементом повсякденного життя людини. У зв’язку з цим певні дії суб’єктів із соціальною інформацією можна кваліфікувати як інформаційну діяльність лише умовно. Наприклад, побутове та особисте спілкування незалежно від того, чи воно здійснюється безпосередньо, чи за допомогою сучасних засобів комунікації, перегляд телепередач та ознайомлення з новинами в мережі Інтернет недоцільно розглядати як цілеспрямовану інформаційну діяльність. В ряді випадків діяльність людини з приводу отримання, споживання, використання інформації, інформаційних ресурсів, користування засобами зв’язку та комп’ютерно-інформаційними технологіями слід вважати не системною інформаційною діяльністю, а окремими діями щодо задоволення інформаційних потреб чи інтересів. Протягом всієї історії людства повноцінне функціонування будь-якого соціального суб’єкта було можливе за умови задоволення інформаційних потреб. Як справедливо зазначає Уханов В.А., інформаційні потреби займають особливе місце в системі суспільних потреб і в системі соціальної діяльності загалом. Реалізація всіх інших потреб – матеріальних та духовних – передбачає задоволення потреби в інформації, оскільки вони можуть бути задоволені тільки за умови участі в інформаційному обміні [21, с. 115].

Водночас задовольняючи інформаційні потреби, людина стає учасником правових відносин, які базуються на праві кожного вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Реалізація права на інформацію передбачає наявність системних процесів створення, обробки, зберігання, надання, поширення, охорони і захисту інформації та інформаційних ресурсів. Здійснення таких процесів, як правило, можливе тільки в процесі інформаційної праці, тобто трудової, професійної, цілеспрямованої індивідуальної чи корпоративної діяльності, результатом якої є інформаційний продукт або інформаційна послуга. Враховуючи важливе загальносуспільне значення такої діяльності, вона повинна здійснюватися на основі матеріальних та процесуальних правових норм. У зв’язку з цим інформаційну діяльність у вузькоюридичному розумінні можна трактувати як систему інтелектуальних, творчих, організаційних і технологічних дій та заходів суб’єктів права, які спрямовані на функціонування та розвиток інформаційної сфери, що здійснюються на основі законодавства в рамках суспільного або корпоративного поділу праці.

Важливе теоретичне і практичне значення має класифікація інформаційної діяльності. В чинному законодавстві України закладено невиправдано спрощений підхід як до самого визначення інформаційної діяльності, так і до її класифікації. Зокрема, Закон України “Про інформацію” поділяє інформаційну діяльність на основні і неосновні види. При цьому, до основних видів відносить створення, збирання, одержання, зберігання, використання, поширення, охорону та захист інформації, в той час як переліку неосновних видів інформаційної діяльності цей закон не містить [22].

Науковцями в галузі інформаційного права запропонована класифікація інформаційної діяльності за соціальною направленістю, функціями інформаційних ресурсів та технологій з урахуванням правомірності інформаційної діяльності. На цій основі виділяється державна, комерційна (недержавна), приватна та неправомірна інформаційна діяльність[23, с. 68].

Взявши за основу цю класифікаційну систему, її можна розширити, застосувавши додаткові класифікаційні принципи.

Так, за сферами суспільного життя інформаційну діяльність можна поділити на політичну, управлінську, господарську та культурну.

Політична інформаційна діяльність – це створення, збирання, одержання, зберігання, використання, поширення інформації при здійснені виборчих процедур та інших способів формування органів державної влади та органів місцевого самоврядування, а також в інших системах, пов’язаних із функціонуванням інститутів влади.

Інформаційну діяльність у сфері державного управління можна трактувати як специфічну інтелектуальну діяльність службовців державних органів влади та органів місцевого самоврядування, що спрямована на інформаційне забезпечення, інформаційну взаємодію, охорону і захист інформації в системі державного управління, а також забезпечення права на доступ до публічної інформації.

Під господарською інформаційною діяльністю слід розуміти діяльність суб'єктів господарювання та суб’єктів інформаційних відносин у сфері нематеріального виробництва, яка спрямована на створення інформаційної та інтелектуальної продукції, її комерційний та некомерційний обіг, а також надання інформаційних послуг з метою отримання прибутку або для досягнення економічних, соціальних та інших результатів без мети одержання прибутку.

Інформаційна діяльність у сфері культури – це творча, інтелектуальна та організаційна діяльність щодо створення та поширення інформаційної продукції, яка має наукову, освітню, художню, естетичну, моральну цінність та надання послуг щодо поширення та користування цією продукцією.

Слід зазначити, що провести чітку межу між інформаційною діяльністю в різних суспільних сферах інколи досить складно, оскільки, наприклад, державне управління можна розглядати як вид політичної діяльності, а інформаційна діяльність у сфері культури може носити і господарський характер.

За характером результату, що виникає внаслідок інформаційної діяльності, її можна поділити на первинну і вторинну. В результаті первинної діяльності виникають нові за змістом або за якістю інформаційні ресурси, тобто відбувається створення, виробництво інформації. Як зазначає Кохановська О.В., створення інформації – це інтелектуально цілеспрямована діяльність, в результаті якої з’являється якісно нова, оригінальна інформація як неекономічний феномен, який може бути втілений у матеріальну об’єктивну форму, придатну для сприйняття третіми особами, бути публічно оголошеною тощо. Виробництво інформації – це вироблення на основі і за допомогою відомої інформації із залученням різного роду засобів та інтелектуальної діяльності нової інформації, яка не підпадає під поняття “створення інформації”, втілена в об’єктивну матеріальну форму, придатну для сприйняття третіми особами, може бути публічно оголошеною тощо і має здатність до тиражування і розповсюдження [24, с. 68].

Вторинна інформаційна діяльність передбачає роботу із вже існуючими інформаційними об’єктами і полягає в їх зборі, отриманні, зберіганні, використанні, захисті, охороні тощо. Наприклад, архівна справа охоплює наукові, організаційні,

правові, технологічні, економічні та інші питання діяльності юридичних і фізичних осіб, пов’язаної із збиранням, обліком, зберіганням архівних документів та використанням відомостей, що в них містяться.

Водночас, в окремих випадках можливе комбінування первинних і вторинних видів інформаційної діяльності. Зокрема, науково-інформаційна діяльність може носити характер як вторинної – збирання, фіксація, зберігання, пошук і поширення науково-технічній інформації, так і первинної – її аналітично-синтетична обробка.

За суб’єктним складом інформаційну діяльність можна класифікувати на ту, що здійснюється державними і муніципальними органами, та діяльність юридичних осіб, які не відносяться до цієї категорії, а також фізичних осіб. Актуальність виділення інформаційної діяльності суб’єктів владних повноважень обумовлюється двома основними факторами:

по-перше, наявністю інформаційної діяльності, яку законодавство дозволяє здійснювати тільки державним органам. Наприклад, добування, аналітична обробка та надання визначеним законом органам державної влади розвідувальної інформації належить виключно до компетенції розвідувальних органів України [25];

по-друге, режимом доступу до інформації, яка виникає в результаті такої діяльності. Зокрема, публічна інформація тобто інформація, що була отримана або створена в процесі виконання суб’єктами владних повноважень своїх обов’язків або яка знаходиться у володінні суб’єктів владних повноважень, носить переважно відкритий характер.

Також, за виявом волі суб’єкта інформаційну діяльність можна поділити на добровільну та обов’язкову. Добровільна інформаційна діяльність здійснюється в межах диспозитивного правового регулювання, яке передбачає самостійний вибір суб’єктом видів, форм і методів діяльності в інформаційній сфері. Так, Закон України “Про інформаційні агентства” передбачає, що їх діяльність спрямована на збирання, обробку, творення, зберігання, підготовку інформації до поширення, випуск та розповсюдження інформаційної продукції. При цьому, гарантується свобода діяльності інформаційних агентств, яка базується на Конституції України та чинному законодавстві [26].

У той же час, є обов’язкова інформаційна діяльність, яка підлягає імперативному регулюванню. В основному, це стосується зберігання, поширення, охорони та захисту інформації. Так, обов’язковому висвітленню в аудіовізуальних засобах масової інформації підлягають: звернення Президента України з посланнями до народу та щорічними і позачерговими посланнями до Верховної Ради України про внутрішнє та зовнішнє становище України; участь Президента України в офіційних заходах, що проводяться в державі; ведення переговорів та укладання міжнародних договорів України при здійсненні керівництва зовнішньоекономічною діяльністю держави тощо [27].

Запропонована класифікація не охоплює всі види інформаційної діяльності, внаслідок ряду причин: по-перше, інформаційну діяльність можна розглядати як мега діяльність, що означає неможливість повної і однозначної її класифікації; по-друге, інформаційна діяльність перебуває в стані високої динаміки, що обумовлює появу нових її видів; по-третє, інформаційна діяльність в різних суспільних сферах (соціальній, політичній, господарській, управлінській) може мати свої класифікаційні підсистеми.

Висновки.

Інформаційна діяльність є надзвичайно складним і багатоплановим соціальним явищем. У теорії суспільних наук тривалий час вона розглядалася як елемент духовної діяльності, що було пов’язано із традиційним поділом суспільних сфер на економічну, політичну, соціальну та духовну. В результаті інформаційного розвитку соціуму та інтелектуалізації всіх суспільних сфер інформаційна діяльність виокремилася з інших видів соціальної діяльності і набула ключового значення. У зв’язку з цим інформаційна

діяльність стала предметом дослідження юридичної науки і включена до системи правового регулювання. Вітчизняними та зарубіжними вченими в галузі юриспруденції введено в обіг термін “інформаційна сфера” як середовище, в якому здійснюється інформаційна діяльність. При цьому, окремі види цієї діяльності знаходяться поза межами правового регулювання внаслідок неможливості врегулювання правовими засобами, а також індивідуальною, а не загальносуспільною значимістю.

Чинне законодавство України, яке регулює інформаційну діяльність, має ряд недоліків, одним з основних серед яких є звужене її трактування як діяльності засобів масової інформації. В той же час, інформаційна діяльність охоплює значно ширше коло суспільних інформаційних відносин. Виходячи з цього її слід розглядати під двома кутами зору: загальносоціальним і вузькоюридичним. У свою чергу, інформаційну діяльність у вузькоюридичному значенні можна класифікувати за сферами суспільного життя, характером результату, суб’єктним складом, виявом волі суб’єкта.

Окремого аналізу потребує встановлення чіткого правового режиму результатів інформаційної діяльності, що може бути предметом подальших досліджень в цьому напрямку.

Використана література

1. Иноземцев В.Л. Очерки истории экономической общественной формации / В.Л. Иноземцев. – М. : Таурус, 1996.– 399 с.

2. Бачило И.Л. Информационное право. Основы практической информатики : учеб. пособие / И.Л. Бачило. – М. : Издание г-на Тихомирова М.Ю., 2001. – 352 с.

3. Маргулис А.В. Диалектика деятельности и потребностей общества / А.В. Маргулис. – Белгород, 1972. – 95 с.

4. Николов В. Структуры человеческой деятельности / В. Николов : под общ. ред. Л.П. Буевой : [пер. с болг. Блинникова Л.В.]. – М. : 1984. – 175 с.

5. Буева Л.П. Человек : деятельность и общение / Л.П. Буева. – М. : Мысль. – 216 с

6. Маркарян Э.С. О генезисе человеческой деятельности и культуры / Э.С. Маркарян. – Ереван : Изд-во АН Армянской ССР, 1973. – 181 с.

7. Демин М.В. Природа деятельности / М.В. Демин. – М. : Изд-во МГУ, 1984. – 167 с.

8. Афанасьев В.Г. Человек в управлении обществом / В.Г. Афанасьев. – М. : Политиздат, 1977. – 382 с.

9. Леонтьев А.Н. Деятельность. Сознание. Личность / А.Н. Леонтьев. – М. : Политиздат, 1975. – 304 с.

10. Перфильев М.Н. Общественные отношения. Методологические и социальные проблемы / М.Н. Перфильев. – Ленинград : Наука, 1974. – 235 с.

11. Уледов А.К. Духовная жизнь общества. Проблемы методологи исследования / А.К. Уледов . – М. : Мысль. – 270 с.

12. Каган М.С. Человеческая деятельность / М.С. Каган. – М., Политиздат, 1974. – 268 с.

13. Урбанизация, научно-техническая революция и рабочий класс. Некоторые вопросы теории, критика буржуазних концепций ; редкол. Э.А. Арабоглы, А.С. Ахиезер, В.А. Мартынов, Е.Т. Фаддеев, О.Н. Яницкий (отв. ред.). – М. : Наука, 1972. – 267 с.

14. Ларцев В. Структуропроцесуальні та потенціало-визначальні компоненти структури суспільства // Людина і політика. – 2001. – № 3. – С. 68-80.

15. Абдеев Р.Ф. Философия информационной цивилизации / Р.Ф. Абдеев. – М. : Владос, 1994. – 336 с.

16. Венгеров А.Б. Право и информация в условиях автоматизации управления (Теоретические вопросы) / А.Б. Венгеров . – М., Юрид. лит., 1978. – 208 с.

17. Арістова І.В., Чернадчук В.Д. Концепція інформаційних правовідносин: сутність та особливості використання у сфері банківської діяльності // Інформація і право. – 2012. – № 3. – С. 47-57.

18. Бєляков К.І. Інформаційна діяльність : зміст та підходи до класифікації // Інформація і право. – № 1. – 2012. – с. 64 – 70.

19. Брижко В.М. Методологічні та правові засади упорядкування інформаційних відносин: монографія / В.М. Брижко. – К. : ТОВ “Пан Тот”, 2009. – 322 с.

20. Бачило И.Л. Информационное право. Основы практической информатики : учеб. пособие / И.Л. Бачило. – М. : Издание г-на Тихомирова М.Ю., 2001. – 352 с.

21. Уханов В.А. Информационная деятельность человека : дис. на соискание ученой степени д-ра филос. наук : 09.00.11 / В.А. Уханов. – Екатеринбург, 1997. – 292 с.

22. Про інформацію : Закон України від 13.01.11 р. № 2938-VI // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 313.

23. Бєляков К.І. Інформаційна діяльність : зміст та підходи до класифікації // Інформація і право. – 2012. – № 1. – С. 64-70.

24. Кохановська О.В. Цивільно-правові проблеми інформаційних відносин в Україні : дис. на здобуття наук. ступеня д-ра юрид. наук : 12.00.03 / О.В. Кохановська ; Київський національний ун-т ім. Тараса Шевченка. – К., 2006. – 531 с.

25. Про розвідувальні органи України : Закон України від 22.03.01 р. № 2331-III. – Режим доступу : //www.zakon4.rada.gov.ua/laws/show/2331-14

26. Про інформаційні агентства : Закон України від 28.02.95 р. № 74/95-ВР. – Режим доступу : //www.zakon4.rada.gov.ua/laws/show/74/95-вр

27. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні: Закон України від 23.09.97 р. № 539/97-ВР. – Режим доступу : //www.zakon4.rada.gov.ua/laws/show/539/97-вр

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.5:001.4

ДОРОГИХ С.О., старший науковий співробітник НДІІП НАПрН України

СУТНІСТЬ ТА ВИЗНАЧЕННЯ ПОНЯТЬ “ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ” ТА “ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ ОРГАНІВ ВЛАДИ”

Анотація. *До питання наукової термінології: сутність та визначення понять “інформаційна діяльність” та “інформаційна діяльність органів влади”.*

Ключові слова: *термінологія, інформаційна діяльність, інформаційна діяльність органів влади.*

Аннотация. *К вопросу научной терминологии: сущность и определение понятий “информационная деятельность” и “информационная деятельность органов власти”.*

Ключевые слова: *терминология, информационная деятельность, информационная деятельность органов власти.*

Summary. *To the question of scientific terminology: essence and definition of the concepts of “information activities” and “information activities of authorities”.*

Keyword: *terminology, information activities, informational activities of authorities.*

Постановка проблеми. Інформаційна діяльність супроводжує людство з найдавніших часів. Вона тісно пов’язана зі всіма сферами людської діяльності, зокрема з діяльністю органів влади – як в аспекті задоволення інформаційних потреб органів влади для прийняття управлінських рішень та створення нормативно-правової бази, так і в аспекті задоволення інформаційних потреб громадян щодо діяльності органів влади. Ще у 1978 році у своїй монографії професор А.Б. Венгеров підкреслював, що в державному управлінні завжди здійснюються певні операції з інформацією (отримання інформації про значення (параметри) стану управлінського об’єкта, обробка отриманої інформації та ін.). Ці операції складають зміст, атрибут будь-якої управлінської діяльності [1, с. 17]. З розвитком інформаційного суспільства значення інформаційної діяльності та її обсяги будуть тільки збільшуватися.

Питання інформаційної діяльності та інформаційної діяльності органів влади порушували у своїх роботах такі вчені, як: О.А. Баранов, І.Л. Бачило, В.М. Брижко, Ю.П. Бурило, А.Б. Венгеров, Г.В. Виноградова, О.О. Городов, Л.П. Коваленко, В.А. Копилов, Б.А. Кормич, А.І. Марущак, О.В. Соснін, О.С. Устинович, О.І. Яременко.

Наразі серед українських науковців широко обговорюється потреба у необхідності переосмислення й кодифікації питань інформації та інформаційних відносин у законодавстві України [2]. Окремим напрямом таких відносин є інформаційна діяльність органів влади України, зокрема законодавчої гілки влади. Відносини, пов’язані з інформаційною діяльністю, повинні бути законодавчо врегульовані, а поняття, що становлять суть інформаційної діяльності, такі як: “інформаційна діяльність”, “інформаційна діяльність органів влади” та окремі види інформаційної діяльності повинні мати законодавчо закріпленні визначення.

В той же час, аналізуючи сучасний стан законодавства у сфері інформаційного права, ми вимушені погодитись з цілим рядом науковців, наприклад, О.А. Баранов та Л.П. Коваленко [3, с. 93; 4, с. 89], які відносять стан понятійного апарата, затвердженого у законах України, до проблем, які потрібно вирішувати.

Визначення поняття “інформаційна діяльність” та її видів, хоча і не були ідеальними і потребували подальшого удосконалення, присутні у першій редакції Закону України “Про інформацію” від 02.10.92 р. [5], проте ці визначення зникають із закону, починаючи з 09.05.11 р., що утворило прогалину в законодавстві України у сфері інформаційного права, яка не ліквідована і сьогодні. Відповідно, це викликає необхідність осмислення, визначення та закріплення цих понять у законодавстві України. Щодо легітимного визначення поняття “інформаційна діяльність органів влади”, то вона на сьогодні відсутня взагалі.

Для осмислення поняття інформаційної діяльності необхідно вивчити її складові тобто об’єкти, суб’єкти, мету, види та галузі, способи, засоби та умови діяльності, а також історію формування визначень, особливо визначень, закріплених у нормативно-правових актах.

Метою статті є визначення та формулювання понять “інформаційна діяльність” і “інформаційна діяльність органів влади”.

Виклад основних положень. Вперше визначення інформаційної діяльності та перелік основних її видів у законодавстві України з’явилося у Законі України “Про інформацію” від 02.10.92 р. [5]. В розумінні цього Закону інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави. З метою задоволення цих потреб органи державної влади та органи місцевого і регіонального самоврядування створюють інформаційні служби, системи, мережі, бази і банки даних.

Таким чином, у визначенні, наданому у Законі, була сформульована мета інформаційної діяльності, а саме: *задоволення інформаційних потреб громадян, юридичних осіб і держави*. Також у Законі окрім визначення інформаційної діяльності наведені її суб’єкти, тобто інформаційні служби та форми здійснення інформаційної діяльності, а саме – створення систем, мереж, баз і банків даних.

Загальними суб’єктами інформаційної діяльності є народ, держава, фізичні та юридичні особи. До спеціальних суб’єктів інформаційної діяльності належать ЗМІ, інформаційні служби, системи, мережі, бази і банки даних, відповідні органи державної влади, бібліотечні, музейні, архівні установи й організації та інші суб’єкти – автори, споживачі, зберігачі та поширювачі інформації.

Об’єктом інформаційної діяльності є насамперед інформація в цілому як документовані або публічно оголошені відомості про події в галузі політики, економіки, культури, а також у соціальній, екологічній та інших сферах [6, с. 74].

До основних видів інформаційної діяльності згідно з першою редакцією Закону України “Про інформацію” [5] відносилися одержання, використання, поширення та зберігання інформації.

Переважна більшість українських науковців у своїх роботах в цілому покладалися на визначення інформаційної діяльності, надане у першій редакції Закону України “Про інформацію” [7, с. 237; 8, с. 170; 9, с. 104]. Зі зміною редакції Закону у 2011 році, з якого це визначення зникло, питання опрацювання поняття інформаційної діяльності та його визначення у законодавстві України постало знову.

Розглядаючи поняття і сутність інформаційної діяльності, автор пропонує зупинитися на трьох важливих аспектах, що характеризують інформаційну діяльність взагалі, а саме: мета інформаційної діяльності, її види та суб’єкти, що безпосередньо її виконують, а далі розглянути окремі особливості, притаманні саме інформаційній діяльності органів влади,, зокрема, законодавчої гілки влади в Україні.

У визначеннях поняття “інформаційна діяльність”, які можемо знайти у словниках, монографіях вітчизняних вчених та нормативно-правових актах, ми бачимо декілька підходів до визначення інформаційної діяльності.

Перший підхід подає визначення інформаційної діяльності з погляду її кінцевої мети, а саме: інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави. Таке визначення ми могли знайти в Законі України “Про інформацію” [5] до набуття чинності новою редакцією у 2011 році. Це визначення наводять у своїх роботах Б.А. Кормич [7, с. 237], А.І. Марущак [8, с. 170], Г.В. Виноградова [9, с. 11], В.М. Брижко [10, с. 164].

Другий підхід ґрунтується на визначенні інформаційної діяльності через її види. При цьому в сучасних поглядах на видову складову інформаційної діяльності переважає погляд на неоднорідність видів інформаційної діяльності, а саме – розділення на види, пов’язані зі здійсненням інформаційних процесів, та види, пов’язані з формуванням організаційного ресурсу та інфраструктури.

Тлумачний словник комп’ютерних інформаційних систем і сховищ даних подає таке визначення інформаційної діяльності: інформаційна діяльність – діяльність, що забезпечує збирання, обробку, збереження, пошук та розповсюдження інформації, а також формування організаційного ресурсу та організацію доступу до нього [11, с. 163].

Відомий російський теоретик інформаційного права В.А. Копилов [12, с. 55-56] та О.В. Соснін [13, с. 149] розглядають основні види інформаційної діяльності як реалізацію інформаційних процесів, а об’єктами цих видів – не інформацію, а інформаційні продукти і ресурси та відносять до видів інформаційної діяльності здійснення фізичними та юридичними особами інформаційних процесів, які охоплюють, по-перше, виробництво, розповсюдження, пошук, одержання, споживання інформації, формування інформаційних ресурсів, підготовку інформаційних продуктів і надання інформаційних послуг. По-друге, до інформаційної діяльності відносять також створення і застосування інформаційних технологій, засобів і механізмів інформаційної безпеки, які формують допоміжну частину інформаційної сфери, що існує для забезпечення функціонування основної частини.

Ю.П. Бурило [14, с. 15], погоджуючись з попередніми авторами, вказує на неоднорідність видів інформаційної діяльності та пропонує їх поділ на основні та допоміжні. На його думку, критерієм їх розмежування є об’єкт діяльності. Якщо об’єктом основних видів інформаційної діяльності є інформація (інформаційні ресурси), то об’єктом допоміжних видів – елементи інформаційно-телекомунікаційної інфраструктури, такі як інформаційно-телекомунікаційні технології (засоби інформатизації та телекомунікацій), інші засоби зв’язку, засоби інформаційної безпеки.

Вказане розмежування видів інформаційної діяльності має, на наш погляд, не лише теоретичне, а й практичне значення, оскільки може бути використане для розвитку вітчизняного законодавства про інформацію. Так, зокрема, має бути доопрацьовано Закон України “Про інформацію” шляхом закріплення зазначеного допоміжного виду інформаційної діяльності та визначення відповідного їй різновиду інформаційних відносин, а саме – інформаційно-інфрастурктурних відносин, об’єктом яких є засоби зв’язку та інформатизації, засоби інформаційної безпеки [14, с. 15].

У своїй роботі Б.А. Кормич [7, с. 237] називає результатом інформаційної діяльності *інформаційні продукти* як матеріальний результат цієї діяльності та *інформаційні послуги* як певну сукупність дій з доведення інформаційної продукції до споживача. На нашу думку, до результатів інформаційної діяльності слід додати також і впорядковані *інформаційні ресурси*, що складаються з множини інформаційних

продуктів, які як об’єкти інформаційних відносин створюються в процесі діяльності, зокрема, й органів державної влади, у вигляді первинних або вторинних документів [15, с. 178] та виступають як база здійснення інформаційних послуг. Слід підкреслити важливість створення інформаційних ресурсів саме у діяльності органів влади, особливо в законодавчій гілці влади, де бази даних нормативно-правових документів та законопроектів є одними з найважливіших інформаційних ресурсів, без яких неможливе виконання законодавчої діяльності та які потребують складного трудомісткого процесу по їх щоденній підтримці в актуальному стані.

Враховуючи важливість інформаційних ресурсів, що створюються органами державної влади в порядку здійснення основної діяльності цих органів, такі ресурси в обов’язковому порядку відносяться до національних інформаційних ресурсів [16, с. 46].

У структурному, предметному сприйнятті інформаційний ресурс являє собою масив чи окремий документ, інший інформаційний об’єкт в інформаційних системах (бібліотеках, архівах, фондах, банках даних тощо), що візуально сприймається й акумулює відомості (інформацію), сформовані за визначеними ознаками чи критерієм [17, с. 163; 18]. Як слушно вказує О.О. Городов, через інформаційні ресурси опосередковується провідна форма організаційного вираження документованої інформації, яка використовується під час її збирання, обробки, зберігання та споживання [19, с. 113], тобто під час інформаційної діяльності.

Таким чином, інформаційна діяльність являє собою діяльність, спрямовану на задоволення інформаційних потреб громадян, юридичних осіб та держави, реалізується через інформаційні процеси, які охоплюють виробництво, поширення, пошук, одержання, споживання, зберігання інформації та утворюють інформаційні продукти і впорядковані інформаційні ресурси, а також через формування інформаційно-телекомунікаційної інфраструктури, засобів зв’язку та засобів інформаційної безпеки.

Щодо визначення інформаційної діяльності органів влади, зокрема законодавчої гілки влади, то на сьогодні таке визначення теж відсутнє в законах України, хоча в окремих проектах і була спроба його ввести. Наприклад, у проекті Закону України “Про інформаційну діяльність органів державної влади та органів місцевого самоврядування” від 02.09.98 р. № 2047 [20] дається наступне визначення: інформаційна діяльність органів державної влади та органів місцевого самоврядування в Україні – задоволення потреб громадян, юридичних осіб в одержанні інформації про роботу органів державної влади та органів місцевого самоврядування шляхом створення, використання, поширення і зберігання інформації про діяльність цих органів.

Певну підміну понять ми можемо побачити в чинному Законі України “Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації” [21], в якому надається наступне визначення: *висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні* – одержання, збирання, створення, поширення, використання і зберігання інформації про діяльність органів державної влади та органів місцевого самоврядування, задоволення інформаційних потреб громадян, юридичних осіб про роботу цих органів. Якщо звернутися до Великого словника сучасної української мови [22], то можна побачити, що дієслово “висвітлення” має значення: робити відомим, пояснювати, розкривати що-небудь у деталях. Тобто, на думку автора, ці дії можна скоріше віднести до такого виду інформаційної діяльності, як “поширення”. В самому ж законі фактично дано визначення інформаційної діяльності органів влади та місцевого самоврядування і перераховуються притаманні інформаційній діяльності види: одержання, збирання, створення, поширення, використання і зберігання

інформації. Окрім цього, “задоволення інформаційних потреб громадян, юридичних осіб про роботу цих органів” становить сутність іншого терміна, що входить до поняття інформаційної діяльності органів влади, – це організація доступу до публічної інформації.

Згідно із Законом України “Про доступ до публічної інформації” від 13.01.11 р. № 2939-VI [23], в якому надається визначення публічної інформації, публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб’єктами владних повноважень своїх обов’язків, передбачених чинним законодавством, або яка знаходиться у володінні суб’єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом (ст. 1).

Таким чином, розглядаючи визначення, які були надані у законопроекті від 02.09.98 р. № 2047 [20] та у Законі України “Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації” [21], слід констатувати, що вони вже застарілі та не містять низки сучасних поглядів на інформаційну діяльність органів влади, як, наприклад, в них відсутні згадування про публічну інформацію, як одного з ключових понять у сфері забезпечення прозорості та відкритості суб’єктів владних повноважень і створення механізмів реалізації права кожного громадянина на доступ до публічної інформації.

У роботах вітчизняних та російських учених можна простежити як змінювались та ускладнювались завдання, що виникали під час виконання інформаційної діяльності органів законодавчої влади.

Так при першому наближенні, інформаційну діяльність органів державної влади умовно поділяли на два напрями: сукупність дій, пов’язаних із задоволенням інформаційних потреб громадян, юридичних осіб та інших суб’єктів, а також сукупність дій, пов’язаних із задоволенням власних інформаційних потреб [8, с. 178].

Яременко О.І. розглядає інформаційну діяльність у сфері державного управління як специфічну інтелектуальну діяльність службовців державних органів і органів місцевого самоврядування, що спрямована на інформаційне забезпечення, інформаційну взаємодію, охорону і захист інформації в системі державного управління, а також забезпечення права на доступ до публічної інформації [24, с. 62]. Тобто задоволення інформаційних потреб громадян, юридичних осіб та інших суб’єктів можна розділити на інформаційну взаємодію з іншими органами влади та місцевого самоврядування та забезпечення права на доступ до публічної інформації.

Відповідно, забезпечення права на доступ до публічної інформації регулюється Законом України “Про доступ до публічної інформації” [23]. Правове регулювання інформаційної діяльності органів влади відображене у статтях 5 “Забезпечення доступу до інформації” та 14 “Обов’язки розпорядників інформації”. Так, стаття 5 вимагає “систематичного та оперативного оприлюднення інформації” в різний спосіб, а в статті 14 розпорядники інформації зобов’язуються оприлюднювати інформацію про свою діяльність і прийняті рішення та систематично вести облік документів, що знаходяться в їхньому володінні. Тобто має місце регулювання таких видів діяльності, як одержання, використання, поширення, зберігання та захист інформації.

Не можна не погодитись з цілою низкою авторів [25, с. 8], які вважають інформаційну діяльність органів влади “професійною”. Тобто специфічною діяльністю спеціальних інформаційних служб та окремих державних службовців, яка потребує необхідного правового регламентування як окрема функція органу влади. Відмітимо також, що Закон України “Про доступ до публічної інформації” [23] вимагає мати

спеціальні структурні підрозділи або призначати відповідальних осіб для забезпечення доступу запитувачів до інформації.

Враховуючи сучасні тенденції до збільшення прозорості та відкритості діяльності органів влади на такі інформаційні структурні підрозділи буде покладатися все більше завдань, що буде збільшувати важливість їх діяльності та потребувати додаткового правового регулювання.

Розвиваючи ідею важливості інформаційної діяльності органів влади автор погоджується з думкою О.С. Устинович, що вже сьогодні є всі підстави виділити “інформаційну діяльність” в якості самостійного напряму роботи органу влади. Розглядаючи інформаційну діяльність федеральних органів виконавчої влади Російської Федерації, автор визначає цю діяльність як: “Особливий, специфічний вид професійної діяльності, спрямований на вирішення завдань інформаційного забезпечення власної функціональної діяльності, організаційно-правового забезпечення доступу до інформації про свою діяльність, публічного (масового) інформування громадян та “постачання” їх значущою для них соціально-політичної, економічної та духовно-патріотичної інформації, інформаційної взаємодії між самими органами влади, а також взаємодії з громадянами, організаціями та інститутами громадянського суспільства, надання їм інформаційних та електронних послуг” [25, с. 8].

В той же час, коли зростає важливість доступу громадян до публічної інформації та збільшується важливість інформаційної діяльності органів влади, з останньої версії Закону України “Про інформацію” [5] зник один з основних видів інформації, такий як інформація про діяльність державних органів влади та органів місцевого самоврядування. На сьогодні інформація про діяльність органів влади входить до поняття “публічна інформація”, проте цей вид інформації теж не включено до її основних видів. На думку автора, ця прогалина повинна бути усунена шляхом внесення відповідного доповнення до ст. 10 Закону України “Про інформацію”.

Також звертаємо увагу на важливу роль співпраці між державними органами та громадянським суспільством як необхідної передумови наявності зворотного зв’язку без якого неможливе ефективне державне управління. Удосконалення умов для забезпечення відкритості та прозорості діяльності органів виконавчої влади та органів місцевого самоврядування, публічності всіх етапів підготовки і прийняття ними рішень, оприлюднення проектів рішень, доступу до інформації про діяльність та рішення зазначених органів є одним із завдань державної політики сприяння розвитку громадянського суспільства в Україні, затвердженої Указом Президента “Про Стратегію державної політики сприяння розвитку громадянського суспільства в Україні та першочергові заходи щодо її реалізації” від 24.03.12 р. № 212/2012 [26]. Все це підвищує значення інформаційної діяльності органів влади.

Підсумовуючи вищевикладені особливості інформаційної діяльності органів влади, зазначимо, що вона являє собою специфічну професійну діяльність службовців державних органів влади, спрямовану на забезпечення власної функціональної діяльності, інформаційну взаємодію з іншими органами влади, об’єднаннями громадян, юридичними та фізичними особами та організацію доступу до публічної інформації.

Інформаційній діяльності законодавчої гілки влади притаманні всі особливості інформаційної діяльності органів влади взагалі, а також певні особливості, як центру створення і збереження законів країни. Відповідно, вона регулюється цілою низкою нормативно-правових актів. В першу чергу слід відмітити важливість права громадян на ознайомлення з законами та іншими нормативно-правовими актами. Це право закріплено у Конституції України [27]. Згідно статті 57 – “закони та інші нормативно-

правові акти, що визначають права і обов’язки громадян, мають бути доведені до відома населення у порядку, встановленому законом”. Порядок опублікування законів, постанов та інших актів Верховної Ради України регулюється ст. 139 Закону України “Про Регламент Верховної Ради України” [28], також у статті 3 Регламенту встановлюється гласність засідань Верховної Ради України. Окрім названих документів, інформаційну діяльність законодавчої гілки влади регламентує Закон України “Про доступ до публічної інформації” [23].

Виходячи з міжнародних стандартів, на яких базується Закон України “Про доступ до публічної інформації”, доступ до інформації про діяльність органів влади розглядають у активному й пасивному аспектах. На відміну від позиції, коли активний і пасивний доступ розглядається як дії особи щодо отримання публічної інформації, міжнародні стандарти розглядають аспекти доступу саме в контексті забезпечення органом влади реалізації права на доступ до публічної інформації.

Пасивний аспект доступу (з боку органу влади) передбачає відповідь органу на запит від особи/групи осіб, забезпечення їхньої участі в засіданні колегіальних органів, надання можливості ознайомитися з публічною інформацією в органі влади.

Активний аспект доступу (з боку органу влади) – обов’язок органу влади оприлюднювати інформацію про свою діяльність, ухвалені документи та проекти, що готуються, реєстр публічної інформації тощо в один або кілька способів – публікувати в ЗМІ, розміщувати на офіційних веб-сайтах, вивішувати на інформаційних стендах тощо [29, с. 13].

Практична реалізація цих аспектів під час інформаційної діяльності законодавчої гілки влади відображається у Програмі інформатизації законотворчого процесу у Верховній Раді України на 2012 – 2017 роки [30], яка має на меті побудову системи електронного парламенту.

Так, одним з напрямів щодо забезпечення участі громадян у засіданні колегіальних органів, є побудова системи обов’язкової трансляції, збереження та пошуку відеозаписів пленарних засідань та засідань комітетів Верховної Ради України в мережі Інтернет. Вирішення забезпечення з боку парламенту активного аспекту доступу вирішується через побудову потужного веб-порталу, який би містив вичерпну інформацію щодо діяльності парламенту, містив бази даних нормативно-правових актів та законопроектів. Також пропонується реалізація функції взаємодії з громадянами та громадськими об’єднаннями через організацію форумів, дискусійних он-лайн груп, Інтернет-опитування та голосування тощо.

Зрозуміло, що впровадження нових інформаційно-комунікаційних технологій щодо інформаційної діяльності законодавчої гілки влади потребує відповідного правового регулювання.

Висновки.

Понятійний апарат у сфері інформаційного права потребує осмислення та удосконалення. Ряд важливих термінів як, наприклад, “інформаційна діяльність” та “інформаційна діяльність органів влади” потребують свого легітимного визначення. Так, поняття “нформаційна діяльність” та поняття окремих видів інформаційної діяльності мали своє визначення у Законі України “Про інформацію” [5] проте у останніх редакціях цього ж закону вони зникли, що викликає цілу низку питань щодо змісту, яке вкладає у ці питання законотворець.

Також у Законі України “Про інформацію” [5] з переліку видів інформації за змістом необґрунтовано зник такий вид інформації як “інформація про діяльність

державних органів влади та органів місцевого самоврядування”, в той же час замість нього не було додано такий вид інформації як “публічна інформація”.

Автором пропонуються такі визначення: *інформаційна діяльність – це діяльність, спрямована на задоволення інформаційних потреб громадян, юридичних осіб та держави, реалізується через інформаційні процеси, які охоплюють виробництво, поширення, пошук, одержання, споживання, зберігання інформації та утворюють інформаційні продукти і впорядковані інформаційні ресурси, а також через формування інформаційно-телекомунікаційної інфраструктури, засобів зв’язку та засобів інформаційної безпеки.*

Інформаційна діяльність органів влади – це специфічна професійна діяльність службовців державних органів влади, спрямована на забезпечення власної функціональної діяльності, інформаційну взаємодію з іншими органами влади, об’єднаннями громадян, юридичними та фізичними особами та організацію доступу до публічної інформації.

Перспектива щодо подальших досліджень. Необхідне опрацювання переліку основних видів інформаційної діяльності та їх визначень.

У подальшому потребує узгодження положення законів “Про доступ до публічної інформації” [23], “Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації” [22] та положень нормативно-правових документів, які будуть регламентувати функціонування системи електронного парламенту.

Використана література

1. Венгеров А.Б. Право и информация в условиях автоматизации управления (теоретические вопросы) / А.Б. Венгеров. – М. : Юридическая литература, 1978. – С. 5.

2. Пилипчук В.Г., Брижко В.М. Проблеми становлення і розвитку інформаційного законодавства в контексті євроінтеграції України // Інформація і право. – 2011. – № 1. – С. 11-19.

3. Баранов О.А. Інформаційне право України : стан, проблеми, перспективи / О.А. Баранов. – К. : Видавничий дім “СофтПрес”, 2005. – 316 с.

4. Коваленко Л.П. Теоретичні проблеми розвитку інформаційного права України : монографія / Л.П. Коваленко . – Х. : Право, 2012. – 248 с.

5. Про інформацію : Закон України від 02.10.92 р. № 2657-XII. – Режим доступу : http://zakon.rada.gov.ua

6. Правове забезпечення інформаційної діяльності в Україні ; за заг. ред. Ю.С. Шемшученка, І.С. Чижа. – К. : ТОВ “Видавництво “Юридична думка”, 2006. – 184 с.

7. Кормич Б.А. Інформаційне право : підручник / Б.А. Кормич. – Х. : Бурун і К, 2011. – 334 с.

8. Марущак А.І. Інформаційне право України : підручник / А.І. Марущак. – К. : Дакор, 2011. – 456 с.

9. Виноградова Г.В. Інформаційне право України : навч. посіб. / Г.В. Виноградова. – К. : МАУП, 2006. – 144 с.

10. Брижко В.М. Основи систематизації інформаційного законодавства : теоретичні та правові засади : монографія / В.М. Брижко. – К. : ТОВ “ПанТот”, 2012 р. – 304 с.

11. Компьютерные информационные системы и хранилища данных. Толковый словарь / [А.Г. Додонов, С.Р. Коженевский, Д.В. Ланде, В.Г. Путятин]. – К. : Феникс; ИПРИ НАН Украины, 2013. – 554 с.

12. Копылов В.А. Информационное право : вопросы теории и практики / В.А. Копылов. – М. : Юристъ, 2003. – 472 с. – (Московская гос. юридическая академия).

13. Соснін О.В. Проблеми державного управління системою національних інформаційних ресурсів з наукового потенціалу України / О.В. Соснін . – К., 2003. – 572 с. – (Інститут держави і права ім. В.М. Корецького НАН України).

14. Бурило Ю.П. Організаційно-правові питання державного управління в інформаційній сфері : дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.07 / Юрій Петрович Бурило; Державний вищий навчальний заклад “Київський національний економічний університет імені Вадима Гетьмана”. – К., 2008. – 222 с.

15. Червякова О. Сутнісні ознаки та види інформаційних ресурсів як об’єктів державного управління // Вісник Академії правових наук України. – 2012. – № 3. – С. 176-184.

16. Основи інформаційного права України : навч. посіб. / [В.С. Цимбалюк, В.Д. Гавловський, В.М. Брижко та ін.] ; за ред. М.Я. Швеця, Р.А. Калюжного, П.В. Мельника. – [2-ге вид., переробл. і допов.]. – К. : Знання, 2009. – 414 с.

17. Бачило И.Л. Информационное право : учебник / И.Л. Бачило. – М. : Юрайт; ИД Юрайт, 2011. – С. 163.

18. Килясханов И.Ш. Информационное право в терминах и понятиях : учеб. пособие / И.Ш. Килясханов, Ю.М. Саранчук. – М. : ЮНИТИ-ДАНА : Закон и право, 2011. – С. 51.

19. Городов О.А. Основы информационного права России : учеб. пособие / О.А. Городов. – СПб. : Юрид. центр Пресс, 2003. – С. 113.

20. Про інформаційну діяльність органів державної влади та органів місцевого самоврядування : проект Закону України від 02.09.98 р. № 2047. – Режим доступу : http://zakon.rada.gov.ua.

21. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації : Закон України від 23.09.97 р. № 539/97-ВР. – Режим доступу : //www.zakon.rada.gov.ua

22. Великий словник сучасної української мови ; уклад. і голов. ред. В.Т. Бусел. – К.-Ірпінь : ВТФ “Перун”, 2005. – 1728 с.

23. Про доступ до публічної інформації : Закон України від 13.01.11 р. № 2939-VI. – Режим доступу : //www.zakon.rada.gov.ua.

24. Яременко О.І. Правові проблеми регулювання інформаційної діяльності у сфері державного управління // Інформація і право. – 2011. – № 3. – С. 56-63.

25. Устинович Е.С. Информационная деятельность как функция федеральных органов исполнительной власти Российской Федерации // Российская юстиция. – 2010. – № 4. – С. 7-10.

26. Про Стратегію державної політики сприяння розвитку громадянського суспільства в Україні та першочергові заходи щодо її реалізації : Указ Президента України від 24.03.12 р. № 212/2012. – Режим доступу : //www.zakon.rada.gov.ua

27. Конституція України : Закон України від 28.06.96 р. № 254/96 ВР // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

28. Про Регламент Верховної Ради України : Закон України від 10.02.11 р. № 1861-VI. – Режим доступу : //www.zakon.rada.gov.ua

29. Методичні рекомендації щодо практичного впровадження Закону України “Про доступ до публічної інформації” / [М.В. Лациба, О.С. Хмара, В.В. Андрусів та ін.]. – [2-е вид., допов.]. – К. : Агентство “Україна”, 2012. – 164 с. – (Укр. незалеж. центр політ. дослідж.).

30. Про затвердження Програми інформатизації законотворчого процесу у Верховній Раді України на 2012-2017 роки : Постанова Верховної Ради України від 05.07.12 р. № 5096-VI. – Режим доступу : //www.zakon.rada.gov.ua

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК: 316.32:165.63

ПОПЕРЕЧНЮК В.М., фахівець І категорії НДІІП НАПрН України

ІНТЕЛЕКТУАЛІЗАЦІЯ СУЧАСНОГО СУСПІЛЬСТВА: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Анотація. *У статті розглядаються ключові аспекти інтелектуалізації сучасного суспільства в контексті розбудови інформаційної цивілізації. Окреслюються основні проблеми цього процесу та пропонуються можливі шляхи до їх розв’язання.*

Ключові слова: *інтелектуалізація, інформаційне суспільство, інформатизація, знання, інформація, інформаційно-комунікаційні технології.*

Аннотация. *Статья посвящена анализу ключевых аспектов интеллектуализации современного общества в контексте становления информационной цивилизации. Выделены основные проблемы этого процесса и предлагаются возможные пути их решения.*

Ключевые слова: *интеллектуализация, информационное общество, информатизация, знания, информация, информационно-коммуникационные технологии.*

Summary. *The article considers key aspects of intellectualization of the modern society in the context of the development of information civilization. Describes main problem of this process and suggests possible ways to address them.*

Keywords: *intellectualization, information society, informatization, knowledge, information, information and communication technology.*

Постановка проблеми. На сьогодні день перед людством стоїть непроста задача – розбудова інформаційного суспільства, яке має примножити здобутки попередніх соціально-економічних формацій та створити нові блага, сприяти їх подальшому розвитку, надати людям нові можливості та ресурси для їх реалізації.

Основним етапом переходу від інформатизації суспільства до розбудови інформаційної цивілізації має стати інтелектуалізація. Адже саме завдяки реалізації цього процесу сучасне суспільство може дійсно досягти якісно нового етапу свого розвитку, головне місце при цьому надається інформаційно-комунікаційним технологіям (далі – ІКТ) та інноваційним можливостям, що неодмінно має сприяти економічному зростанню [1].

Дане питання почало розглядатися відносно недавно, тому, на жаль, воно залишається малодослідженим, зокрема, у філософії, соціології та юриспруденції. Процес інтелектуалізації ще не посів належного місця у житті суспільства. Фрагментарні прояви прагнення до підвищення інтелектуального рівня населення є, але вони зустрічаються переважно в економіці та мають місце лише на великих підприємствах для інтенсифікації виробництва та нарощування матеріальних ресурсів.

Серед представників правової сфери дана проблематика розглядалась у працях К. Бєлякова, В. Брижка, О. Дзьобаня, О. Лисенко, В. Пилипчука та ін. Значна увага приділяється суміжним даній проблематиці питанням, зокрема інформаційному суспільству (І. Арістова, В. Брижко, І. Жиляєв, Р. Калюжний, А. Колодюк, Н. Савінова, М. Швець та ін.), інформації та знанням (О. Баранов, В. Гітт, К. Шеннон та ін.), інформатизації (Г. Бахтіна, С. Грипич, В. Пожуєв, В. Фурашев та ін.). Більшого наукового резонансу це питання здобуло в економічному контексті (М. Ажажа, В. Врублевський, П. Грішнова, А. Гайдабрус, О. Другов, К. Хаврова та ін.).

Метою статті є визначення особливостей інтелектуалізації українського суспільства та основних проблем розбудови інформаційного суспільства.

Виклад основних положень. Складні соціально-економічні перетворення, що тягнуть за собою перегляд вже давно усталених форм буття, руйнування стереотипів та пріоритетів сучасного суспільства, науковці вже “охрестили” “інформаційним суспільством” або “суспільством знань”. Відсутність однозначного визначення пов’язана із різновекторністю наукових підходів та стрімким розвитком людської цивілізації, що розкриває принципово нові перспективи та можливості, а також засоби для їх реалізації.

Переломною подією для сучасної науки можна вважати 32-у Генеральну конференцію ЮНЕСКО, що відбулась у 2003 році, на якій уперше було рекомендовано використовувати термін “суспільство знань” [2, с. 82-84]. Ця подія започаткувала науковий дискурс навколо назви та самого визначення нового етапу цивілізаційного розвитку, що затягнувся і триває вже 10 років.

Дана концепція знайшла своє продовження у поглядах А. Хана (заступника Генерального директора ЮНЕСКО з питань комунікації та інформації), він вважає, що інформаційне суспільство є функціональним блоком суспільства знань, адже в основу інформаційного суспільства входять технічні інновації, а суспільство знань включає в себе соціальне, культурне, економічне, політичне та інше підґрунтя [3].

Подібної позиції дотримується й І. Мелюхін. Беручи за основу модель розвитку людства Е. Тоффлера: “аграрне – індустріальне – постіндустріальне” суспільство [4, с. 4], він пропонує під інформаційним суспільством розуміти наступний етап історичного розвитку людства по ланцюгу “аграрне – техногенне – антропогенне”, де інформаційне суспільство є другим етапом техногенного [5].

Існує й інша наукова позиція. Так І. Арістова вважає, що “суспільство знань” є одним із етапів розвитку інформаційного, адже останнє включає в себе сучасні розробки у сфері інформаційно-комунікативних технологій, а також на наступному етапі (знаннєвому) має включати в себе соціальні, етичні та політичні параметри [6, с. 11-12].

Виходячи з аналізу запропонованих позицій можна побачити, що першими підвалинами розбудови інформаційного суспільства є активний розвиток та впровадження ІКТ в усі сфери суспільного життя, в основу якого покладений процес інформатизації, що полягає у “…сукупності 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” [7].

Наступний етап включає в себе низку соціальних, правових, організаційних, політичних, культурних, економічних, науково-технічних та ін. процесів що мають створити сприятливі умови для гармонійного та різнобічного розвитку особистості, надання можливості кожному реалізувати свій потенціал, а також віднайти дієві механізми для протистояння інформаційним викликам та загрозам. На даному етапі одне із ключових місць відводиться інформації та знанням, адже вони є стратегічним, якісно новим ресурсом, а також самоціллю нової соціально-економічної формації. Але системною проблемою інформаційного суспільства та глобального інформаційного простору є відсутність єдиного розуміння сутності інформації, як основи сучасної світобудови [8, с. 16].

Низка законодавчих актів містить визначення “інформації”, але, на жаль, вони зводяться виключно до відомостей або даних, які мають певну матеріальну форму свого закріплення [9], що повною мірою не відбиває сутності та соціальної значимості даного поняття, воно має технологічний характер і застосовується з метою спрощення та зручності подальшої побудови, розвитку і регламентації інформаційних відносин [10, с. 51].

Поняття знання ще й досі не знайшло свого відображення у правовому полі, хоч сучасні вчені приділяють значну увагу даному поняттю, адже, так само як інформація, знання є стратегічним ресурсом інформаційного суспільства. Радянський енциклопедичних словник визначає “знання” як *“перевірений суспільно-історичною практикою і засвідчений логікою результат процесу пізнання дійсності, адекватне її відображення у свідомості людини у вигляді понять, суджень, теорій”* [11, с. 840].

Парадоксальною є ситуація, що у Постанові Кабінету Міністрів України “Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи” (що втратила чинність у 2006 році) взагалі йде ототожнення понять “інформація” та “знання”, зокрема визначається, що *“інформація – сукупність відомостей, знань і повідомлень про об`єкти, явища і процеси”* [12]. Отже, можна говорити не лише про відсутність адекватного визначення “інформації”, а й про ототожнення двох якісно нових та фундаментально значимих ресурсів нового етапу розвитку людства.

Наступною не менш важливою проблемою розбудови інформаційного суспільства є деструктивні явища його розбудови: *по-перше*, збільшення інформаційних потоків, а також їх перенасиченість інформацією сприяє посиленню інформаційного шуму; *по-друге*, зростання “цифрової нерівності”, що лише ускладнює соціально-економічні процеси у суспільстві; *по-третє*, футурошок, породжений кардинальною зміною усталених цінностей та пріоритетів, а також відсутність чітко сформованих нових; *по-четверте*, “інформаційна колонізація”, яка виникає внаслідок відсутності або недостатності власних інформаційних ресурсів, породжує необхідність послуговуватись іноземними інформаційними ресурсами, що підкріплюються політичними прагненнями розвинених країн підкорити собі інші; *по-п’яте*, кіберзлочинність; *по-шосте*, можливість втручання в особисте життя людини тощо [13].

Тобто, як бачимо, у гонитві за новими технологічними можливостями, розвитком телекомунікацій, роботі на кількість, а не на якість ми забуваємо про наслідки нашої діяльності, адже збільшення інформаційних потоків – це не підвищення рівня освіченості громадян, інтенсифікація виробництва новітніх ІКТ – ще не інформаційне суспільство. Тому важливо розумно та планомірно реалізовувати заходи державної політики у сфері розбудови інформаційного суспільства, враховуючи комплексність та багатоаспектність цього процесу.

Погоджуючись з думкою О. Лисенко, що інформаційне суспільство має об’єднати націю навколо інтелектуальних, творчих, культурних, наукових ідей та здобутків [14], основним процесом переходу від інформатизації до інформаційного суспільства, який консолідував би навколо себе попередні здобутки та надав можливість ефективно реалізувати майбутні прагнення, у цій сфері пропонується розглядати інтелектуалізацію суспільства.

К. Бєляков пропонує розглядати інтелектуалізацію в рамках інформатизації суспільства, що є її заключним етапом та основною метою, пройшовши вже електронізацію, комп’ютеризацію та медіатизацію. Інтелектуалізація є складною гіперсистемою видів і підвидів людської діяльності, в основі якої лежить трудова,

суспільно-політична, навчальна, побутова, соціально-культурна діяльність, а також дозвілля [15, с. 14].

Інтелектуалізація, базуючись на основних принципах інформаційних відносин, апріорі висуває такі свої вимоги до інформації, як: повнота, об’єктивність, точність, універсальність, оперативність [16], зокрема, остання повноцінно може реалізуватись лише за допомогою ІКТ окрім вищеперерахованого можна додати також мобільність інформації, що значним чином може полегшити життя населення.

Унаслідок недостатньої розробки даної проблематики інтелектуалізація, розглядається переважно, у вузькому її розумінні та застосовується до певних сфер суспільного життя. Так, під інтелектуалізацією розуміють економічну категорію, а не суспільно необхідний процес розвитку людини в цілому, що розкриває нові перспективи та можливості. При цьому втрачається її реальний соціальний зміст, адже з економічної точки зору людину починають розглядати як ресурс, носій інтелектуального потенціалу, тобто спостерігаємо у дії принцип “людина для держави”, що кардинально різниться від основної мети нової цивілізації, яка полягає у пріоритетності інтересів людини, наданні можливості кожному реалізувати свій потенціал, а також сприяти суспільному та особистісному розвитку, підвищуючи якість та рівень життя суспільства, створити умови, де кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними [17].

Звісно, інтелектуалізація економіки може стати першим та досить успішним кроком до інтелектуалізації суспільства, адже конкуренція, породжена цим процессом, може стати продуктивним двигуном прогресу – як виробництва, так і людства в цілому. Підвищення вимог до працівників породжує конкуренцію на ринку праці, що у свою чергу потребує спеціальних знань, умінь та навичок з боку працівника, а збільшення питомої ваги розумових функцій людини на виробництві (управління, контроль, налагодження) сприятиме підвищенню кваліфікації та освітньо-культурного рівня населення [18].

Але не варто забувати і про інші сфери суспільного життя, адже ефективність проведення процесу інтелектуалізації можлива лише за рахунок різнобічного розвитку особистості, інтелектуалізації усіх сфер суспільного життя, широкого впровадження ІКТ для задоволення потреб населення, створення відповідної нормативно-правової бази, запровадження ефективних заходів державної політики та конкурентоспроможної економіки, стане оновою для гармонійного розвитку освіти і науки, проведення комплексних фундаментальних та прикладних досліджень у різних сферах суспільного життя, що неодмінно сприятиме інтелектуалізації суспільства та гармонійному розвиткові особистості. Інтелектуалізація має позитивно вплинути на кількість і якість інформації та знань у суспільстві, підвищити творчі та креативні здібності людей, створити соціальні та технологічні передумови для кращого використання інтелекту, а також для насичення системами штучного інтелекту і підвищення їх віддачі, всіх сфер суспільного життя, насамперед управління, науки, освіти, медицини, охорони навколишньою середовища [19, с. 8].

На основі проведеного аналізу сучасних проблем розбудови інформаційного суспільства можна зробити висновок, що інтелектуалізація суспільства є комплексним та багатоаспектним процесом, тому для його ефективного впровадження умовно можна виділити такі взаємопов`язані складові:

І. *Законодавче забезпечення* надання можливості кожній людині доступу до інформації, а також надання кожному можливості реалізувати свій потенціал. Заходами першої необхідності є систематизація інформаційного законодавства, зокрема,

залишається нагальною проблемою для врегулювання суспільних відносин у цій сфері прийняття Інформаційного кодексу України. Окрім того, необхідно внести зміни до Закону України “Про інформацію”, у якому надати визначення поняття “знання”, а також нове тлумачення терміна “інформація”. Розширити перелік принципів інформаційних відносин такими: оперативність та простота одержання, використання, поширення та зберігання інформації; універсальність та зрозумілість інформації. Прийняти програму інтелектуалізації населення України, у якій би викладались основні етапи її проведення та заходи державної політики даного процесу.

II. Запровадження низки *організаційних заходів* як з боку державних, так і недержаних інституцій. У першу чергу ці заходи мають стосуватись освітньої діяльності, адже гармонійний розвиток освіти і науки у поєднанні з інформаційними технологіями закладає основу для інтелектуалізації усіх сфер людського життя [20]. Підвищення рівня та якості освіти в Україні (як середньої, так і вищої). Створення відповідного ресурсного забезпечення проведення навчання та підвищення кваліфікації, популяризація та активне впровадження дистанційного навчання. Запровадження електронних бібліотек із повним доступом до їх джерельної бази. Особливо важливим є підвищення рівня освіти та спонукання до інтелектуального “збагачення” дорослого населення.

III. *Підвищення комп’ютерної грамотності* населення, адже завдяки розповсюдженню ІКТ, а також їх популярності серед населення знання отримують матеріального виразу, а їх закріплення в інформаційних ресурсах дає можливість максимально зручно та ефективно задовольняти потреби людей у різних сферах своєї діяльності [21, с**.** 15]. На базі ВНЗ, а також підприємств, установ та організацій створити курси і семінари щодо використання ІКТ для задоволення, насамперед виробничих та побутових потреб населення.

IV**.** *Підвищення рівня інформаційної культури* населення. Зокрема, В. Пилипчук вважає, що основою для майбутнього суспільства має бути баланс між духовними, соціальними і матеріальними цінностями, що реально сприятиме сталому розвитку людини, суспільства та міжнародної спільноти [22 с. 8]. Даний процес має полягати у низці організаційно-правових заходів державної політики, в основу якої має бути покладена система базових компонентів культури суспільства, пов’язаних з інформатизацією суспільної діяльності, що включає культуру правил організації подання, сприймання та використання інформації, культуру правил суспільних відносин із використанням мережі Інтернет і культуру суспільних правовідносин із застосуванням нових комп’ютеризованих інформаційних технологій [23].

Отже, як бачимо, поняття “інформаційне суспільство” нерозривно пов’язане з високим рівнем освіченості та інформаційної обізнаності громадян, адже сприйняття, перетворення та продукування нових відомостей, їх розповсюдження вимагають від людини правильного та адекватного усвідомлення отриманих даних, що неможливо без здатності людського інтелекту – мислення. А реалії сучасного інформаційного суспільства вимагають від людей як користувачів інформаційних потоків здатності до осмислення та критичного сприйняття отриманої інформації.

Висновки.

По-перше, інтелектуалізація є комплексним багатоаспектним процесом, що включає в себе сукупність організаційних, правових, економічних, соціальних, культурних та інших заходів державної політики, що спрямовані на розвиток особистісного потенціалу кожної людини, надання їй можливості оперативного та

безпосереднього одержання, використання, поширення, зберігання та захисту інформації та знань.

По-друге, інтелектуалізацію варто розглядати як у широкому, та і вузькому розумінні. Інтелектуалізація (у вузькому розумінні) – це розробка нових механізмів виробництва, які вимагали б наявності певних спеціальних знань у працівників. Інтелектуалізація (у широкому розумінні) суспільного життя – якісне інформаційне наповнення інформаційних ресурсів, збільшення їх кількості та доступності для різних верств населення, підвищення рівня освіченості населення та інформаційної культури.

По-третє, основна мета інтелектуалізації полягає у полегшенні доступу до роботи з інформацією та отриманні нових знань, що підвищує рівень освіченості та кваліфікації людини, а основним засобом є застосування ІКТ. Головним гаслом процесу інтелектуалізації суспільства має стати: “Освіта упродовж усього життя”.

По-четверте, інтелектуалізація є перехідним етапом від комп’ютеризації до інформаційного суспільства, що дасть можливість повноцінно використовувати ІКТ та примножувати блага цивілізації. Адже лише якісна інформаційна складова дає можливість для розбудови нової цивілізації. Особлива роль у даному процесі належить принципам інформаційних відносин (ст. 2 Закону України “Про інформацію”) [24], які є не лише основоположними ключовими ідеями суспільних відносин у даній сфері, а й окреслюють певний вектор обов’язкових вимог до інформації як до основи сучасної світобудови.

По-п’яте, знання та інформація є основними складовими характеристики розвитку інформаційного суспільства, вони нерозривно пов’язані між собою та мають взаємозалежний зв'язок, що значним чином впливає на подальший розвиток людства. Знання є якісно новою довершеною формою інформації, адже містять осмислене узагальнення людського досвіду. При цьому, отримавши матеріальну форму вираження знання набувають для суспільства інформаційного змісту (тобто є суб’єктивною формою інформації) та не мають настільки універсального характеру, як остання. Але слід зважати, що інформація у певних випадках має деструктивний вплив на особистість, іноді вона є просто “непотрібною” суб’єкту (інформаційний шум), що не можна сказати про знання.

Перспективи подальших досліджень варто зосередити на правових засадах розвитку інформаційного права, організаційних аспектах розбудови інформаційного суспільства та його інтелектуалізації, а також методологічних основах підвищення рівня інформаційної культури та комп’ютерної грамотності населення.

Висловлені у статті висновки та пропозиції не вичерпують даної проблематики, а лише підкреслюють її гостроту та актуальність як для юридичних, так і для суміжних наук, а також акцентують увагу на значимості цього питання для розбудови інформаційного суспільства.

Використана література

1. Чамара І. М. Інтелектуалізація праці як найважливіша умова економічного розвитку. – Режим доступу : //www.experts.in.ua/baza/analitic/index.php?ELEMENT_ID=10927

2. От информационного общества – к обществам знания. ЮНЕСКО ; сост. Е.И. Кузьмин, В.Р. Фирсов. – СПб., 2004. – 239 с. – (Всемирный саммит по информационному обществу).

3. На пути к обществам знаний : интервью с заместителем Генерального директора ЮНЕСКО по вопросам коммуникации и информации А.В. Ханом // Наука в информа-ционном обществе ; сост. Е.И. Кузьмин, В.Р. Фирсов. – СПб., 2004. – С. 22-26.

4. Тоффлер Э. Третья волна / Э. Тоффлер. : [пер. с англ.]. – М. : ООО “Издательство АСТ”, 2004. – 371 с.

5. Мелюхин И. С. Информационное общество : истоки, тенденции, проблемы развития / И.С. Мелюхин. – М. : Изд-во Моск. ун-та, 1999. – 208 с.

6. Арістова І. Методологічні засади розбудови суспільств знань // Правова інформатика. – 2008. – № 3 (19). – С. 10-17.

7. Про Національну програму інформатизації : Закон України від 04.02.98 р. № 74/98-ВР. – Режим доступу : //www.zakon4.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80

8. Пилипчук В.Г. Актуальні проблеми становлення і розвитку правової науки в інформаційній сфері // Інформація і право. – 2012. – № 1(4). – С. 15-22.

9. Див.: Про захист економічної конкуренції : Закон України від 11.01.01 р. № 2210-III. – Режим доступу : //www.zakon2.rada.gov.ua/laws/show/2210-14.; Про телекомунікації : Закон України від 11.01.01 р. № 2210-III. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2210-14.; Про адміністративну взаємодопомогу у сфері митних відносин : Міжнародна конвенція від 27.06.03 р. – Режим доступу : //www.zakon4.rada.gov.ua/laws/show/976_011 та ін.

10. Фурашев В.М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки // Інформація і право. – 2012. – № 1(4). – С. 46-55.

11. Советский энциклопедический словарь ; научно-редакционный совет: А.М. Прохоров (пред.). – М. : Советская энциклопедия, 1981. – 1600 с.

12. Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи : Постанова Кабінету Міністрів України від 20.01.97 р. № 40. – Режим доступу : //www.zakon4.rada.gov.ua/laws/show/40-97-%D0%BF

13. Див.: Колесніков Б.П. Державні механізми управління ризиками розвитку інформаційного суспільства в Україні : автореф. дис. на здобуття наукового ступеня доктора наук з державного управління : спец. 25.00.02 “Механізми державного управління” / Колесніков Борис Петрович ; Донецький державний університет управління. – Донецьк., 2011. – 39 с.

14. Лисенко О.О. Правовий захист суспільства від шкідливої інформації : автореф. дис. на здобуття наук. ступеня канд. юридичних наук : спец. 12.00.07 “Адміністративне право і процес; фінансове право; інформаційне право” / Лисенко Ольга Олександрівна; Харківський національний університет внутрішніх справ. – Х., 2011. Режим доступу : //www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCwQFjAA&url=http%3A%2F%2Fwww.irbis-nbuv.gov.ua%2Fcgi-bin%2Firbis_nbuv%2Fcgiirbis_64.exe%3FC21COM%3D2%26I21DBN%3DARD%26P21DBN%3DARD%26Z21ID%3D%26Image_file_name%3DDOC%2F2011%2F1LOOSHI.zip%26IMAGE_FILE_DOWNLOAD%3D1&ei=OHBeUoy_NuyX4wSQqoHIAw&usg=AFQjCNGucNjKQrV35cp_vJ2nBA_pWuXWjQ&sig2=v9V7UopWNq-po5P Hi4rhwA

15. Бєляков К.І. Організаційно-правове та наукове забезпечення інформатизації в Україні : проблеми теорії та практики : автореф. дис. на здобуття наук. ступеня доктора юридичних наук : спец. 12.00.07 – Адміністративне право і процес; фінансове право; інформаційне право / Бєляков Костянтин Іванович ; Національна академія наук України ; Інститут держави і права ім. В.М. Корецького. – К., 2009. – 41 с.

16. Апшай Н.І. Місце та роль бібліотеки в інформаційному просторі ВНЗ. – Режим доступу : //www.sportpedagogy.org.ua/html/journal/2010-09/10anidoi.pdf

17. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07 р. № 537-16. – Режим доступу : //www.zakon2.rada.gov.ua/laws/show/537-16.

18. Семченко О. О. Інтелектуалізація праці як основа виробничих сил і відносин. – Режим доступу : //www.rusnauka.com/6_NITSB_2010/Economics/58198.doc.htm

19. Врублевський В., Мороз О., Саєнко Ю. Доктрина Кравчука : начерк програми інтелектуалізації і формування модерної української нації. – К. : Інтелект, 2001. – 83 с. – (Українське товариство “Інтелект нації”; Інститут соціології НАН України).

20. Другов О. О. Інтелектуалізація як шлях до підвищення конкурентоспроможності реального сектору економіки України. – Режим доступу : //www.khibs.edu.ua/2(7)2009/R5/1.pdf

21. В. Брижко До питання щодо гуманітарної інформатизації // Правова інформатика. – 2003. – № 1. – С. 11-17.

22. Пилипчук В.Г. Концептуальні аспекти становлення і розвитку інформаційного суспільства : *матеріали “круглого столу” [Філософські та суспільно-правові проблеми становлення і розвитку інформаційного суспільства], (Київ, 20 березня 2013 р.)* : упорядн. : Андрусишин Б.І., Майстренко І.А., Пилипчук В.Г., Фурашев В.М. – Ужгород, ТОВ “ІВА”. – 2013. – 194 с.

23. Новицька Н. Б. Організаційно-правові аспекти інформаційної культури в управлінській діяльності : автореф. дис. на здобуття наук. ступеня канд. юридичних наук : спец. 12.00.07 – Адміністративне право і процес; фінансове право; інформаційне право / Новицька Наталія Борисівна; Національна академія державної податкової служби України. – Ірпінь, 2007. – Режим доступу : //www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fwww.irbis-nbuv.gov.ua%2Fcgi-n%2Firbis_nbuv%2Fcgiirbis64.exe%3FC21COM%3D2%26I21DBN%3DARD%26P21DBN%3DARD%26Z21ID%3D%26Image_file_name%3DDOC%2F2007%2F07nnbkud.zip%26IMAGE_FILE_DOWNLOAD%3D1&ei=UndeUpuMFLSu4QTS3YGgAw&usg=AFQjCNH76owYSkhkI5AVp6OWowHqa56Z_w&bvm=bv.54176721,d.bGE

24. Про інформацію : Закон України від 02.10.92 р. // Відомості Верховної Ради України. – 1992 р. – № 48. – Ст. 650 : в редакції Закону України від 13.01.11 р. № 2938-VI // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 313.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 343

СЕЛЕЗНЬОВА О.М., *кандидат юридичних наук, доцент,*
доцент кафедри цивільно-правових дисциплін
юридичного факультету,
ПВНЗ “Буковинський університет” (м. Чернівці)

ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: СУТНІСТЬ, ОСОБЛИВОСТІ, СТАНОВЛЕННЯ

Анотація. *У статті розглядаються особливості інформаційного суспільства в період його становлення, значна увага приділяється інформаційній свідомості. Проводиться розмежування категорій інформаційного суспільства та віртуального суспільства, причини різних рівнів інформаційного суспільства.*

Ключові слова: *інформаційне суспільство, інформаційна свідомість, віртуальне суспільство, Інтернет, мережево-інформаційна свобода.*

Аннотация. *В статье рассматриваются особенности информационного общества в период его становления, значительное внимание уделяется информационному сознанию. Проводится разграничение категорий информационного общества и виртуального общества, причины различных уровней информационного общества.*

Ключевые слова: *информационное общество, информационное сознание, виртуальное общество, Интернет, сетево-информационная свобода.*

Summary: *The article deals with features of information society during its formation, considerable attention is paid to information consciousness. The categories of information society and virtual society are distinguished. Article specifies the reasons for different levels of the information society.*

Keywords: *information society, information consciousness, virtual society, Internet, network and information freedom.*

Постановка проблеми. Людство у своєму шляху пройшло кілька етапів соціального розвитку – починаючи від первісних форм суспільного життя до багатогранного індустріалізму, який проте не є остаточним вибором організації людиною свого існування. Дедалі частіше говориться про появу та блискавичне становлення постіндустріального суспільства, котре називають інформаційним. Сам термін “інформаційне суспільство” з’являється на початку 70-х років ХХ століття; його вживають у своїх працях Ю. Ханші, Д. Белл, Ф. Махлуп та деякі інші науковці. Разом з тим, стрімка розбудова інформаційного суспільства обумовлює проведення ґрунтовних досліджень цього явища. Зважаючи на його постійну трансформацію та глобальний характер, актуальність наукового аналізу інформаційного суспільства не викликає сумнівів.

Аналіз останніх досліджень та публікацій. Свою увагу на сутність інформаційного суспільства звертали вчені різних галузей науки – філософії, соціології, політології (Р. Абдєєв, Д. Дубов, В. Іванов, М. Кастельс, А. Колодюк, В. Скалацький, Е. Тоффлер та інші). Розглядали інформаційне суспільство у своїх доробках і дослідники-юристи: І. Бачило, К. Бєляков, В. Брижко, В. Копилов, Н. Кушакова-Костицька, А. Новицький, Н. Савінова, П. Уваров та інші). Однак існуючі на сьогодні теоретичні узагальнення інформаційного суспільства потребують свого подальшого вивчення.

Метою статті є розкриття особливостей інформаційного суспільства та з’ясування умов його становлення в Україні.

Виклад основних положень. Як зазначає Є. Горошко, у XX столітті формування глобальних інформаційних мереж та систем, поява нових комунікаційних технологій вперше в історії людства створили умови пов’язати буквально кожного з кожним, об’єднати інформаційні ресурси нашої цивілізації та забезпечити доступ до них практично будь-якому жителю Землі [1, с. 407]. Такий стан речей дозволяє говорити про існування нової фази форми існування людини – інформаційного суспільства.

“Інформаційне суспільство” не представляє собою стале поняття. Оскільки сьогодні можна спостерігати його становлення, характерні ознаки інформаційного суспільства тільки формуються. Однак у сучасній науці існують неодноразові спроби дати визначення інформаційному суспільству. Так, приміром, останнє розглядають як витвір соціологічної концепції, що визначає головним чинником розвитку суспільства виробництво й використання науково-технічної та іншої інформації [2, с. 66], або обумовлюють як гуманітарну категорію, що описує якісні суспільні трансформації, зміщення акцентів із виробничої до невиробничої сфер, зміну характеру інформаційних потоків, групових та індивідуальних ідентичностей [3, с. 5] тощо. Такі визначення хоча і розкривають певну бік сутності інформаційного суспільства, проте не є повними та остаточними, через те, що категорія інформаційного суспільства носить міжгалузевий та міждисциплінарний характер. На наш погляд, така категорія може мати ознаки, притаманні їй особливості, але стале поняття (з огляду на його мінливість та всеохопленість) надати не представляється можливим. Наявні в сучасній науці різноманітні концепції та підходи лише підкреслюють багатоманітність проявів сутності інформаційного суспільства.

Впровадження інформаційних технологій відбувається швидко та носить масовий характер. Така ситуація зумовлює виникнення технократичного підходу, згідно з яким рівень інформаційного суспільства визначається кількістю інформаційних технологій. Іншими словами, чим більше застосовується інформаційних технологій в різних сферах життя, тим вищий рівень інформаційного суспільства. Думається, що такий підхід не є достатньо зваженим. Ми приєднуємося до позиції, коли технологічна особливість інформаційного суспільства є лише однією із складових частин процесу формування інформаційного суспільства. Зокрема, Н.Б. Новицька зазначає, що крім технологічної складової, в основі формування інформаційного суспільства лежать ще гуманітарна та правова складові [4, с. 165].

Формування інформаційного суспільства – неоднозначний складний процес, що передбачає перехід з одного стану в розвитку цивілізації до іншого. Його складність обумовлюється низкою особливостей. Розглянемо їх.

Згідно з С. Пюкке говорити про наявність інформаційного суспільства можна в тому випадку, коли більше половини його членів зайнято у сфері виробництва комунікативної інформації та надання інформаційних послуг [5]. Таке твердження є достатньо дискусійним. Чи є інформаційним суспільство, де такою діяльністю зайнята третина населення або якщо така діяльність тільки починає впроваджуватися? Зазначена ситуація дозволяє тільки характеризувати рівень інформаційного суспільства. Прагнення, можливості держави та окремої людини відіграють неабияку роль у формуванні інформаційного суспільства – від найнижчого до найвищого його рівнів.

Разом з тим, неправильним було б вважати, що суспільство, де інформація має важливе значення, буде інформаційним. В останньому інформацію можна зберігати, передавати, продавати, поширювати, користуватися. Тобто вчиняти із нею свідомі та спрямовані задля якоїсь цілі відповідні дії. Можна погодитися з С. Яскулою – “у сучасному інформаційному просторі зростає роль можливості орієнтації та механізмів відбору інформації” [6, с. 247]. Це і є показником позитивного розвитку інформаційного

суспільства, адже, як пише Н. Кушакова-Костицька, саме таке суспільство “характеризується насамперед тим, що головна роль у ньому належатиме інформаційній діяльності, яка стане найвищою цінністю” [7, с. 132].

Для зародження та подальшого становлення інформаційного суспільства відіграє першочергову роль інформаційна свідомість. На думку А.В. Колодюка, формування інформаційної свідомості – це фундаментальна передумова для використання інформаційно-комунікативних технологій в житті кожного громадянина [8, с. 10]. Дійсно, не усвідомивши роль та значення, а отже, потребу використання інформаційних технологій у побуті та суспільному житті, про існування і тим паче подальшу розбудову інформаційного суспільства не може бути й мови.

Інформаційну свідомість можна поділити на такі види:

а) за суб’єктним критерієм:

1) інформаційна свідомість людини – відображає ставлення особи до інформаційних технологій на побутовому рівні;

2) інформаційна свідомість колективу – обумовлює розуміння та використання групою осіб певної сукупності інформаційних знань (колектив науковців інституту, що займається проблемами інформаційного простору, колектив програмістів, студентське середовище відповідного факультету вищого навчального закладу і т.д.);

3) інформаційна свідомість народу – передбачає загальне уявлення про інформаційну сферу народом певної держави;

4) інформаційна свідомість людства – уявляється як глобальний показник усвідомлення людьми усіх країн інформаційного простору, його масштабу та можливостей;

б) за значимістю:

1) буденна інформаційна свідомість – характерна більшості людей;

2) професійна інформаційна свідомість – створюється цілеспрямовано та притаманна порівняно невеликому колу осіб із спеціальними знаннями.

Категорія інформаційної свідомості дає можливість розкрити поняття “споживача” та “неспоживача” інформації. Відокремлюючись від інформаційного надбання суспільства або володіючи занадто низьким рівнем інформаційної свідомості, людина представляє собою “неспоживача” інформації, тим самим випадаючи з інформаційного простору.

Зазначене поняття (“неспоживач” інформації) не нове і уже розглядалося в науці ще у 80-х роках XX століття [9], проте набирає значення та сучасного змісту з кожною новою фазою інформаційного суспільства. Особливим завданням стоїть зменшення кількості неспоживачів інформації, що сприяє тим самим позитивному розвитку інформаційного суспільства.

Існування неспоживачів інформації, різних видів інформаційної свідомості (або її відсутність), неоднаковий економічний та політико-правовий стан держав зумовлюють нерівномірність утворення та розвитку інформаційного суспільства. Одні країни прагнуть досягти найвищого рівня інформаційного суспільства, спрямовуючи у заходи з формування інформаційної свідомості та інформатизацію різних сфер життя значні фінансові ресурси, другі – обмежуються інформатизацією у провідних галузях та декларуванням основних принципів існування інформаційного суспільства, а треті – відпускають ситуацію на самоплив, обґрунтовуючи це браком коштів, важким економічним станом, невисокою інформаційною культурою населення. І звичайно, можна говорити, що інформаційне суспільство є суспільством без кордонів та не обумовлено певною територією, однак навряд хто буде заперечувати, що рівень інформаційного суспільства у Сполучених Штатах Америки незрівнянно вищий, ніж, скажімо, у Кенії. Тому, характеризуючи інформаційне суспільство як суспільство без

кордонів, варто розуміти під цим, що між споживачами інформації здійснюється обмін цією інформацією за допомогою відповідних засобів зв’язку (наприклад, завдяки мережі Інтернет), і при цьому справді кордони держав не відіграють ніякого значення.

Широке використання мережі Інтернет, загальна інформатизація, запровадження електронного документообігу сприяють зменшенню паперових носіїв інформації. Це є однією з вагомих особливостей інформаційного суспільства. В усі часи паперові книги та документи цінувалися дуже високо. Це був один з найбільш поширених способів зберегти інформацію та передати її наступним поколінням. В інформаційному суспільстві здійснюється переворот такого стану речей. Доступ до інформації можливий за допомогою загальнодержавних електронних інформаційних ресурсів, і паперові носії втрачають свою вагу.

Розглядаючи Інтернет як невід’ємний атрибут інформаційного суспільства, виникає питання розмежування понять “інформаційне суспільство” та “віртуальне суспільство”. Як підмічає Д.В. Дюжев, інформаційне суспільство є ціннісно-смисловою реальністю, складно організованим соціально-правовим утворенням життя людей на всіх рівнях – від локального до глобального [10, с. 11]. Віртуальне суспільство також характеризується складно організованою формою існування людини. Люди об’єднуються у спільноти, обговорюють насущні проблеми, купляють (продають) товари, вчаться тощо. Таке суспільство володіє і цінністю, і певною реальністю. Однак це є життя в мережі, а тому віртуальне суспільство відзначається “несправжністю”, значним обмеженням фізичних можливостей. Іншими словами, віртуальне суспільство є похідним явищем від інформаційного суспільства. Створюючи всі умови для виникнення та існування віртуального суспільства, інформаційним суспільством обумовлюється закономірність: чим вищий рівень самого інформаційного суспільства, тим більш структуровано якісним буде віртуальне суспільство. Це, до речі, є ще одним показником прояву застосування інформаційних технологій.

Розглядаючи віртуальне суспільство, визначимо також аспект юридично-філософського змісту його існування. За словами І.В. Вишева та А.В. Святова, формування інформаційного суспільства – це насамперед прогресивний процес, який сприяє розширенню людської свободи [11, с. 114]. Віртуальним суспільством обумовлюється нова складова свободи – мережево-інформаційна свобода, яка полягає у вільному виборі людиною віртуального співтовариства, відборі на власний розсуд потрібної інформації, а також користуванні (без обмежень, але в межах законодавства) продуктами і товарами, які забезпечуються віртуальним суспільством. Фактично можна говорити, що в інформаційному суспільстві забезпечуються не тільки природні, політичні та соціальні права людини, а й мають місце та охороняються державою інформаційні права, у тому числі право на мережево-інформаційну свободу, яка уможливлюється за допомогою існування віртуального суспільства.

Держава, що прагне досягти високого рівня інформаційного суспільства, повинна бути зацікавлена у співпраці з іншими державами, взявши за мету розширення інформаційного простору, більш повне застосування інформаційних технологій, всебічний розвиток віртуального суспільства. Подібний інтерес пояснюється такою особливістю, як глобальний характер інформаційного суспільства.

Як уже зазначалося вище, інформаційне суспільство не може обмежитися якоюсь територією, але рівні його різні. Причинами, за яких рівень інформаційного суспільства розвинутих країн відрізняється від інших, є:

1) незабезпечення органами державної влади фінансових ресурсів;
2) незацікавленість населення;

3) низький щабель інформаційної культури;

4) нормативне неврегулювання інформаційних відносин і відсутність національної стратегії;

5) невелика кількість інформаційно-комп’ютерних технологій;

6) незначний доступ до Інтернету;

7) незначні прояви вивчення та застосування можливостей інформаційної сфери в освіті;

8) низька якість життя та короткий строк середньої тривалості життя людини.

І щоб максимально згладити відмінності, передусім необхідна взаємодія різних держав. Одним із проявів такої взаємодії є безперервний культурно-інформаційний процес, що полягає в обміні важливої інформації про інформаційне суспільство. Так, наприклад, в Україні у свій час мав місце проект Британської ради “Бібліотеки в інформаційному суспільстві”, у ході якого проводилися зустрічі-дискусії, інформаційні дні та брифінги, семінари, здійснювалося формування ресурсної бази з актуальних питань розвитку бібліотечної справи й забезпечення вільного доступу до її використання, а також була реалізована програма видання британських книжок українською мовою, корисних для бібліотекарів та інформаційних працівників [12, с. 5].

Така співпраця набуває особливо актуального значення для України, адже становлення інформаційного суспільства в нашій державі носить дещо ситуативний та фрагментарний характер. Основними негативами (за Є.С. Цимбаленком) є: інформаційна нерівність, маніпулювання інформацією засобами інформаційно-комунікаційних технологій через збільшення обсягів інформації, психологічна прив’язаність особи до комп’ютера, залежність від засобів комунікації та іншої цифрової техніки, ототожнення особи з віртуальним образом у віртуальній реальності, зменшення рівня міжособистісного спілкування, стирання національно-культурних особливостей, нав’язування цінностей одних культур іншим [13, с. 64]. Крім цього, О. Олійник називає й інші: правова неврегульованість суспільних відносин, пов’язаних з формуванням, розвитком, використанням і захистом інформаційних ресурсів, безсистемний бурхливий стан інформації, окупованість українського ринку засобів інформатизації та захисту інформації іноземними фірмами, недостатній рівень фінансування науки, щоб витримати конкурентну боротьбу в інформаційно-технологічному секторі економіки [14, с. 100].

З огляду на таку ситуацію всебічне сприяння формуванню інформаційного суспільства є першочерговим завданням як для вищих державних органів, так і для решти суб’єктів інформаційних відносин. Деякі кроки у даному напрямі вже зроблено. Як відзначає А.М. Новицький, в Україні йде робота щодо нормативно-правового регулювання процесів суспільних відносин, пов’язаних із становленням і формуванням інформаційного суспільства в Україні. Даними нормативними актами визначено основні стратегічні напрями та поставлено завдання для всіх органів влади щодо реалізації загальнодержавної програми будівництва відносин, які будуть відповідати теоретичним баченням науковців щодо інформаційного суспільства [15, с. 189].

Таким чином, створення нової нормативно-правової бази, удосконалення існуючих актів значно покращують перебіг становлення інформаційного суспільства в Україні. Однак залишається досить багато аспектів, на які слід звернути увагу при переході до вищого щабля розвитку інформаційного суспільства.

Висновок.

Інформаційне суспільство – новий етап розвитку людської цивілізації. Багато країн тільки починають прямувати до нього. Разом з тим, це невідворотний процес, який, однак, у кожній державі має свій шлях. Інформаційне суспільство, перебуваючи у стані

свого становлення, на даний момент не може мати наукової дефініції, яка задовольняла б різні галузі науки. Проте інформаційне суспільство має низку особливостей, які потребують подальшого дослідження. Такі дослідження є вкрай актуальними для України, оскільки інформаційне суспільство в державі тільки починає формуватися.

Використана література

1. Горошко Е. Интернет и становление информационного общества в Украине / Е. Горошко : *збірник наук. праць [“Соціальні виміри суспільства”]*. – 2009. – Вип. 1 (12). – С. 407-416.
2. Дудко О.С. Феномен терміна “інформаційне суспільство” в міжнародній інформаційній політиці // Інформаційне суспільство. – 2011. – Вип. 14. – С. 66-71.
3. Дубов Д. В. Інформаційне суспільство в Україні : глобальні виклики та національні можливості : аналіт. доп. / Д.В. Дубов, О.А. Ожеван, С.Л. Гнатюк. – К. : НІСД, 2010. – 64 с.
4. Новицька Н.Б. Право і мораль як соціальні регулятори формування інформаційного суспільства в Україні // Науковий вісник Національного університету ДПС України (економіка, право). – 2012. – № 1 (56). – С. 164-169.
5. Пюкке С. Информационное общество и проблемы социального развития. – Режим доступу : //www.i-u.ru
6. Яскула С. Общества в новом информационном пространстве : *збірник наук. праць : [Міжнародний науковий форум : соціологія, психологія, педагогіка, менеджмент]*. – К. : Вид-во НПУ ім. М. П. Драгоманова, 2010. – Вип. 2. – С. 235-249.
7. Кушакова-Костицька Н. Від свободи слова – до інформаційного суспільства // Право України. – 2004. – № 7. – С. 129-133.
8. Колодюк А.В. Інформаційне суспільство : сучасний стан та перспективи розвитку в Україні : автореф. дис. на здобуття наук. ступеня канд. політ. наук / А.В. Колодюк. – К., 2005. – 20 с.
9. Бурый-Шмарьян О.Е. Непотребители информации (причины их появления, категории, характеристики) // Проблемы информационного обеспечения фундаментальних и прикладних научных исследований. – М.,1983. – Ч. 1. – С. 37-89.
10. Дюжев Д.В. Інформаційне суспільство: соціально-правова парадигма суспільного розвитку : автореф. дис. на здобуття наук. ступеня канд. філософ. наук / Д.В. Дюжев. – Донецьк, 2004. – 19 с.
11. Вышев И.В. Переход к информационному обществу – новый фактор решения проблемы практического бессмертия человека / И.В. Вышев, А.В. Святов : *материалы научно-практической конференции (Екатеринбург, 17 – 18 декабря 2003 г.).* – Екатеринбург, 2003. – С. 112-116.
12. Інформаційне суспільство : новини, інформація та досвід Великої Британії. – К., 2000. – 44 с.
13. Цимбаленко Є.С. Інформаційне суспільство : стан розбудови і проблеми // Інформаційне суспільство. – 2011. – Вип. 14. – С. 59-65.
14. Олійник О. Захист інформації в умовах інформаційного суспільства // Право України. – 2005. – № 10. – С. 100-103.
15. Новицький А.М. Правові передумови формування інформаційного суспільства в Україні // Науковий вісник Національного університету ДПС України (економіка, право). – 2009. – № 4 (47). – С. 185-190.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 002.55: 316.324.8

БАЙРАЧНА Л.К., *кандидат філософських наук, доцент*
кафедри конституційного права України
Національного університету “Юридична
академія України імені Ярослава Мудрого”

РОЛЬ ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ У ФОРМУВАННІ ПОЛІТИЧНОГО ІМІДЖУ ДЕРЖАВНОЇ ВЛАДИ

Анотація. *Розглядається особливість формування політичного іміджу державної влади засобами масової інформації в сучасних умовах. Показано, що політичний імідж державної влади містить у собі три компоненти: імідж політичного діяча (лідера), імідж правлячої політичної партії й політичний імідж держави. Доводиться, що засоби масової інформації є найважливішим фактором формування певної політичної свідомості.*

Ключові слова: *засоби масової інформації, імідж політичного діяча (лідера), імідж правлячої політичної партії, політичний імідж держави.*

Аннотация. *Рассматривается особенность формирования политического имиджа государственной власти средствами массовой информации в современных условиях. Показано, что политический имидж государственной власти включает в себя три компонента: имидж политического деятеля (лидера), имидж правящей политической партии и политический имидж государства. Доказывается, что средства массовой информации являются важнейшим фактором формирования определенного политического сознания.*

Ключевые слова*: средства массовой информации, имидж политического деятеля (лидера), имидж правящей политической партии, политический имидж государства.*

Summary*. The article considers feature forming political image of the government by media in the modern world. It is shown that the political image of the government comprises three components: the image of a politician (leader), the image of the ruling political party and the political image of the state. We prove that the media is a critical factor in shaping a political consciousness.*

Keywords: *media, the image of a politician (leader), the image of the ruling political party, the political image of the state.*

Постановка проблеми. У сучасному суспільстві фактор іміджу відіграє особливу роль у політичних процесах. Імідж учасників політичного процесу здатний визначити хід і результат виборів, а політичний імідж державної влади здатний вплинути на наступний вектор розвитку сучасного соціуму. Необхідними умовами для подальшого успішного просування реформ, побудови соціальної держави, вирішення проблем розвитку суспільства виступають обґрунтованість і суспільна підтримка дій влади. Імідж, виступаючи в ролі основного символічного посередника між представниками влади й суспільством, є найважливішим засобом інформаційно-комунікаційного впливу на різні соціальні групи з метою формування певної політичної свідомості й спонукання їх до певних дій (або бездіяльності). Тому проблеми формування й керування політичним іміджем державної влади і впровадження його в масову свідомість набувають особливо важливе значення в умовах трансформацій, які відбуваються в державній системі України, що знаходить своє відображення в законодавстві [1; 9; 10]. Виникнення й широке поширення нових технологій в області формування та впровадження іміджу суб’єктів політики в масову свідомість постійно надає даній проблемі злободенний характер і актуальність.

Аналіз наукових доробок з даної теми свідчить**,** що проблема ролі засобів масової інформації (далі – ЗМІ) у формуванні політичного іміджу державної влади спирається на вагому теоретичну базу. Теоретичним підґрунтям дослідження проблеми взаємодії влади і ЗМІ стали теорії зв’язку мас-медіа і демократії Д. Кіна, чотири теорії преси у трактуванні Ф. Сіберта, Т. Перерсона і У. Шрамма та їх критика Ф. Уебстером; теорії “паблік-рілейшнз” С. Блека, С. Катліпа, А. Сентера, Х. Брума, які були продовжені у сучасних розробках М. Метіса, Т. Репкової, Л. Швидунової та ін. Комунікативні моделі взаємодії політики і суспільства, їх вплив на суспільно-політичні процеси розглянуті на основі досліджень філософів-постмодерністів Ю. Габермаса, Е. Тофлера, М. Маклюена, Г. Лассуела, Ж. Бодрійяра. Використані також праці І. Панаріна, В. Попова, С. Михайлова, А. Русакова, М. Грачева, в яких висвітлені проблеми інформаційної політики та взаємодії політики й ЗМІ.

На сьогодні вітчизняними науковцями досліджуються окремі проблеми взаємодії державної влади і ЗМІ, зокрема стосовно ролі ЗМІ у формуванні позитивного іміджу державної влади (роботи І. Колосовської, Ю. Падафета, О. Порфімович, О. Швець); відкритості владних інституцій та технології інформаційної взаємодії в процесі прийняття управлінських рішень (праці Я. Гонцяж, Н. Гнидюк, І. Ібрагімової та ін.); розвитку системи зв’язків з громадськістю як інституту державного управління (роботи С. Колоска, О. Мех, Л. Руіс Мендісабаль). У процесі визначення шляхів оптимізації взаємодії влади і ЗМІ на особливу увагу заслуговують дослідження О. Бабінової, Н. Дніпренко, О. Д’якової, О. Нестеренко, О. Радченко, Ю. Работи, А. Серанта, В. Середюк-Буз, Т. Слінько. Ці дослідження дають можливість всебічно й ретельно розглянути зазначену проблему.

Метою статті є виявлення особливостей формування політичного іміджу державної влади ЗМІ в сучасних умовах. Для досягнення поставленої мети необхідно проаналізувати й узагальнити наявні теоретичні дані про імідж суб’єктів політики, про процес його формування; виявити основні технології формування й підтримки політичного іміджу, використані у процесі взаємодії представників влади й суспільства

Виклад основних положень. Політичний імідж це штучно створюваний, стійкий, соціально-психологічний образ того або іншого суб’єкта політики, що впливає на поводження особистості в політичній сфері суспільства та включає в себе як загальні характеристики, властиві іміджу взагалі, так і особливі ознаки, властиві конкретному різновиду політичного іміджу. Політичний імідж державної влади містить у собі три компоненти: імідж політичного діяча (лідера), імідж правлячої політичної партії й політичний імідж держави.

Структура іміджу політичного діяча представлена набором іміджевих характеристик: моральні характеристики (чесність, порядність, справедливість, принциповість, обов’язковість); професійні характеристики (компетентність, освіченість, діловитість, працездатність, відповідальність, рішучість); соціальні характеристики (турбота про населення, розуміння його проблем, доброта, людяність, чуйність); персональні характеристики (фізичні й психофізіологічні особливості, характер, тип особистості). Імідж політичного діяча (лідера) синтезує сукупність уявлень про зовнішність, особистісні й професійні якості, місце в певній ієрархії, переконання, спосіб життя й стиль політичної діяльності. Він здатний формувати у свідомості громадян певне ставлення до політики в цілому (як до сфери громадського життя), мотивувати відповідне політичне поводження, викликати в населення інтерес до соціально-політичних та інших процесів, що відбуваються в суспільстві.

За допомогою іміджу створюється яскравий образ політика, який запам’ятовується. Дійсно, якщо подивитися на ситуацію, яка склалася в Україні у 90-х роках ХХ ст., то можна зазначити, що суспільство проявило значно більше уваги політикам, які зруйнували стереотипне уявлення про керівника, що склалося у радянські часи, і продемонстрували принципово нову модель поведінки (наприклад, перший Президент незалежної України Л. Кравчук, який стояв у витоків злому тоталітарної системи, перший з вітчизняних керівників зняв краватку і не приховував свої людські слабкості) – ніж політикам, які не зуміли створити свого образу. Нинішня ситуація нестабільності в Україні робить затребуваними образи політиків, що асоціюються у масовій свідомості з типом сильної особистості (лідер – “захисник”), здатним захистити населення від хаосу і гарантувати суспільну безпеку. Інший популярний образ – це політик-господарник, здатний облаштувати життя регіону чи країни в цілому.

Про політика як реальну людину та її лідерський потенціал ми, як правило, судимо за тим образом, який складається під впливом ЗМІ, політичної реклами і самих заяв політика, а також за результатами його діяльності. При цьому “віртуальний” образ політика не завжди збігаються з реальним прототипом.

Імідж політичної партії містить у собі програмно-ідеологічну, діяльнісну, особистісну (лідерську) і зовнішню (атрибутивну) складові. Програмно-ідеологічна складова є основою іміджу політичної партії, оскільки відображає основний зміст створення й діяльності політичної партії. Партія, що не має своєї програми й ідеології, не може бути повноцінною політичною партією, оскільки позбавлена будь-якого політичного змісту. Формування іміджу партії за допомогою діяльнісної складової припускає ініціювання й проведення партійними органами спеціальних PR-заходів, спрямованих на підвищення популярності партії. Лідери політичної партії зазвичай виступають її обличчям, особливо в процесі комунікацій з виборцями, тому їхній імідж багато в чому буде проектуватися на імідж всієї політичної партії, а в деяких випадках і повністю асоціюватися з ним. Зовнішня (атрибутивна) складова іміджу партії – це певний набір основних атрибутів політичної партії: емблема (логотип), колірна гама партійної символіки, стиль написання назви й слоганів партії, прапори, єдине стильове рішення Інтернет-ресурсів політичної партії й т. п.

Структура іміджу держави містить у собі умовно-статичні характеристики (природний ресурсний потенціал, геополітичні параметри й т. д.); умовно-динамічні характеристики (соціально-психологічні настрої в суспільстві, показники економічного розвитку країни, правовий простір держави, політико-правовий режим, ефективність владної конструкції); характеристики-константи, тобто історично сформовані національні образи-символи, пов’язані з географічними, історико-культурними й іншими особливостями.

Формування політичного іміджу – це складний і багатоступінчатий процес, що включає в себе певні стадії. Найбільш важливими є такі стадії, як визначення очікувань і вимог цільової аудиторії до політичного лідера або партії; впровадження необхідних характеристик у формований імідж; просування сформованого іміджу за допомогою засобів масової комунікації; постійне коректування основних параметрів іміджу відповідно до потреб цільової аудиторії. У процесі формування політичного іміджу державної влади визначення найбільш ефективних методів, прийомів і способів впровадження іміджу в масову свідомість є особливо важливим завданням при розробці іміджевої стратегії. Формування політичного іміджу й впровадження його в масову й індивідуальну свідомість громадян здійснюється в процесі політичної комунікації за допомогою спеціальних засобів інформаційно-психологічного впливу, таких як політична реклама, політична пропаганда й політичний PR.

Для застосування перерахованих методів і прийомів формування іміджу необхідне комунікаційне середовище, сукупність умов, що дозволяють громадянам здійснювати передачу, обмін інформацією шляхом взаємодії один з одним. У зв’язку з цим багаторазово зростають роль і значення ЗМІ. Усе більш важливу роль відіграє характер взаємодії ЗМІ й органів влади. При цьому чітко проявляється двоїста роль самих ЗМІ в системі “держава – ЗМІ – громадянське суспільство”. З одного боку, ЗМІ в силу своєї природи, об’єктивно в більшому або меншому ступені включені в управлінський механізм державних структур. З іншого, вони орієнтовані на задоволення інформаційних потреб і інтересів як окремої особистості, так і всіх соціальних інститутів. Крім цього, характер взаємовідносин у системі “держава – ЗМІ – громадянське суспільство” багато в чому визначається особливостями історичного розвитку України [3].

Завдання органів влади в цих умовах – забезпечення політичної рівноваги, балансу інтересів, стабільності. Від того, як взаємодіють суб’єкти інформаційного простору в системі “органи влади – ЗМІ – суспільство”, залежить рівень розвитку демократії в суспільстві й державі. Тому проблема узгодження позицій державних і суспільних структур, соціальних інститутів і спільнот у формованому ЗМІ інформаційному просторі стає досить актуальною й вимагає глибокого наукового дослідження. ЗМІ є одним з основних каналів передачі інформації про партію, лідера, об’єднання, державну владу й, відповідно, формують про них певне уявлення (імідж).

Ми охарактеризуємо основні ЗМІ, задіяні у формуванні політичного іміджу: друковані видання (газети, журнали), радіо й телебачення. Необхідно відзначити, що ЗМІ є каналом поширення як політичної реклами, так і вільної інформації (експертні оцінки аналітиків у друкованих виданнях, телевізійних виступах і новинах). Саме ця особливість ЗМІ та їх використання у виборчих кампаніях також дозволяє говорити про формування презентіруемого і перцептивного (перцепція – багатофункціональний процес, який передбачає сприйняття зовнішніх ознак людини, співвіднесення їх з її особистісними характеристиками, інтерпретацію і прогнозування на цій основі її вчинків) політичного іміджу за допомогою ЗМІ. Тобто знання того, як структурувати інформацію, де, ким і коли вона буде найбільше ефективно сприйнята, який вплив на населення мають експертні оцінки та новини – у цьому закладена основа формування ефективного іміджу й зближення презентіруемого й перцептивного його компонентів [4, с. 25].

Дослідження ЗМІ і їх ролі у формуванні політичного іміджу й виборчих кампаніях має свою історію у світовій науці. Перше дослідження мас-медіа і їх ролі в політиці було проведено під час президентської кампанії 1940 року в Америці Полем Лазарсфельдом, що вивчав ефект впливу ЗМІ на рішення електорату про голосування [7, с. 177]. Однак історія вивчення ЗМІ і їх ролі почалася задовго до нього.

У передемпіричну епоху наприкінці XIX – початку XX століття було досить багато досліджень, присвячених вивченню впливу преси. До цієї проблеми зверталися Max Weber (1910), Walter Lipman (1922), John Dewey (1927), Robert Ezra Park (1940). Властне емпіричні дослідження медіа-ефекту почалися в 30-і роки XX століття.

Роботи Лазарсфельда присвячені вивченню аудиторії й впливу на неї медіа у виборах 1940 і 1948 років. Крім цього, велися дослідження механізму коментаря й експертної оцінки та вивчення персонального впливу промови на аудиторію [19 – 21].

Дослідники стверджували, що найбільшої ефективності впливу медіа досягають у тому випадку, коли вони співзвучні поглядам аудиторії, тобто що медіа-навіювання (медіа-вплив) у під час виборчих кампаній неефективні й досягають зазвичай того, хто вже сформував своє рішення про голосування. Так само стверджувалося, що медіа підвищують ефективність особистого впливу авторитетного політичного лідера на

аудиторію. Тобто політична реклама в медіа повинна бути максимально персоніфікована. Тільки тоді вона буде ефективна.

Учень Лазарсфельда Joseph Klapper (1960) сформулював модель “обмеженого впливу” медіа, що протягом десятиліття залишалася домінуючою парадигмою в дослідженні ЗМІ. Але, зрештою, його опонентам, K. Lang and G.Lang (1959), V. Key (I960), J. Blumler (1964), вдалося довести широкомасштабну ефективність впливу медіа [14].

З 1970-х років дослідження медіа в США й Західній Європі концентруються навколо критичної й культурологічної парадигм. Критична парадигма багато в чому виходить із того припущення, що медіа-ефекти вивчаються на базі теорії “стимул – реакція” без проміжної стадії – “медіації” (посередництво). Зверталася увага тільки на один тип ефекту – навіювання. Пізніше стало вивчатися “медіа – послання”.

Найбільш фундаментальні з досліджень, що розвивають культурологічну парадигму, затверджують, що “медіа-ефект” – це відбиття “поведінкової гегемонії”. Ретельно вивчаються культурні традиції й ігнорується вивчення впливу індивідів. Вважається, що медіа-ефект сегментує аудиторію, дегуманізує її й відокремлює індивіда від культури. Згідно з цим аудиторія конструює значення повідомлень відповідно до культурної традиції.

Подібні у своїх оцінках ролі ЗМІ представники медіаорієнтованого й медіацентристського підходів, які розглядають систему відносин “ЗМІ – особистість”.

У першому випадку увага приділяється механізму підпорядкування людини силі впливу масової інформації; вивчається виконання її соціальних функцій і владна домінанта. Цей напрям представлений школою експериментальної риторики.

Медіацентристський підхід, що припускає місце розташування людини в центрі медіа-системи, вивчає людину як споживача масової інформації. Тут досліджуються тільки соціально-психологічні функції масової комунікації у відриві від соціальних. Найбільш відома концепція “використання й задоволення”, прихильники якої затверджують, що скоріше індивіди пристосовують ЗМІ до своїх здатностей, ниж ЗМІ підкоряють собі людей. Обираючи насамперед ту інформацію, що відповідає його потребам, індивід впливає на формування інформаційного ринку, крім того, він самостійно інтерпретує інформацію, яка до нього надходить. Можна погодитися з тим, що людина свідомо й цілеспрямовано відбирає інформацію, але проте, що вона активно впливає на структурування інформаційного ринку, говорити поки важко. Хоча, звичайно, приклади такого роду зворотного зв’язку в інформаційних структурах є: інтерактивне телебачення, комп’ютерні мережі. Але найчастіше, особливо в комунікативних політичних процесах, аудиторія – пасивна маса, не здатна протистояти потоку навіюваних повідомлень, ідей і уявлень та інших ідеологічних махінацій. За допомогою пропаганди ЗМІ нав’язують пасивному індивідові зразки й мірила, завдяки яким він судить про себе й про інших. Створюючи нову реальність, що представляє собою ілюзорний, складний світ, ЗМІ пропонують людині способи досягнення своїх бажань, дають їй забуття [13, с. 53].

Найбільш часто каналами поширення інформації, до яких вдаються партії та їх лідери, представники державної влади, є друковані видання, радіо і телебачення.

Політична інформація в газетах і журналах – найдавніший і традиційно використовуваний канал у політичному маркетингу.

Модифікація друкованих видань, що відбулася в результаті розвитку ринку, конкуренція з електронними засобами масової комунікації і в Україні, і за кордоном, зовсім перетворили друковані видання. Особливо це знайшло відображення у кількості опублікованого матеріалу. Частина видання стала віддаватися під рекламу. У розряд комерційних потрапила й політична реклама. І тут постало питання: а якою повинна бути політична реклама в газеті?

Газетна політична реклама не вважається найефективнішою із всіх видів реклами, які використовуються у виборчих кампаніях. По витратах на одного читача в щоденних газетах вона вважається дуже дорогою й легко ігнорується виборцями. Незважаючи на це, багато політичних діячів продовжують використовувати газети для розміщення політичної реклами.

Усе більш поширеною формою реклами стає випуск власної газети або періодичного видання, цілком або здебільше присвяченого партії, кандидатові або блоку. Як показує практика, такого роду видання не відрізняються коректністю: туди включаються не тільки рекламні матеріали про партію, блок або кандидата, а й телевізійні програми, кулінарні рецепти, анекдоти тощо. Проте треба відзначити, що такі видання, розповсюджувані безкоштовно, заповнюють відсутність інформації й періодичних видань у населення у зв’язку з дорожнечею підписки й падінням тиражу видань.

Виступ в пресі, спілкування з журналістами в процесі формування політичного іміджу не є такими потужними і поширеними каналами вербальної комунікації, як радіо.

Радіо у виборчих кампаніях було вперше використане під час президентських виборів 1928 року в США. Саме тоді виборці вперше змогли скласти враження про кандидатів, використовуючи радіоінформацію. Першим усвідомив якісно нові можливості радіо Президент Ф. Рузвельт, якій став активно використовувати його у своїй виборчій кампанії 1936 року. Згодом з поширенням телебачення роль радіо у виборчій боротьбі відійшла на другий план, і тільки із середини 1970-х років відбулося своєрідне відродження радіокомунікації в політичних кампаніях. Радіо стало популярним у політиків завдяки двом причинам: по-перше, миттєве упізнання імені; по-друге, вербальна активність. Політики люблять говорити, люблять сперечатися і висловлювати різні аргументи з різних проблем [14, с. 501]. Політична реклама на радіо вважається найефективнішою по витратах на кожного слухача. Більше того, реклама на радіо – відносно дешеве задоволення, що залежить винятково від рейтингу радіостанції. Якщо в США, у середньому, витрати виборчої кампанії національного рівня на телебаченні обходяться в 1 мільйон доларів, то радіореклама коштує в п’ять разів менше.

Радіоповідомлення успішно використовують для формування іміджу партії, об’єднання або кандидата. Більше того, радіо має деякі переваги перед іншими ЗМІ. Радіоповідомлення й політична реклама на радіо адресовані аудиторії, що погано охоплюється газетами або телебаченням: водіям, що перебувають на шляху, домогосподаркам, людям похилого віку, традиційно слухаючій радіопрограми молодіжній аудиторії.

Радіоімідж партії, об’єднання або кандидата дозволяє виборцям добудувати своє уявлення про політичного діяча або державну владу, а не нав’язує конкретні, не підлягаючі зміні образи. Запорука успіху радіореклами – її простота й повторюваність.

Якщо ми говоримо, що за радіо як каналом політичної комунікації – під час виборчої кампанії майбутнє, то сьогодні популярнішим каналом поширення інформації є телебачення. Якщо 69 % інформації, яку зчитують з телевізійного екрана, являє собою чисто візуальну інформацію, і лише 31 % – вербальну, то зрозуміло, що тут закладено потужний арсенал впливу. Візуальний канал оцінюється аудиторією як найбільш достовірний, оскільки перед нею залишається якби невідфільтрований шматочок дійсності.

Телебачення як джерело політичної інформації може бути використане в декількох жанрах: це “платна реклама” (рекламні ролики, звернення кандидатів до виборців, дебати, проведені кандидатами без участі журналістів) і вільна інформація (новини, коментарі, дебати, проведені журналістами).

Дослідження й аналіз текстів телевізійних новин і так званої вільної інформації приводять до розуміння того, що цей канал інформації відіграє усе більш значиму роль

при формуванні іміджу партії, об’єднання, кандидата в електоральному процесі, державній владі в цілому.

На наш погляд, повідомлення в новинах може мислитися аудиторією, з одного боку, як факт, тобто повідомлення про певні події, що прагне залучити аудиторію, з іншого боку, новини можуть стати основою для політичної активності виборців, тобто повідомлення може бути “добудовано” в рамках політичних уподобань того чи іншого виборця. Саме ці характеристики жанру, свобода чи видимість свободи інформації приваблюють до нього як політиків, так і виборців.

У політичному полі в реальному електоральному процесі ефективне поєднання політичної реклами і вільної політичної інформації може забезпечити формування позитивного іміджу партії, об'єднання, державної влади в цілому.

Висновки.

У демократичному суспільстві вважається цілком природним прагнення влади впливати на засоби масової інформації з метою використання їх можливостей для вирішення тих завдань, які вона перед собою ставить. Держава може й повинна бути важливим чинником регулювання діяльності ЗМІ й свободи слова. Але відсутність чіткої межі в цій сфері може призвести або до посилення елементів тоталітарності, коли домінує контроль влади над ЗМІ, або до псевдодемократії, коли вседозволеність позбавляє газетно-журнальні публікації та телерадіопрограми конструктивізму й ефективності. Формування іміджу державної влади відбувається в процесі політичної комунікації, в результаті впровадження в масову свідомість образів суб'єктів політики, які конструюються за допомогою технологій політичної реклами, пропаганди і політичного PR, що використовуються в ЗМІ.

Передбачається, що в ЗМІ дані технології зазнають значних змін, так само як і деякі стадії процесу створення політичного іміджу. Обумовлюються ці зміни специфічними особливостями інформаційного простору XX-XXI ст.ст., появою нових форм політичної комунікації, сучасними можливостями електронних ЗМІ.

В умовах інтенсивної інтернетизації політичної системи ЗМІ отримують все більше можливостей застосовувати найбільш ефективні технології формування політичного іміджу державної влади. У масову свідомість прагнуть впровадити свої іміджі конкуруючі суб’єкти політичного процесу. В українських умовах це іміджі десятків партій, блоків та незалежних кандидатів. У свідомості людей ці іміджі стикаються, конкурують, і кінцевий підсумок залежить від того, який саме імідж буде впроваджений ЗМІ в масову свідомість різних груп населення і знайде в ній для себе сприятливе ідеологічне, політичне і психологічне обґрунтування.

Подальший розвиток досліджень. Незважаючи на інтерес українських науковців до різних аспектів означеної проблеми, питання взаємодії державної влади і ЗМІ поки що не досліджувалися з точки зору концептуальних підходів до оптимізації їх інформаційної співпраці. Тому, на наш погляд, подальші дослідження слід спрямувати у напрямі конкретних рекомендацій щодо сучасних форм і методів співпраці влади і ЗМІ в умовах демократизації системи державно-управлінських відносин в Україні.

Використана література

1. Інформаційне законодавство України : збірник законодавчих актів у 6 томах ; за заг. ред. Ю.С. Шемшученка та І.С. Чижа. – К. : ТОВ Видавництво “Юридична думка”, 2005.

2. Колосок С.В. Зв’язки з громадськістю у формуванні іміджу органів державного управління : дис. на здобуття наук. ступеня канд. наук з держ. упр. : 25.00.01 / С.В. Колосок. – К., 2003. – 183 с.

3. Лашкіна М.Г. Концептуальні засади взаємодії органів державної влади та засобів масової інформації в умовах демократизації державного управління в Україні : дис. на здобуття наук. ступеня канд. наук : 25.00.01 / Марія Григорівна Лашкіна. – К., 2008. – 187 с.

4. Мельникова Т.С. Пропаганда как технология политического манипулирования // Власть. – 2010. – № 8. – С. 22-29.

5. Мельникова Т.С. Роль средств массовой информации в политической жизни современного общества. // Проблемы гуманитарных наук : история и современность.– Саратов, 2009. – Вып. 7. – С. 42-53. – (Альманах).

6. Мех О.В. Служби із зв’язків з громадськістю в органах виконавчої і законодавчої влади та місцевого самоврядування на сучасному етапі розвитку України : дис. на здобуття наук. ступеня канд. філол. наук : 10.01.08 / О.В. Мех. – К., 2004. – 173 с.

7. Почепцов Г.Г. Имидж : от фараонов до президентов / Г.Г. Почепцов. – К. : “АДЕФ-Украина”, 1997. – 328 с.

8. Почепцов Г.Г. Коммуникативные технологии двадцатого века / Г.Г. Почепцов. – М.-К., 2000. – 354 с.

9. Про підсумки парламентських слухань “Суспільство, засоби масової інформації, влада: свобода слова і цензура в Україні” : постанова Верховної Ради України від 16.01.03 р. № 441-IV // Відомості Верховної Ради України. – 2003. – № 16. – Ст. 130. – Режим доступу : //www.zakon 2.rada.gov.ua/laws/show/1761-15

10. Про прийняття за основу проекту Закону України “Про інформаційну відкритість органів державної влади та вищих посадових осіб України” : постанова Верховної Ради України від 17.12.04 р. № 2265-IV. – Режим доступу : //www.zakon1.rada.gov.ua/cgi-bin/laws/main.cgi

11. В.В. Речицкий. Символическая реальность и право / В.В. Речицкий. – Львов : ВНТЛ-Классика, 2007. – 730 с.

12. Руіс Мендісабаль Л.М. Зв’язки з громадськістю як комунікативний аспект державного управління : дис. на здобуття наук. ступеня канд. наук з держ. управління : 25.00.01 / Ліліана Миколаївна Руіс Мендісабаль. – К., 2001. – 189 с.

13. Избирательная кампания : стратегия, тактика, психологические аспекты / [И.М. Слепенков, Ю.П. Аверин, Б.Ф. Усманов, Э.М. Розенталь]. – М. : Российский центр избирательных технологий. – 1995. – 68 с.

14. Сэлмор С., Кандидаты, партии и избирательные кампании. Как делают выборы в Америке. – (Технология и организация избирательных кампаний : зарубежный и отечественный опыт) / С. Сэлмор, Б. Сэлмор; под ред. Комаровского В.С.. – М. : АиК-сервис. – 1995. – 726 с.

15. Уэбстер Ф. Теории информационного общества / Ф. Уэбстер ; *[пер. с англ. М.В. Арапова, Н.В.Малыхиной]* ; под. ред., Е.Л. Вартановой. – М. : Аспект Пресс. – 2004.– 400 с.

16. Шпаковский В. История связей с общественностью : электронный учебник для дистанционной формы обучения / В. Шпаковский – Режим доступу: //www.window.edu.ru/window_catalog/files/r24481/pr.pdf

17. Public relations : история вопроса // Услуги и цены. – 2005. – № 3. – Режим доступу : //www.uslugy.ru/a-id- 5867.html

18. Joseph Klapper The Effects of Mass Communication. – N.-Y., 1960. – P. 252.

19. P. Lazersfeld, B. Berelson, H. Gaudet. The People’s Choice. – N.Y., 1944.

20. P. Lazersfeld, M. Rosenberg. The Language of Social Research. – Glencoe. 1955.

21. P. Lazersfeld, W. Thielens. The Academic Mind : Social Sciences in the Time of Crisis. – N.Y., 1958.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.951:004

ЗОЛОТАР О.О., *кандидат юридичних наук, старший науковий співробітник,*
Науково-дослідний інститут інформатики і права НАПрН України
ТРУБІН І.О., *кандидат юридичних наук,*
Науково-дослідний інститут фінансового права

КЛАСИФІКАЦІЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Анотація. *Стаття присвячена аналізу наукових поглядів та стану нормативно-правового регулювання класифікації загроз інформаційній безпеці.*
Ключові слова*: інформаційна безпека, класифікація, загроза інформаційній безпеці.*

Аннотация*. Статья посвящена анализу научных взглядов и состояния нормативно-правового регулирования классификации угроз информационной безопасности.*
Ключевые слова: *информационная безопасность, классификация, угроза информационной безопасности.*

Summary*. The article is concerned with analysis of scientific views and the legal regulation of the classification of information security threats.*
Keywords*: information security, classification, information security threat.*

Постановка проблеми. В сучасних умовах розвиток більшості країн світу відбувається під впливом інтеграційних процесів. Якщо в окремих випадках (на рівні окремих країн) спостерігається добровільне об’єднання, то в інших заінтересовані у відповідному процесі держави спонукають до об’єднання шляхом використання спеціальних засобів та проведення відповідних заходів, зокрема і в інформаційній сфері, спрямованих на завдання шкоди для досягнення власних цілей.

Саме інформаційна сфера є однією з найбільш важливих, і її захист визначається серед пріоритетів державної політики. Необхідність підтримання безпеки схвалена на державному рівні, що пояснює активну діяльність уповноважених органів влади спрямовану на забезпечення інформаційної безпеки відносин, пов’язаних із збиранням, накопиченням, обробкою та передачею інформації.

Осторонь від цих перетворень не залишається й наука. Вчені досить активно беруть участь у розробці теоретичних положень, що стосуються інформаційної безпеки та можуть бути враховані у процесі прийняття політичних рішень. Предметом наукових дискусій є, як загальні організаційно-правові аспекти інформаційної безпеки, так і спеціальні, до яких можна віднести визначення загроз інформаційній безпеці, їх класифікацію тощо.

Варто зазначити, що питання пов’язані з темою дослідження, зустрічаються в працях: Берко А., Бодрука О., Бойченко О., Гуцу С., Живко З., Євдоченко Л., Кормича Б., Кузьменко Б., Євдоченко Л., Ліпкана В., Литвиненка О., Логінова А., Макарової М., Марущака А., Максименка Ю., Пилипчука В., Погребняка А. та інших.

Незважаючи на значний рівень наукового осмислення проблем інформаційної безпеки, питання загроз, зокрема їх класифікації, мають дискусійний характер, що й обумовлює актуальність статті. Водночас, теоретичні розробки досліджуваного питання необхідні для формування дієвої системи моніторингу та управління у сфері інформаційної безпеки, а також вдосконалення відповідної нормативно-правової бази.

Метою статті є узагальнення наукових поглядів щодо класифікації загроз інформаційній безпеці та оцінка положень відповідних нормативно-правових актів.

Задля досягнення поставленої мети визначені *завдання*:

– дослідження та узагальнення сучасних наукових підходів до класифікації загроз інформаційній безпеці;

– аналіз положень національного законодавства, що визначає загрози національній безпеці;

– формулювання авторського концептуального підходу до класифікації загроз інформаційній безпеці.

Виклад основного матеріалу. Розвиток інформаційного суспільства і, як результат, перетворення в різних сферах суспільних відносин, включаючи й економічні, призвели до появи ряду позитивних і негативних наслідків. До позитивних наслідків відносять такі: пришвидшення передачі інформації значного обсягу, прискорення її обробки та впровадження [16, с. 3], своєрідну трансформацію інформації, яка в наш час ототожнюється з цифровим або віртуальним простором.

Б. Кормич зазначає, що основні дії щодо збирання, зберігання, передачі та розповсюдження інформації здійснюються за допомогою спеціальних технічних засобів і технологій. Відповідно з розвитком науки та техніки ці інформаційні засоби і технології перетворилися на один із найважливіших компонентів інформаційних процесів, одночасно із самою інформацією та суб’єктами інформаційних відносин [9, с. 322]. Значною мірою розвиток вищезгаданих інформаційних засобів й технологій має одночасні негативні прояви – як то збільшення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків і баз даних, порушення технологій обробки інформації, запуску програм-вірусів, знищення та модифікація даних в інформаційних системах, перехоплення інформації в технічних каналах її витоку [16, с. 3].

У зв’язку з цим окремим предметом наукових дискусій є питання щодо безпеки та захищеності відносин, пов’язаних зі збором, обробкою, зберіганням й використанням інформації. У співвідношенні з поняттями “безпека” та “захищеність” “загрозою” можна вважати можливу небезпеку, тобто будь-які дії чи події, які можуть настати за різних обставин у навколишньому середовищі та стати передумовою порушення безпеки і завдання збитків.

Узагалі в інформаційних відносинах протягом останніх років сформувався та закріпився термін “інформаційна безпека”, під яким розуміють стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдано шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [16]. Тобто вже в цьому визначенні закладено певні підстави для класифікації, однак про це згодом.

На думку В. Ліпкана, загрози національним інтересам та національній безпеці в інформаційній сфері є синонімом поняття “інформаційна безпека” [13].

Інформаційна безпека є невід’ємним напрямом розбудови інформаційного суспільства, розвиток якого повинен відбуватись не тільки через нарощування технологічних можливостей здійснення інформаційного обміну, а й шляхом глибокого усвідомлення усіма суб’єктами інформаційних відносин – власниками інформації та її користувачами, виробниками інформаційних технологій і засобів, постачальниками послуг, державою – необхідності здійснення всіх заходів щодо інформаційних ресурсів та забезпечення інформаційної безпеки держави [3, с. 51].

Щодо правової науки, то, на думку А. Марущака, поглиблення досліджень з проблем інформаційної безпеки потрібно віднести до пріоритетів розвитку інформаційного права України. Загрози національній безпеці України, що виникають у сфері національних інформаційних ресурсів, зумовлюють актуальність наукових пошуків з проблем правомірного використання телекомунікацій у сучасному інформаційному суспільстві, юридичних механізмів протидії кібернетичним загрозам [17, с. 22].

Рівень сучасних викликів і загроз в інформаційній сфері наочно підтверджує справедливість і виключну значущість положень статті 17 Конституції України про те, що захист державного суверенітету і забезпечення інформаційної безпеки є однією з основних функцій держави і всього українського народу [20, с. 20].

Інформаційна безпека як складова національної безпеки відповідно до сучасного розвитку її теорії в узагальненому вигляді ґрунтується на таких базових елементах: національні інтереси – загроза – захист [18, с. 8]. Саме загрози стану захищеності суспільних відносин є важливим елементом процесу забезпечення інформаційної безпеки.

На нашу думку, це пояснюється тим, що інформаційну небезпеку створюють інформаційні загрози, які поширюються в інформаційному просторі. При цьому, інформаційні загрози – це сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства, держави в інформаційній сфері [19, с. 59].

Враховуючи те, що інформаційна безпека є невід’ємною складовою національної безпеки, її регулювання потребує дієвих механізмів у формі політичних рішень або прийнятих нормативно-правових актів. Функціонування відповідного механізму, на нашу думку, можливе лише за умови належного рівня наукового осмислення теоретичних положень щодо інформаційної безпеки взагалі та сутності загроз зокрема. Чинники, що зумовлюють ескалацію загроз інформаційній безпеці, мають комплексний характер – вони охоплюють усі сфери життєдіяльності людини, суспільства і держави, а відповідно мають міжвідомчий характер. Таким чином, на практиці аналіз загроз – це завжди суб’єктивний процес сприйняття певною особою чи соціальною групою певних факторів через призму власних інтересів і фахового рівня. Разом із тим, об’єктивне визначення загроз передбачає чітке усвідомлення параметрів, поза межами яких певне явище втрачає можливості саморегуляції та потребує зовнішнього втручання для збереження стабільності соціальної системи, а також певних умов, що перетворюють ті ж самі фактори або на реальну, або на потенційну загрозу [2].

Досліджуючи відносини у сфері забезпечення інформаційної безпеки, науковці звертають свою увагу на таке поняття, як “загрози інформаційній безпеці”. Подальше заглиблення в процес наукового пізнання згаданого питання дало змогу виявити відсутність єдності у поглядах, що стосуються класифікації відповідних загроз як на нормативно-правовому, так і на науковому рівнях.

Відповідно до Закону України “Про основи національної безпеки України” до загроз національним інтересам і національній безпеці в інформаційній сфері відносять наступні: 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 [23].

Доктрина інформаційної безпеки України визначає основні реальні та потенційні загрози інформаційній безпеці України, класифікуючи їх за сферами життєдіяльності особи, суспільства і держави, зокрема: у зовнішньополітичній сфері, сфері державної безпеки, воєнній, внутрішньополітичній, економічній, соціальній та гуманітарній, науково-технологічній, в екологічній сферах [5].

У Законі України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 − 2015 роки” загрозами інформаційній безпеці визначено: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [24].

У Державному стандарті України “Захист інформації. Технічний захист інформації. Основні положення” – ДСТУ 3396.0-96 безпосереднє формулювання класифікації загроз відсутнє, проте в ньому передбачено можливі шляхи реалізації загроз. Саме вони дають можливість уявити або визначити ймовірні загрози інформаційним відносинам (відносинам щодо збору, обробки й накопичення інформації). У частині 4.1.3 підпункту 4.1 пункту 4 визначено, що загрози можуть здійснюватися:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів [7].

Як критерій можна використати: спосіб впливу на інформацію або шляхи реалізації загроз.

Постанова Кабінету Міністрів України “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” містить пункт 16 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, який визначає, що для забезпечення захисту інформації в системі створюється комплексна система захисту інформації (далі – система захисту), яка призначається для захисту інформації від:

– витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

– несанкціонованих дій з інформацією, у тому числі з використанням комп’ютерних вірусів;

– спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування [22].

Як критерій можна використати: спосіб впливу на інформацію або шляхи реалізації загроз.

Державний стандарт України “Захист інформації. Технічний захист інформації. Терміни та визначення” – ДСТУ 3396.2-97 містить ряд термінів, пов’язаних з інформаційною безпекою, які мають пряме відношення до класифікації загроз [8].

Так, пункт 5 “Загроза для інформації” містить наступні визначення:

5.1. Витік інформації – неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання.

5.2. Порушення цілісності інформації – спотворення інформації, її руйнування або знищення.

5.3. Блокування інформації – унеможливлення санкціонованого доступу до інформації.

Класифікація загроз відповідно має наступний вигляд: загрози витоку інформації; загрози порушення цілісності інформації; загрози блокування інформації. Загальний критерій не визначено.

Така різноманітність класифікацій в чинному законодавстві обумовлена не лише різноманітними підходами до вибору класифікаційних ознак та цілями класифікації, а й відсутність належного теоретичного обґрунтування сутності загроз інформаційній безпеці. З метою узагальнення існуючих наукових поглядів щодо класифікації загроз інформаційній безпеці та визначення концептуального підходу до формулювання цього елементу правовідносин пропонуємо розглянути окремі з них.

Згадуваний вище професор В. Ліпкан пропонує класифікувати загрози інформаційній безпеці відповідно до загальної класифікації загроз національній безпеці: за джерелами походження: природного походження, техногенного походження, антропогенного походження; за ступенем гіпотетичної шкоди: загроза та небезпека; за повторюваністю вчинення: повторювані та продовжувані; за сферами походження: екзогенні та ендогенні; за ймовірністю реалізації: вірогідні, неможливі, випадкові; за рівнем детермінізму: закономірні та випадкові; за значенням: допустимі та неприпустимі; за структурою впливу: системні, структурні та елементні; за характером реалізації: реальні, потенційні, здійснені, уявні; за ставленням до них: об’єктивні та суб’єктивні; за об’єктом впливу – особа; суспільство; держава [13].

В іншій праці, інтегруючи різноманітні підходи, а також пропозиції щодо розв’язання даного питання, запропоновано такі види загроз інформаційній безпеці: розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання [12].

Схожі погляди на перелік загроз інформаційній безпеці висловлює: А. Логінов у власному дисертаційному дослідженні. Зокрема, вчений визначає загрози як:

- розкриття інформаційних ресурсів;
- порушення цілісності інформаційних ресурсів;
- збій у роботі обладнання [14].

Б. Кузьменко та О. Чайковська пропонують класифікацію загроз, яка ґрунтується на визначенні властивостей інформації:

- загрози порушення конфіденційності інформації, в результаті реалізації яких інформація стає доступною суб’єкту, що не володіє повноваженнями для ознайомлення з нею;
- загрози порушення цілісності інформації, до яких відноситься будь-яке зловмисне спотворення інформації, оброблюваної з використанням автоматизованих систем;
- загрози порушення доступності інформації, що виникають в тих випадках, коли доступ до деякого ресурсу автоматизованих систем для легальних користувачів блокується [10, с. 6-7].

У свою чергу С. Гуцу [4] та О. Литвиненко [11] сходяться на тому, що основні загрози інформаційній безпеці можна представити у такому вигляді:

– загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

– загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання);

– загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову).

Л. Євдоченко, формуючи власний підхід до класифікації інформаційних загроз та з метою вироблення рекомендацій щодо організації державою дієвих форм і методів забезпечення інформаційної безпеки, визначає і класифікує загрози за кількома критеріями: за способом впливу на об’єкти інформаційної безпеки (інформаційні, фізичні й програмно-математичні, організаційно-правові); за джерелами надходження (внутрішні та зовнішні); за характером вияву (політичні, економічні, організаційно-технічні) [6, с. 8].

Визначальною для процесу наукового пізнання є теза, що:

– трактування проблем, пов’язаних з інформаційною безпекою, для різних категорій суб’єктів може істотно відрізнятися, наприклад, безпека для закритих державних організацій та комерційних структур;

– інформаційна безпека не полягає винятково у захисті інформації. Це принципово ширше поняття. Суб’єкт інформаційних відносин може постраждати (отримати матеріальні і/або моральні збитки) не тільки від несанкціонованого доступу до інформації, а й від пошкодження системи, що зумовить перерву в роботі [1, с. 20].

Тому цілком логічними та вартими на увагу є класифікації загроз які мають більш вузький або, іншими словами, спеціальний характер, зокрема загрози інформаційній безпеці мережевих ресурсів.

Наприклад, М. Макарова виділяє такі ймовірні загрози в мережі:

– дані навмисно перехоплюються, читаються або змінюються;

– користувачі ідентифікують себе неправильно (з шахрайською метою);

– користувач отримує несанкціонований доступ з однієї мережі до іншої [15, с. 188].

У цьому ж контексті ширшу класифікацію пропонує А. Погребняк, який зазначає, що загрози можуть бути як випадковими, так і навмисними.

До випадкових загроз відносяться: а) помилки обслуговуючого персоналу і користувачів; б) втрата інформації внаслідок неправильного її збереження; в) випадкове знищення або заміна; г) збій у роботі устаткування, електроживлення, дискових систем, комплектуючих елементів мережі; ґ) некоректна робота програмного забезпечення, зокрема внаслідок зараження комп’ютерними вірусами тощо [21, с. 46-47].

До навмисних загроз відносяться: а) несанкціонований доступ до інформації і мережевих ресурсів; б) розкриття і модифікація даних і програм, їх копіювання; в) розкриття, модифікація або підміна трафіка обчислювальної мережі; г) розробка і поширення комп’ютерних вірусів, введення в програмне забезпечення логічних бомб; ґ) крадіжка магнітних носіїв і розрахункових документів; д) руйнування архівної інформації або навмисне її знищення; е) фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому; є) перехоплення та ознайомлення з інформацією, яка передана по каналах зв’язку [21, с. 50].

Висновки.

Будь-яка з наведених класифікацій до певної міри є умовною, оскільки:

1) залежно від мети та методів наукового пізнання може здійснюватись за різними підставами;

2) має суб’єктивний характер, тобто залежно від суб’єкта, що її здійснює, та його здатності розрізняти ознаки об’єкта класифікації.

У підсумку також варто відзначити теоретико-прикладне значення класифікації інформаційній безпеці. Вона обумовлена потребою внутрішньо-логічної впорядкованості цієї системи і, на нашу думку, виконує дві важливі функції – евристичну и аналітичну. Евристична функція забезпечує пошук, виявлення існуючих загроз, орієнтацію в них, вивчення сукупності певних груп, що стосуються окремих об’єктів та суб’єктів безпеки, умов часу і простору. Аналітична функція полягає у розробці методів аналізу цих загроз, перевірки її достовірності, виявлення шляхів їх нейтралізації.

Так, на теоретичному рівні вироблення єдиного підходу до критеріїв класифікації не є самоціллю, оскільки залежить від конкретних потреб теорії та практики. Водночас, це є одним із шляхів упорядкування понятійно-категоріального апарату такої науки та галузі, як інформаційне право. З практичної точки зору питання, що досліджується, безпосередньо пов’язане з реалізацією цілей розвитку інформаційного суспільства та напрямів відповідної національної політики, що визначаються в Основних засадах розвитку інформаційного суспільства в Україні на 2007 – 2015 роки.

Використана література

1. Берко А.Ю. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції / А.Ю Берко, В.А. Висоцька, І.В. Рішняк // Вісник Національного університету “Львівська політехніка”. – 2008. – № 610. – С. 20-33.

2. Бодрук О. Структури воєнної безпеки : національний та міжнародний аспекти : монографія / О. Бодрук. – К. : НІПМБ, 2001. – 300 с. – С. 37

3. Бойченко О. В. Політика інформаційної безпеки в системі інформаційного забезпечення органів внутрішніх справ // Форум права. – 2009. – № 1. – С.50-55.

4. Гуцу С.Ф. Правові основи інформаційної діяльності. – Режим доступу : http://studrada.com.ua

5. Доктрина інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 14/2009. – Режим доступу : // www.president.gov.ua

6. Євдоченко Л.О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації : автореф. дис. на здобуття наук. ступеня канд. наук з держ. упр. : 25.00.01 / Л.О. Євдоченко. – Л., 2011. – 24 с.

7. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. – [Чинний від 1997.01.01]. – Режим доступу : //www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=5D34EDB7C9C9D4491C0171ACCAD297E1?art_id=38883&cat_id=38836

8. Захист інформації. Технічний захист інформації. Терміни та визначення : ДСТУ 3396.2-97. – [Чинний від 1998.01.01]. – Режим доступу : //www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=5D34EDB7C9C9D4491C0171ACCAD297E1?art_id=38934&cat_id= 38836

9. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : дис. на здобуття наукового ступеня д-ра юрид. наук. : 12.00.07 / Б.А. Кормич. – Х., 2004.

10. Кузьменко Б.В. Захист інформації : навч. посіб. – Ч. 2 / Б.В. Кузьменко, О.А. Чайковська. – К. : Видавничий відділ КНУКіМ, 2009. – 69 с.

11. Литвиненко О. Проблема інформаційної безпеки в контексті міграційних процесів. – Режим доступу : //www.nbuv.gov.ua/portal/soc_gum/Ukralm/2012_7/lytvynenko.pdf

12. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції. – Режим доступу : //www.pidruchniki.ws/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi

13. Ліпкан В.А. Національна безпека України. – Режим доступу : //www.pidruchniki.ws/15341220/politologiya/ponyattya_vidi_zagroz_natsionalnim_interesam_natsionalniy_bezpetsi_informatsiyniy_sferi

14. Логінов А.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : дис. на здобуття наукового ступеня кандидата юридичних наук : 12.00.07 / А.В. Логінов. – Національна академія внутрішніх справ України. – К., 2005.

15. Макарова М.В. Електронна комерція : посібник для студентів вищ. навч. закладів / М.В. Макарова. – К. : Видавничий центр “Академия”, 2002. – 272 с.

16. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук. : 12.00.01 / Ю.Є. Максименко – К., 2007. – 22 с.

17. Марущак А.І. Пріоритети розвитку інформаційного права України // Інформація і право. – 2011. – № 1. – С. 20-24.

18. Олійник О.В. Організаційно-правові засади захисту інформаційних ресурсів України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.07 / О.В. Олійник. – К., 2006. – 20 с.

19. Соціально-правові основи інформаційної безпеки : навч. посібник / [В.М. Петрик, А.М. Кузьменко , В.В. Остроухов та ін.] ; за ред. В.В. Остроухова. – К. : Росава, 2007. – 496 с.

20. Пилипчук В.Г. Системні проблеми розвитку правової науки в інформаційній сфері // Вісник Академії правових наук України. – 2011. – № 3. – С. 16-27.

21. Погребняк А.В. Технології комп’ютерної безпеки : монографія / А.В. Погребняк. – Рівне : МЕГУ, 2011. –117 с.

22. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 29.03.06 р. № 373 // Офіційний вісник України. – 2006. – № 13.

23. Про основи національної безпеки України : Закон України : від 19.06.03 р. № 964-IV // Відомості Верховної Ради України. − 2003. – № 39.

24. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 − 2015 роки : Закон України : від 09.01.07 р. № 537-V // Відомості Верховної Ради України. − 2007. – № 12. – Ст. 102.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

І н ф о р м а ц і й н і т е х н о л о г і ї

УДК 004:347.453.8

САНДУЛ В.С., головний спеціаліст відділу взаємоз’єднання мереж та інфраструктури Департаменту зв’язку Національної комісії, що здійснює державне регулювання у сфері зв’язку та інформатизації України

УРЕГУЛЮВАННЯ ВІДНОСИН МІЖ ОПЕРАТОРАМИ ТЕЛЕКОМУНІКАЦІЙ ПРИ ВЗАЄМОЗ’ЄДНАННІ МЕРЕЖ

***Анотація**. Щодо удосконалення нормативно-правової бази для врегулювання відносин між операторами телекомунікацій при взаємоз’єднанні мереж та використанні технології мереж наступного покоління (Next Generation Networks – NGN).*

***Ключові слова:** телекомунікаційні послуги технології мереж наступного покоління (Next Generation Networks – NGN), оператори/провайдери, споживачі телекомунікаційних послуг.*

***Аннотация.** О совершенствовании нормативно-правовой базы для урегулирования отношений между операторами телекоммуникаций при взаимосоединении сетей и использовании технологии сетей следующего поколения (Next Generation Networks – NGN).*

***Ключевые слова:** телекоммуникационные услуги, технологии сетей следующего поколения (Next Generation Networks – NGN), операторы/провайдеры, потребители телекоммуникационных услуг.*

***Summary.** Regarding the improvement of legal framework for the regulation of mutual relations between telecommunications operators in взаимосоединении networks, using the technology of next generation networks eration (Next Generation Networks – NGN).*

***Keywords:** telecommunication services technology next-generation networks (Next Generation Networks – NGN), operators/providers, consumers of telecommunication services.*

Постановка проблеми. Галузь телекомунікацій займає досить важливе місце у життєдіяльності суспільства. Її стан та розвиток впливають на рівень якості життя, а саме – на якість освіти, культури та інформації, яку отримує людина, і, врешті-решт, є необхідним підґрунтям, що створює умови покращання матеріальної забезпеченості спільноти [1].

Зростаючі потреби суспільства у нових високотехнологічних телекомунікаційних послугах сприяють швидкому та динамічному розвитку галузі зв’язку.

Держава сприяє максимальному задоволенню потреб суспільства шляхом удосконалення нормативно-правової бази у сфері телекомунікацій для забезпечення взаємодії у новій структурі телекомунікаційних мереж з метою підвищення ефективності їх використання відповідно до міжнародних вимог та стандартів і нових технологічних рішень [2].

Метою статті є удосконалення нормативно-правової бази щодо врегулювання взаємовідносин між операторами телекомунікацій при взаємоз’єднанні мереж для задоволення споживачів у телекомунікаційних послугах, при використанні технології мереж наступного покоління (Next Generation Networks – NGN).

Виклад основних положень. Концепцією розвитку телекомунікацій в Україні встановлено, що стратегія розвитку спрямована насамперед на здійснення заходів на базі телекомунікаційних мереж наступного покоління, що передбачає конвергенцію телекомунікаційних та інформаційних мереж і послуг [3].

Питання законодавчого врегулювання відносин та взаємодії між суб’єктами ринку телекомунікацій при взаємоз’єднанні їх телекомунікаційних мереж, побудованих за ієрархічною архітектурою, були розглянуті раніше, а необхідність та вплив державного регулювання таких відносин детально обґрунтовані в [2].

Принципи демократичності, конвергенції та адаптивності сформулювали образ сучасних систем зв’язку, систем NGN та нову ідеологію систем зв’язку.

На заміну діючих мереж зв’язку, побудованих у відповідності з принципами ієрархії та з положеннями нормативно-правових документів, що встановлюють технічні вимоги, приходять нові покоління мереж зі своїми технічними та технологічними рішеннями і відповідним обладнанням.

На етапі розвитку цифрового зв’язку, коли трафік даних виявився важливішим за голосовий, а комп’ютер – важливішим за телефон, з’явилось технічне рішення, що ґрунтується на технології NGN [4]. Основним елементом інфраструктури NGN є обладнання комутації пакетів.

Технологія NGN є революційною по суті, а її можливості призведуть до корінних змін як у ставленні до користувачів, так і в відносинах між суб’єктами ринку телекомунікацій.

Концепція NGN передбачає, що передача даних важливіша за передачі голосу, а в технологічному сенсі – комутація пакетів і пакетний трафік важливіші за комутацію каналів.

За допомогою інтеграції різних мереж утворюється єдина мережева інфраструктура на базі IP, що забезпечує надання послуг ATM/FR, Internet, IP-VPN і Ethernet. Такою інфраструктурою є NGN.

Згідно з визначенням, наведеним у Рекомендації МСЕ-Т Y.2001 [5], мережа наступного покоління (NGN) – це мережа з пакетною комутацією, здатна забезпечити користувачів різноманітними вузькосмуговими та широкосмуговими послугами, включаючи послуги телефонного зв’язку, заснована на широкосмуговій мережі з пакетною технологією транспортування, що забезпечує необхідну якість послуг QoS (Quality of Service), в якій функції пов’язані з наданням послуг, що не залежать від технологій транспортування інформації. Мережа NGN дає користувачам необмежений доступ до різних послуг провайдерів і підтримує узагальнену мобільність, яка дозволяє користувачам отримати доступ до послуг у будь-якому місці і в будь-який час.

NGN передбачає вільний доступ для користувачів за їх вибором до мереж і до конкуруючих постачальників служб та/або до служб/послуг. Вона підтримує узагальнену мобільність, яка буде давати можливість постійного і повсюдного забезпечення служб для користувачів. NGN реалізує принцип глобальної доступності послуги, тобто будь-яка послуга в будь-якому місці будь-яким способом у будь-який час.

Зважаючи на вищенаведене, NGN як доктрина диктує для спільноти необхідність поставити персональний комп’ютер у центр нових технологічних рішень у галузі зв’язку, що, як наслідок, потребує корінної модернізації існуючих мереж та систем зв’язку [4].

Втрачає сенс сам термін “канал зв’язку”, що призводить до втрати підстав для стандартизації каналів первинної мережі, а поняття первинної мережі стає аморфним та невизначеним. Таким чином, на заміну традиційним мережам зв’язку з ієрархічною структурою приходять мережі NGN. З’являються такі поняття, як транспортна мережа та мережа доступу. Це призводить до зменшення формалізації відносин між транспортною мережею та мережею доступу порівняно з відносинами між первинною та вторинною мережею, а отже, стають менш прозоро визначені точки стику (взаємоз’єднання), насамперед між транспортними мережами.

В більшості публікацій з NGN наводиться узагальнена архітектура NGN, в якій виділяються такі чотири рівня:

1. Рівень доступу (Access), що містить мережу абонентського доступу до транспортної пакетної мережі.

2. Транспортний рівень (Transport), що включає магістральну пакетну мережу (мережу, побудовану на базі протоколів пакетної комутації IP або ATM, в даний час найчастіше на базі технології MPLS і протоколу IP).

3. Рівень управління комутацією (Control), включає сукупність функцій з управління всіма процесами обслуговування викликами в телекомунікаційній мережі.

4. Рівень послуг і експлуатаційного управління (Servise), який містить логіку виконання послуг та/або додатків і управляє цими послугами, має відкриті інтерфейси для використання сторонніми організаціями (для розробки програм і нових послуг).

Спрощено чотири рівні NGN представлені на Рис.

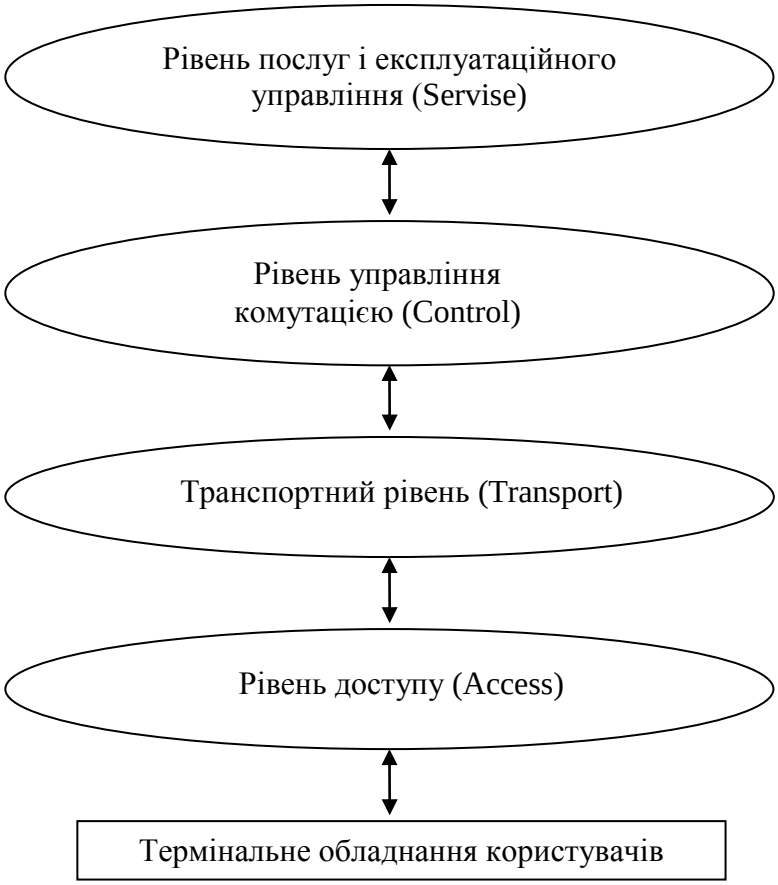


Рис. Рівні технології мереж наступного покоління (NGN).

Виходячи з вищенаведеного та враховуючи, що рекомендаціями МСЕ – Т Y.2091 [6] та МСЭ-Т Y.2111 [7] не встановлені однозначні вимоги щодо взаємодії та взаємоз’єднання мереж, можливе та доцільне їх взаємоз’єднання на рівні управління і комутації шляхом взаємоз’єднання технічного оснащення.

Що ж до нормативного врегулювання при взаємоз’єднанні мереж операторів телекомунікацій при використанні ними технології NGN, то наша держава відрізняється від інших країн досить сильним “телефонним” характером сучасного регулювання у сфері телекомунікацій. В ньому закладено принцип телефонної ієрархії побудови мереж, які є одноранговi за своєю суттю, що не сприяє розвитку IP-технологій та відповідного сервісу.

Потреба бізнесу змушує операторів телекомунікацій розвивати мультисервісні IP-мережі, IP-сервіси та відповідні технології. За таких обставин не зовсім доцільним стає модернізація та розвиток TDM-мереж.

Відповідно до Закону України “Про телекомунікації” (далі – Закон) [8] телекомунікації є невід’ємною частиною виробничої та соціальної інфраструктури України і призначені для задоволення потреб фізичних та юридичних осіб, органів державної влади в телекомунікаційних послугах. Закон визначає, що метою державного регулювання у сфері телекомунікацій є максимальне задоволення попиту споживачів на телекомунікаційні послуги, створення сприятливих організаційних та економічних умов для залучення інвестицій, збільшення обсягів послуг та підвищення їх якості, розвитку та модернізації телекомунікаційних мереж з урахуванням інтересів національної безпеки [6].

На реалізацію зазначеної мети повинні бути направлені зусилля державних органів, і в першу чергу – на створення такої нормативно-правової бази, яка усіляко б сприяла розвитку та модернізації телекомунікаційних мереж.

Створенням міжнародних стандартів NGN займаються ITU-T, ETSI та інші організації. І хоча роботи ведуться вже не перший рік, ця діяльність перебуває на початковому етапі. Перші рекомендації МСЕ з даного питання були опубліковані ще у 2004 році та знайшли свій розвиток у Рекомендаціях МСЕ-Т Y.2091 “Терміни та визначення для мереж наступних поколінь” та МСЕ-Т Y.2111 “Функції управління ресурсами і встановленням з’єднань в мережах наступних поколінь”. Передбачається, що в найближчі роки серія рекомендацій Y.2000 буде поповнюватися, а на ринку з’являться технічні засоби NGN, що відповідають цим рекомендаціям. І хоча нормативна база мереж наступного покоління поки що розвинена слабо, впровадження NGN у всьому світі відбувається повним ходом.

В Україні розробка нормативно-правової бази галузі зв’язку з проблематики NGN проводиться тільки в рамках, визначених рекомендаціями МСЕ. Прийнятих документів, що повною мірою відповідали б зазначеним міжнародним рекомендаціям, поки що недостатньо. До цього часу розвиток законодавчої бази України з питань зв’язку проходив в основному з урахуванням традиційної архітектури мереж. Закон України “Про телекомунікації” та прийняті у 2005 – 2013 роках на його основі підзаконні акти не враховують зміни телекомунікаційного ландшафту, і зокрема процеси конвергенції послуг мереж зв’язку та інформаційних послуг.

Проблеми регулювання ринку NGN в Україні стосуються також аспектів ліцензування операторської діяльності, побудови мереж, приєднання до інших мереж, нумерації, системи оперативно-розшукових заходів. Для подальшого розвитку ринку NGN потрібне коригування багатьох основоположних документів, що регулюють телекомунікаційний ринок України, таких як Закон України “Про телекомунікації”, Правила взаємоз’єднання телекомунікаційних мереж загального користування, Правила надання та отримання телекомунікаційних послуг. Правила доступу до ККЕ, Порядок проведення експертизи при досудовому врегулюванні спору, Порядок взаєморозрахунків між операторами телекомунікацій за послуги доступу до телекомунікаційних мереж загального користування.

Недостатній рівень правового регулювання даного питання є одним із стримуючих факторів розвитку NGN-мереж в Україні.

Наприклад, Закон України “Про телекомунікації” заперечує можливість провайдерів взаємоз’єднувати свої телекомунікаційні мережі, а загальні вимоги до

структури побудови мереж NGN, визначені відповідними міжнародними рекомендаціями, не виключають такої можливості.

У той же час, Правила взаємоз’єднання телекомунікаційних мереж загального користування передбачають для операторів можливість взаємоз’єднувати свої телекомунікаційні мережі незалежно від технологій, які застосовуються для передавання інформації, проте тільки для мереж, що функціонують у складі ТМЗК.

Також, Правилами встановлено, що вимоги до порядку взаємоз’єднання мереж, які функціонують у складі ТМЗК за різними технологіями, установлюються відповідно до законодавства.

Водночас, чинним Законом України “Про телекомунікації” та відповідними нормативно-правовими актами технічні вимоги до взаємоз’єднання визначені нечітко та неоднозначно, що призводить до довільного тлумачення їх операторами і непорозумінь, які виникають при взаємоз’єднанні телекомунікаційних мереж.

У результаті оператори “ходять під дамокловим мечем”. З одного боку, вони змушені відповідати на дії конкурентів та потреби ринку, з іншого –виконувати нечітко та неоднозначно визначені вимоги нормативно-правових актів.

Спираючись на досвід роботи регуляторних органів країн ЄС, регулятор повинен забезпечувати і в першу чергу вирішувати завдання, пов’язані із:

1. Захистом прав абонента (користувача) з метою забезпечення вимог до якості телекомунікаційних послуг та доступних за ціною сервісів, які надає оператор, провайдер телекомунікацій.

2. Захистом прав інвестора з метою організації захисту від неринкових та антиконкурентних дій, що призводять до непередбачуваності при взаємоз’єднанні мереж, використанні номерного ресурсу та не виключають можливості реалізації політики фінансового протекціонізму при формуванні тарифних планів, зведення адміністративних і ринкових бар’єрів у процесах видачі і переоформлення ліцензій.

3. Формуванням середовища економічної ефективності для учасників ринку, за якого ймовірність об’єктивних факторів що сприяють виникненню ситуацій неокупності витрат, виключається.

4. Захистом конкуренції при взаємодії операторів, провайдерів телекомунікацій при наданні послуг абонентам.

Висновки.

Враховуючи вищезазначене, позиція держави має бути такою, щоб навіть за відсутності міжнародного законодавства удосконалювати національну законодавчу базу, що створить сприятливі умови для задоволення потреб споживачів у телекомунікаційних послугах.

Відповідь на запитання, що потрібно зробити для забезпечення окреслених задач може бути такою:

внести зміни до Закону України “Про телекомунікації”, які сприяли б створенню відповідної нормативної бази для реалізації технології NGN, передусім у частині, що стосується взаємоз’єднання телекомунікаційних мереж;

створити нормативну базу для опису спільного технологічного використання IP- та TDM-технологій;

визначити підходи для встановлення ставок інтерконтенту між двома операторами, які використовують різні технології, що забезпечують перехід від TDM-мереж до IP-мереж.

Зазначені заходи сприятимуть реалізації технології NGN, що призведе до підвищення рівня якості сучасних телекомунікаційних послуг та задоволення потреб споживачів у нових та якісних телекомунікаційних послугах.

Використана література

1. Братіца М.С., Сандул В.С. Про заходи забезпечення якості телекомунікаційних послуг // Інформація і право. – № 2(5)2012. – С. 146-153.

2. Сандул В.С. До питання удосконалення державного регулювання у сфері телекомунікацій // Правова інформатика. – № 4(28) 2010. – С. 30-33.

3. Концепція розвитку телекомунікацій в Україні : Розпорядження Кабінету Міністрів України від 07.06.06 р. № 316-р. – Режим доступу : //www.kmu.gov.ua

4. Бакланов И.Г. Б19 NGN : принципы построения и организации / И.Г. Бакланов ; под. ред. Ю.Н. Чернышова. – К. : Эко-Трейд, 2008.

5. Рекомендації МСЕ-Т Y.2001. “Загальні принципи та загальна еталонна модель мереж наступного покоління”. – Сектор стандартизації МСЕ. – Режим доступу : //www.itu.int/ITU-T/ipr

6. Рекомендації МСЕ-Т Y.2091. “Терміни та визначення для мереж наступних поколінь”. – Сектор стандартизації МСЕ. – Режим доступу : //www.itu.int/ITU-T/ipr

7. Рекомендація МСЕ-Т Y.2111. “Функції управління ресурсами і встановленням з’єднань в мережах наступних поколінь”. – Сектор стандартизації МСЕ. – Режим доступу : //www.itu.int/ITU-T/ipr

8. Про телекомунікації : Закон України від 18.11.03 р. № 1280-IV. – Режим доступу : //www.rada.gov.ua

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 004.67+519.83

ЛАНДЕ Д.В., *доктор технічних наук, старший науковий співробітник*

ЖИТТЄВИЙ ЦИКЛ ІНФОРМАЦІЙНИХ ОБ’ЄКТІВ

Анотація. *Інформаційна компонента інформаційно-аналітичної системи – це змістовна складова її інформаційного забезпечення, сукупність інформаційних об’єктів. У статті наведено опис моделей життєвого циклу інформаційних об’єктів, основні методи підвищення живучості інформаційної складової інформаційно-аналітичних систем. Ці методи спрямовані на зменшення рівня вразливості інформаційних об’єктів у межах інформаційної інфраструктури.*

Ключові слова: *інформаційна складова, життєвий цикл, живучість, інформаційний об’єкт, інформаційні потоки, математичне моделювання.*

Аннотация. *Информационная компонента информационно-аналитической системы – это содержательная составляющая ее информационного обеспечения, совокупность информационных объектов. В статье приведено описание моделей жизненного цикла информационных объектов, основные методы повышения живучести информационной составляющей информационно-аналитических систем. Эти методы направлены на уменьшение уровня уязвимости информационных объектов в пределах информационной инфраструктуры.*

Ключевые слова: *информационная составляющая, жизненный цикл, живучесть, информационный объект, информационные потоки, математическое моделирование.*

Summary*. Information component of information-analytical system is a meaningful component of its information security, a set of information objects. The paper describes the model of the life cycle of information objects, the main methods to improve the survivability of the information component of information-analytical systems. These techniques are aimed at reducing the vulnerability of the information objects within the information infrastructure.*

Keywords: *information component, life cycle, survivability, information object, information flows, mathematical modeling.*

Постановка проблеми. Сучасний інформаційний простір є динамічною документальною системою, що складається з пов’язаних за змістом елементів – інформаційних об’єктів, які утворюють в динаміці своєї еволюції інформаційні потоки [1].

На цей час у зв’язку з розвитком інформаційних технологій особливе місце серед завдань, що отримали актуальність, займають завдання, пов’язані з моделюванням їх життєвого циклу, а саме – окремих етапів:

- генерування інформації (формування і развитку);
- передачі інформації;
- формування сховища інформаційних ресурсів (баз даних, інформаційних масивів, окремих документів тощо);
- безпосереднього використання інформаційної складової;
- реакції на деструктивні впливи, відновлення, руйнування;
- утилізації (архівування) інформації.

Питання життєвого циклу інформаційних об’єктів знаходить широке відображення у законодавчих актах України. Зокрема, у Законі України “Про інформацію” від 02.10.92 р. № 2657-XII (ч.1 ст. 3) регламентуються інформаційні відносини на всіх етапах життєвого циклу інформаційних об’єктів, зокрема “створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації”.

Закон України “Про захист персональних даних” від 01.06.10 р. № 2297-VI “регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних” (ст. 1).

Закон України “Про науково-технічну інформацію” від 25.06.93 р. № 3322-XII “порядок формування і реалізації” науково-технічної інформації в інтересах науково-технічного, економічного і соціального прогресу країни. Це далеко не повний перелік законодавчих актів у інформаційній сфері щодо означених питань.

Виклад основних положень. Основним об’єктом моделювання інформаційних потоків [2] сьогодні є їх тематичні зрізи, послідовності документів, що відповідають певній тематиці. Тематичним інформаційним потокам можна поставити у відповідність часові ряди, для вирішення завдань аналізу яких все частіше застосовуються статистичний, дисперсійний, фрактальний, Фурье і вейвлет-аналіз [3].

Динаміка тематичних інформаційних потоків визначається комплексом як внутрішніх, так і зовнішніх нелінійних механізмів, що мають враховуватися при моделюванні (можливо, у неявному вигляді). Досить часто задовільним виявляється спрощене розуміння тематичного інформаційного сюжету як деякої залежної від часу величини $n(t)$, поведінка якої описується нелінійними рівняннями. Сьогодні при моделюванні інформаційних потоків використовуються переважно нелінійні моделі, застосовуються методи нелінійної динаміки, теорії клітинних автоматів, перколяції, самоорганізованої критичності [1, 4].

Багато сучасних інформаційно-аналітичних систем містять у своєму складі засоби відображення статистики входження в бази понять, відповідних запитам користувачів. Зокрема, у рамках цих досліджень використовувалася система контент-мониторинга веб-простору InfoStream (//www.infostream.ua), що має цю функціональність.

Моделювання інформаційних потоків.

Для вивчення інформаційних сюжетів як складних багатопараметричних систем, параметри яких ще мало вивчені, найбільш відповідною методикою є математичне моделювання. Життєвий цикл інформаційних об’єктів при цьому може описуватися, наприклад, моделлю дифузії інформації [5]. Процеси дифузії інформації, як і процеси дифузії, у фізиці досить точно моделюються за допомогою методів клітинних автоматів. Модель дифузії інформації, яку розглядатимемо надалі, є двовимірною.

У системі клітинних автоматів найближчими сусідами, що входять до околу елемента $y_{i,j}$, вважаються елементи, розташовані поряд з ним (так званий окіл Мура – кожна клітина має вісім сусідів). Значення клітини на кроці еволюції $t + 1$ в порівнянні з кроком t має вигляд:

$$y_{i,j}(t+1) = F(y_{i-1,j-1}(t), y_{i-1,j}(t), y_{i-1,j+1}(t), y_{i,j-1}(t), y_{i,j}(t), y_{i,j+1}(t), y_{i+1,j-1}(t), y_{i+1,j}(t), y_{i+1,j+1}(t)).$$

У рамках цієї моделі поширення новин в інформаційному просторі, застосовуються окіл Мура й імовірнісні правила поширення новин за заданою тематикою. Передбачається, що клітина може перебувати в одному з трьох станів: 1 – “свіжа новина” (клітина забарвлюється у чорний колір); 2 – новина застаріла, але збережена у вигляді відомостей (сіра клітина); 3 – клітина не має інформації (клітина біла, інформація не дійшла або забута). Правила розвитку інформаційного сюжету наступні:

– спочатку усе поле складається з білих клітин за винятком однієї – чорної, яка першою “прийняла” новину;

– біла клітина може перефарбовуватися тільки в чорний колір або залишатися білою (вона може отримувати новину або залишатися такою, якою була);

– біла клітина перефарбовується, якщо виконується умова: $Cpm > 1$, де: p – псевдовипадкова величина ($0 < p < 1$), m – кількість чорних кліток в околі, C – константа ($C = 1{,}5$ при $m = 1$; $C = 1$ при $m \neq 1$);

– якщо клітина чорна, а навколо неї виключно чорні і сірі, то вона перефарбовується в сірий колір (новина застаріває, але зберігається як відомість);

– якщо клітина сіра, а навколо неї виключно сірі і чорні, то вона перефарбовується в білий колір (забування інформації при її загальновідомості).

Описана система клітинних автоматів цілком реалістично відбиває процес розвитку інформаційного сюжету (Рис. 1). Типові залежності кількості клітин (послідовності кількості однотипних клітин), що перебувають в різних станах, в залежності від кроку еволюції наведені на Рис. 2.

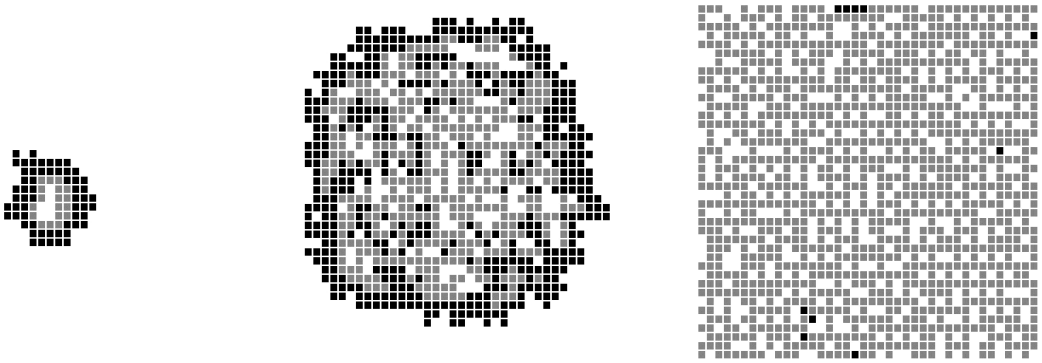


Рис. 1 – Стан еволюції системи клітинних автоматів.

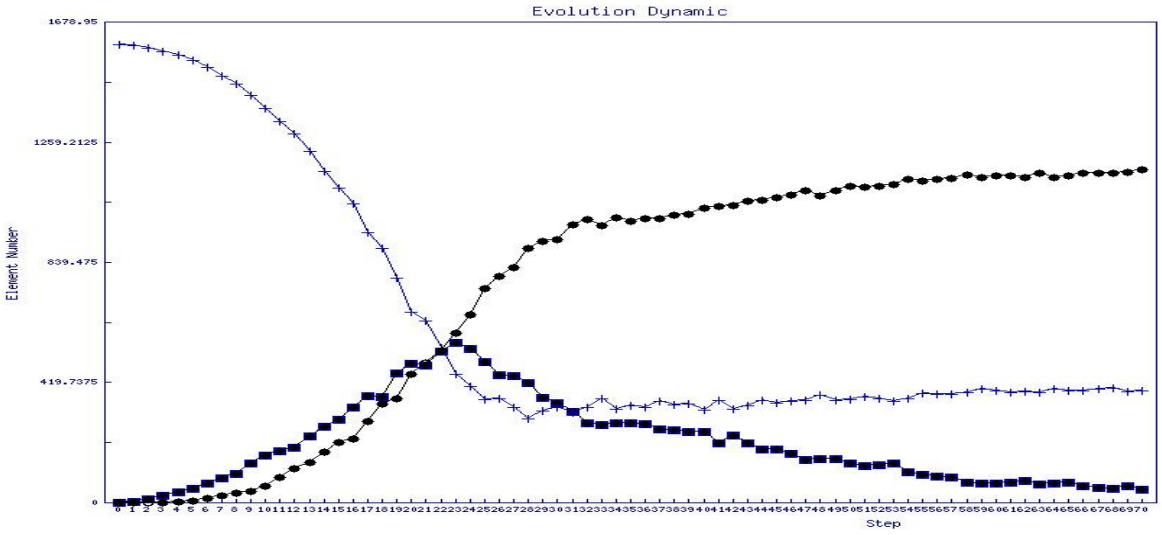


Рис. 2 – Розподіл клітин залежно від номера такту системи клітинних автоматів:
білі клітини – (+); сірі клітини – (•); чорні клітини – (■).

При аналізі наведених графіків можна звернути увагу на такі особливості: 1 –сумарна кількість клітин, що перебувають в усіх трьох станах на кожному кроці ітерації постійна і дорівнює розміру поля; 2 – при стабілізації клітинних автоматів співвідношення кількості сірих, білих і чорних клітин приблизно становить: 0,75: 0,25: 0. Саме чорні клітини утворюють актуальний інформаційний сюжет, динаміка якого представлена на Рис. 1.

Цілком реалістичні профілі динаміки тематичних інформаційних потоків також були досягнуті за допомогою мультиагентної моделі [2]. У рамках цієї моделі окремі документи асоціюються з агентами, життєвий цикл агентів – з життєвим циклом документів в інформаційному просторі. Відповідно, простір агентів асоціювався з тематичним інформаційним потоком.

Передбачається, що протягом дискретних моментів часу відбувається еволюція популяції агентів. При цьому окремі агенти можуть:

1) самозароджуватися (народжуватися з причин, що виникають поза мультиагентного простору);

2) породжувати нових агентів;

3) “гинути” – зникати з простору агентів;

4) отримувати посилання від інших агентів.

Кожен агент має “потенціал”, що залежить від його віку (часу життя на даний момент), авторитетності (посилань, проставлених на нього) і плодючості (кількості породжених безпосередньо ним агентів).

Управляючі параметри моделі наступні:

1) ймовірність “самозародження” P_1;

2) потенціал агента Pot, що залежить від кількості посилань на нього (ns), часу його життя (t) і кількості породжених ним агентів (k): $Pot = \frac{ns + k}{t}$;

3) ймовірність “народження” від існуючого: $P_2 \cdot Pot$;

4) ймовірність “загибелі” агента: P_3 / Pot;

5) ймовірність посилання на агента: $P_4 \cdot Pot$.

Варіювання параметрами управління P_1, P_2, P_3 і P_4 дозволили змоделювати наведені на Рис. 2 профілі поведінки тематичними інформаційними потоками.

На Рис. 3 наведено приклад можливої динаміки мультиагентної системи: процеси народження нових агентів від існуючих позначені суцільними стрілками, процеси проставляння посилань на агентів представлені пунктирними стрілками, живі агенти – чорними кругами, “мертві” агенти до моменту $t = 5$ – незаповненими колами.

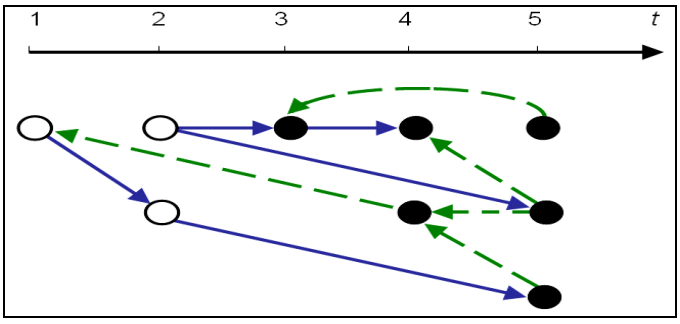


Рис. 3 – Фрагмент мультиагентного простору.

Слід зазначити, що дана модель не бере до уваги:

1) конкуренції агентів усередині агентного простору (передбачається тільки співпраця шляхом проставляння посилань і породження нових агентів);

2) конкуренції різних тематичних інформаційних потоків (враховується лише неявно, як причина, що обумовлює параметри функціонування даної мультиагентної системи).

Також слід зазначити, у запропонованій моделі враховується загальновідома практика проведення інформаційних кампаній в соціальних мережах, що полягає в реєстрації великого числа акаунтів-роботів (роїв), від імені яких проставляються посилання (лайки) на матеріали, що публікуються від імені акаунтів з того ж рою і на цільові інформаційні сторінки – документи.

В результаті проведених досліджень була реалізована програма еволюції простору агентів, досліджена еволюція мультиагентної системи при різних значеннях параметрів, знайдені аналогії з реальними тематичними інформаційними потоками, динаміка яких була визначена за допомогою системи InfoStream.

У разі інформаційних потоків, які асоціюються з конкретними тематичними інформаційними потоками, необхідно описувати динаміку кожного з таких потоків окремо, зважаючи на те, що зростання одного з них автоматично приводить до зменшення інших і навпаки. Тому обмеження на кількість повідомлень за усіма тематиками поширюється і на сукупність усіх тематичних сюжетів новин. У разі вивчення загального інформаційного потоку спостерігається явище “перетікання” публікацій з одних тематичних сюжетів, що втрачають актуальність, до інших.

Зазначимо, що запропонована модель дозволяє відрізняти інформаційні потоки, поведінка яких визначається природними закономірностями медійного простору, від потоків, висвітлення яких у медійних засобах має вплив зовнішніх чинників. Зокрема, таким індикатором може бути відхилення від характерних форм розподілу, поява періодичних зон нестабільності значень, відповідних динаміці тематичних інформаційних потоків, або, навпаки, суттєва локальна стабільність цих значень.

Як приклад, на Рис. 4 наведено динаміку публікацій в RUNet тематичних інформаційних потоків за запитами: “Банки Кипра”, “Офшор”, “Вирджинские острова” за березень-квітень 2013 року в період відомих кризових подій, яку отримано за допомогою системи InfoStream [6].

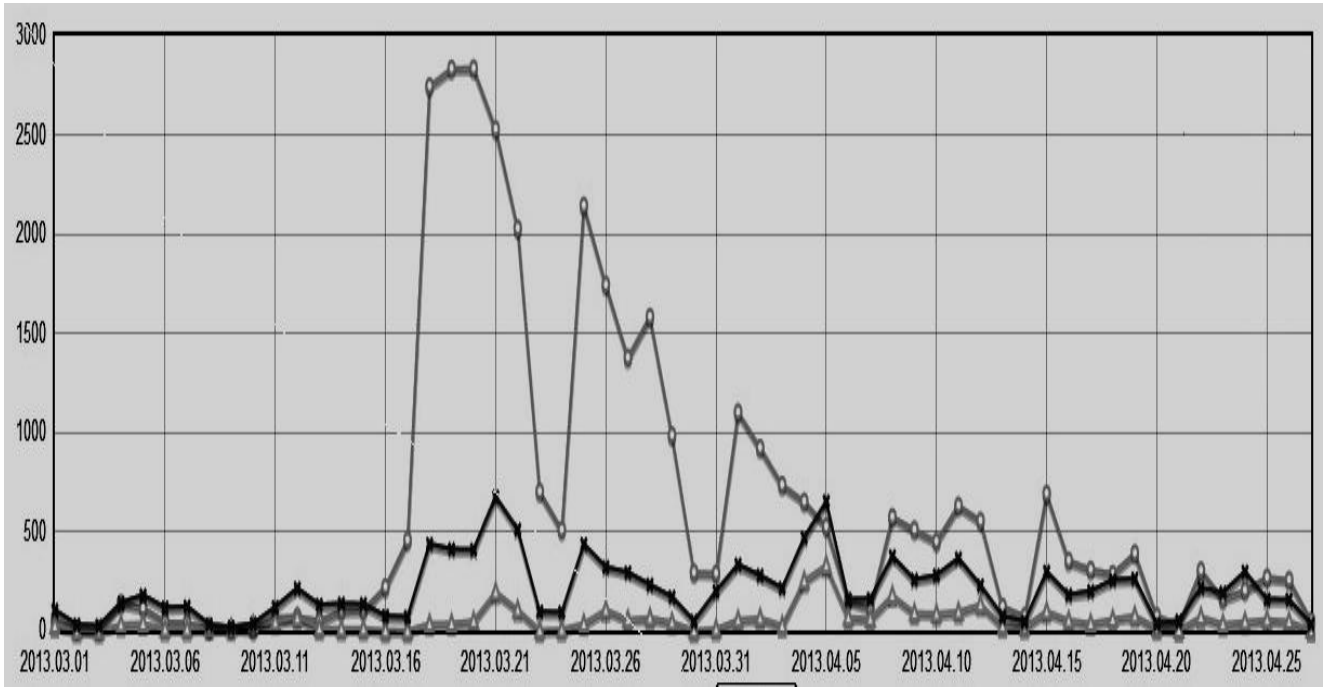
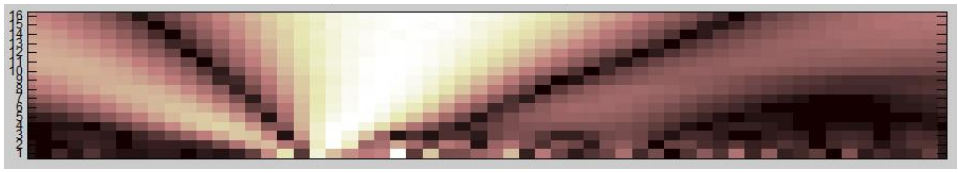


Рис. 4 – Діаграма динаміки тематичних інформаційних потоків за запитами:
o – “Банки Кипра”; Δ – “Вирджинские острова”; x – “Офшор”.

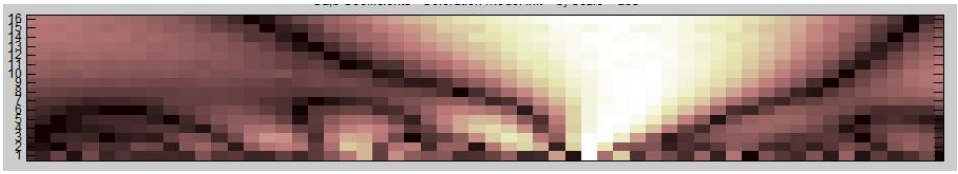
Як видно з Рис. 4, пік публікацій, пов’язаних з банківською кризою на Кіпрі припадає на 17 – 18 березня 2013 року, в той час, як більшість публікацій по островах Вірджинії з’явилися 4 – 5 квітня, коли там у значно менших масштабах, стали відбуватися події, подібні до кіпрських. При цьому слід зазначити слабку взаємну кореляцію динаміки інформаційних потоків, пов’язаних з Кіпром і островами Вірджинії. В цьому випадку коефіцієнт взаємної кореляції відповідних числових рядів становив всього 0,3. При цьому відзначається високий рівень взаємної кореляції рядів, відповідних тематикам “Офшор” і “Банки Кипра” (0,73), а також “Офшор” і “Вирджинские острова” (0,77).

Мабуть, прояви інформаційних операцій в області офшорних банків у даному випадку краще за все побачити при аналізі загальнішої тематики – “Офшори”. На графіці відповідного числового ряду чітко видно дві області локальних екстремумів, відповідних кризовим ситуаціям на Кіпрі і на островах Вірджинії. Можна зробити припущення, що якщо динаміка часткового інформаційного потоку в якийсь момент починає істотно відрізнятися від динаміки потоку, відповідного загальнішій тематиці (як в даному випадку – “Банки Кіпру” і “Офшор”), то можливий прояв ознак початку інформаційної операції, що відноситься до вузької тематики.

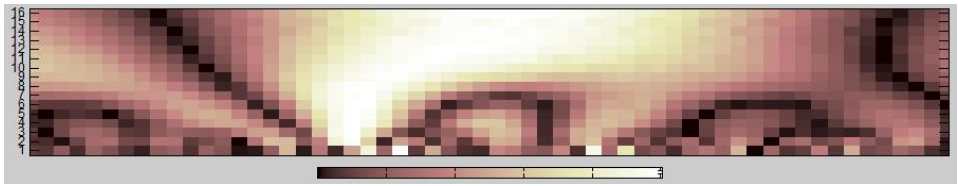
При проведенні вейвлет-аналізу (Рис. 5) було прийнято рішення щодо використання вейвлету “Мексиканський капелюх” як найбільш близького за формою до діаграми, відповідної тренду інформаційних операцій [6].



а) “Банки Кипра”



б) “Вирджинские острова”



г) “Офшор”

Рис. 5 – Вейвлет-спектограми, що відповідають динаміці тематичних інформаційних потоків за запитами.

Дані процеси є чітко видимими як на вейвлет-спектограмах, так і на відповідних їм скелетонах (графіках ліній екстремумів).

Живучість інформаційних об’єктів.

Поняття живучості інформаційної складової мережі Інтернет може розглядатися як здатність інформаційних об’єктів (новинних повідомлень, статей, документів, відеороликів і т. д.) своєчасно виконувати свої функції інформування в умовах дії

дестабілізуючих чинників. Такими чинниками можуть бути усунення окремих об’єктів з інформаційного простору, втрата інформаційними об’єктами властивостей актуальності, доступності [7, 8].

Оцінка живучості інформаційних об’єктів може проводитися на усіх етапах їх життєвого циклу. Існує декілька підходів до проведення оцінки живучості, що мають найбільш загальний характер. Живучість можна оцінити стосовно деякої стандартної зовнішньої дії або щодо множини зовнішніх дій. У цьому випадку вирішується завдання знаходження множини характеристичних векторів станів інформаційного об’єкта (у простому випадку – розподіл даних по серверах), в яких реалізується конфігурація, що забезпечує виконання мети функціонування. Потужність цієї великої кількості може служити мірою живучості усього інформаційного об’єкта.

При аналізі живучості інформаційних об’єктів виникає проблема інформування за різними аспектами незалежно від наявності або відсутності несприятливих чинників. У зв’язку з цим як кількісний критерій оцінки живучості доцільно використовувати відношення кількості функцій, що виконуються об’єктом за наявності певних несприятливих дій або множини таких дій, до загальної кількості функцій інформаційного об’єкта, з урахуванням критичності виконуваних і невиконуваних функцій. Критичність кожної конкретної функції визначається індивідуально для кожного конкретного інформаційного об’єкта виходячи з його специфіки. Кількісний показник живучості конкретного інформаційного об’єкта в заданих умовах можна обчислювати за формулою:

$$S = \sum_{i \in \Delta} \alpha_i \,/\, \sum_{j \in \Theta} \alpha_j ,$$

де: Θ – множина всіх функцій інформування, Δ – множина функцій інформаційного об’єкта, що виконуються при заданих умовах $(\Delta \subseteq \Theta)$, α_n – критичність *n*-ої функції.

Таким чином, кількісна оцінка живучості інформаційного об’єкта буде вимірюватися в інтервалі [0, 1], живучість тим вище, чим більша її кількісна оцінка.

Методи підвищення живучості інформаційної складової спрямовані на зменшення рівня її вразливості в мережах і системах інформаційної інфраструктури. Поняття живучості включає поняття надійності, безпеки, відмовостійкості тощо. Тому, зокрема, методи забезпечення живучості інформаційно-аналітичних систем (далі – ІАС) включають до свого складу також методи забезпечення цих характеристик, але не обмежуються ними. Нижче наведено основні методи, які застосовуються для підвищення живучості інформаційної складової [9]:

1. Регулярна перебудова метаданих та індексів інформаційних ресурсів ІАС. У системі організації інформаційних ресурсів одним з ключових чинників є метадані (класифікації, переліки об’єктів, термінологічні словники, тезауруси, уніфіковані форми представлення даних, стандарти, патенти й інші форми нормативних і правових документів).

2. Багатократне дублювання даних (реалізація надмірності даних). Надмірність вводиться штучно при проектуванні баз даних у цілях підвищення надійності системи в умовах роботи із збоями. При цьому передбачається регулярне здійснення реплікації дублюючих блоків інформації з перевіркою ідентичності.

3. Реалізація резервного та архівного копіювання інформаційних ресурсів ІАС.

4. Застосування децентралізованих систем зберігання інформації разом із дублюванням критичних блоків інформації.

5. Резервне дублювання не тільки інформації, а й цілих апаратно-програмних комплексів.

6. Застосування сертифікованого антивірусного захисту.

7. Застосування засобів електронного цифрового підпису, хешування даних (як засіб проти спотворення даних).

8. Постійна перевірка валідності джерел інформації.

9. Видалення (архівування) зайвої, непотрібної інформації, інформаційного шуму.

10. При здійсненні процедур обробки даних з можливою втратою інформації (автоматичне реферування, переклад, JPEG-перетворення зображень) необхідно зберігати першоджерела документів в інформаційному сховищі (депозитарії).

11. Забезпечення доступу аналітиків (аналітичних програмних модулів) до будь-якого фрагмента інформаційного репозитарію ІАС з метою оперативного виявлення впливу на інформаційну складову, здійснення регулярного цілеспрямованого аналізу, контролю і коригування стану програмного та інформаційного забезпечення.

12. Ранжирування інформації. Інформація, що зберігається в ІАС, має бути ранжирувана за ступенем важливості, рівнем конфіденційності та належністю відповідним підрозділам.

13. Розподіл прав доступу до інформації. Реалізація визнаних політик безпеки.

14. Фільтрація вихідної інформації, яка поступає з ІАС безпосередньо для прийняття рішень, шляхом цензурування з метою відсіювання несприятливої для зовнішнього світу інформації.

15. Розподіл частин ІАС (“відкритої”, корпоративної тощо) можливо реалізувати на різних рівнях (паролі, файрволи, фізичне роз’єднання).

16. Обмеження доступу до інформації. Цей метод припускає наявність розвиненого периметра безпеки, що має як централізоване, так і децентралізоване керування, який був би в змозі оцінювати вхідну інформацію (“службову” і “корисну”), і виключати інформацію небезпечного змісту.

17. Протоколювання подій в системі, ведення системних журналів з метою виявлення можливих фрагментів даних, які зазнали втручання.

18. Забезпечення працездатності апаратних засобів, коректне відключення носіїв даних при зупинці системи, окремих блоків і модулів.

19. Зберігання в системі різних версій програм обробки/візуалізації, що допоможе уникнути помилок при реалізації принципу “наслідування”.

20. Наявність конверторів форматів даних і підсистем інтеграції ПЗ (підсистеми імпорту, експорту і синхронізації даних між різними додатками) для забезпечення використання вихідних даних у різних форматах.

21. Застосування засобів термінового зберігання критично важливих документів, доступних у режимі “тільки читання”. Резервне зберігання інформації на знімних носіях, розміщення в захищених приміщеннях. Задовольнити нові вимоги можна, використовуючи декілька підходів.

22. Зберігання історії (версій) інформаційних документів. Майже всі сучасні документальні сховища підтримують версіонність інформаційних документів.

23. Використання надійних каналів передачі вхідних даних. Безпека має забезпечуватися шифруванням трафіку між серверами додатків і клієнтами. Використання декількох каналів інформації з подальшим порівнянням при занесенні в інформаційне сховище (реплікації).

24. Застосування систем виявлення зовнішнього впливу (вторгнення), за допомогою яких можна зафіксувати факт атак на інформаційну інфраструктуру, оцінити

можливі збитки і виконати адекватні дії у відповідь. При цьому зовнішні впливи на інформаційну складову нині прийнято вважати інформаційними операціями [6], відповідно для забезпечення її живучості необхідно застосовувати методи моніторингу і протидії інформаційним операціям.

Висновки.

Забезпечення живучості аналітичної складової охоплює усі ланки життєвого циклу інформаційних об’єктів, а саме:

- отримання аналітиками вихідної інформації;
- аналіз інформації за визначеною проблемою, що зібрана;
- обробка інформації;
- підготовка документів (інформаційних об’єктів);
- верифікація інформаційних об’єктів;
- використання інформаційних об’єктів.

Наведені вище моделі і методи придатні для опису загальних тенденцій динаміки розвитку інформаційних процесів, однак проблема прогнозування залишається відкритою. Мабуть, більш реалістичні моделі можуть бути отримані з урахуванням додаткового набору чинників, більшість яких не відтворюються в часі.

Використана література

1. Ланде Д.В. Інформаційні потоки в глобальних комп’ютерних мережах / О.Г. Додонов, Д.В. Ланде, В.Г. Путятін. – К : Наукова думка, 2009, – 295 с.

2. Додонов А.Г., Ландэ Д.В. Мультиагентная модель поведения тематических информационных потоков : *материалы VI Всероссийской мультиконференции по проблемам управления (30 сентября – 5 октября 2013 г).* – Том. 4. – Ростов-на-Дону : Издательство Южного федерального университета, 2013. – С. 102-107.

3. Ланде Д.В. Основи інформаційного і соціально-правового моделювання : монографія / Д.В. Ланде, В.М. Фурашев. – К. : ТОВ “ПанТот”, 2012. – 144 с.

4. Ландэ Д.В. Интернетика : Навигация в сложных сетях : модели и алгоритмы / Д.В. Ландэ , А.А. Снарский , И.В. Безсуднов . – М. : Либроком (Editorial URSS), 2009. – 264 с.

5. Ландэ Д.В. Модель диффузии информации / Д.В. Ландэ : *сб. науч. тр. Ин-та проблем регистрации информации НАН Украины [Информационные технологии и безопасность. Менеджмент информационной безопасности]*. – 2007. – Вып. 10. – С. 51-67.

6. Додонов А.Г., Ландэ Д.В. Динамика информационных потоков при выявлении информационных операций : *материалы XIII Международной научно-практической конференции [“Информационная безопасность”]*. – Ч. 1. – Таганрог : Изд-во ТТИ ЮФИ, 2013. – С. 42-49.

7. Ландэ Д.В. Живучесть информационных систем / А.Г. Додонов, Д.В. Ландэ. – К. : Наук. думка, 2011. – 256 с.

8. Knight J.C., Strunk E.A., Sullivan K.J. Towards a Rigorous Definition of Information System Survivability // Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX’03), 2003.

9. Додонов О.Г., Ланде Д.В. Методи підвищення живучості інформаційної складової корпоративних інформаційно-аналітичних систем підтримки прийняття рішень // Реєстрація, зберігання і обробка даних. – 2012. – № 2-14. – С. 48-58.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 004.67

БЕРЕЗІН Б.О., науковий співробітник,
Інститут проблем реєстрації інформації НАН України

ДОВГОТЕРМІНОВЕ ЗБЕРІГАННЯ ПРАВОВОЇ ІНФОРМАЦІЇ

Анотація. *Розглядаються особливості довготермінового зберігання правової інформації. Запропановано моделі загроз, негативних впливів при довготерміновому зберіганні. На основі моделей розробляються методи планування зберігання, які забезпечують живучість інформаційних об’єктів.*

Ключові слова: *правова інформація, довготермінове зберігання, моделі загроз, планування зберігання, живучість інформаційних об’єктів, ступеневий розподіл.*

Аннотация. *Рассматриваются особенности долговременного хранения правовой информации. Предложены модели угроз, неблагоприятных воздействий при долговременном хранении. На основе моделей разрабатываются методы планирования хранения, которые обеспечивают живучесть информационных объектов.*

Ключевые слова: *правовая информация, долговременное хранение, модели угроз, планирование хранения, живучесть информационных объектов, степенное распределение.*

Summary. *The features of digital preservation of legal information are analyzed. The models of the threats and adverse effects during digital preservation are proposed. On the basis of models author develops methods for preservation planning provide survivability of information objects.*

Keywords*: legal information, digital preservation, the threat model, preservation planning, survivability of information objects, power-law distribution.*

Постановка проблеми та аналіз публікацій. За даними IDC, обсяги інформації, що створювались у світі за останні роки, становили у 2010 р. – 1,15 зеттабайт, а у 2012 р. вже 2,8 зеттабайт. Зростання загального обсягу інформації, що зберігається, веде до зростання обсягів даних, які повинні зберігатися довготерміново. Одна з перших у світі довідково-правових систем Lexis почала розроблятися наприкінці 60-х років минулого сторіччя в США. Зараз це одна з найбільших у світі баз даних правової інформації LexisNexis, яка надає доступ до мільярдів документів з більш як 45 тис. правових, новинних та бізнес-джерел. LexisNexis охоплює публікації з правової інформації починаючи з XIX сторіччя у США, Великобританії, Канаді та інших країнах [1]. До числа найбільших баз даних правової інформації також відносять Westlaw, яка об’єднує більше ніж 40 тис. баз даних, та HeinOnline, особливістю якої є представлення документів тільки у вигляді PDF-файлів, відсканованих з першоджерел.

Все частіше в США уряди штатів публікують закони, положення про органи та установи, нормативно-правові акти органів виконавчої влади та судові накази і рішення в Інтернеті. У деяких штатах важливі правові матеріали рівня штату більше не публікуються в друкованому вигляді і доступні тільки в глобальній мережі. Для регламентації процедур забезпечення автентичності, довготермінового зберігання та доступності матеріалів через п’ятдесят, сто років штатами приймається “Типовий закон про правові акти, що публікуються в електронному вигляді” (“Uniform Electronic Legal Material Act” – UELMA) [2]. Якщо штат зберігає правові матеріали в електронному вигляді, він повинен забезпечити їх резервне копіювання і відновлення, а також цілісність матеріалів та їх постійну придатність до використання. UELMA не вимагає застосування будь-яких технологій, залишаючи вибір технологій для аутентифікації і

забезпечення збереження на розсуд штатів. Гнучкість закону, який дозволяє штатам вибрати будь-яку технологію, що забезпечує отримання встановлених кінцевих результатів, дає кожному штату можливість підібрати для себе найкращий і найбільш економічноефективний метод. Крім того, такий гнучкий і орієнтований на кінцевий результат підхід враховує те, що технології будуть з часом змінюватися; ні в який момент часу закон не “прив’язує” штат до якоїсь конкретної технології.

Один з напрямів довготермінового зберігання правової інформації пов’язаний з забезпеченням постійного доступу до інформації, що створюється тільки в цифровому вигляді (без друкованої копії) [3 – 5]. В роботі [3] наголошується на високому ризику втрати правової інформації, що створюється у вигляді веб-сторінок (публікації в електронних журналах, на блогах тощо). Це пов’язано з тим, що більшість проектів зберігання інформації спрямовано на оцифрування друкованих документів. Представлено проект Chesapeake Prtoject, запроваджений кількома правовими бібліотеками США для збору та зберігання правової інформації, доступної на веб-ресурсах, з метою включення її до національних програм зберігання.

Робота [4] присвячена дослідженням стабільності URL – тобто доступності посилань на веб-ресурси з правової інформації з плином часу. В одному з цих досліджень для набору з близько 600 веб-ресурсів (відібраних з метою довготермінового зберігання в рамках Chesapeake Prtoject) аналізувалась доступність відповідних URL-посилань в Інтернеті. В результаті виявилось, що протягом першого року стали недоступними більш як 8 % URL, за другий рік кількість недоступних URL зросла до більш як 14 %, на третьому році недоступних посилань стало блізько 28 %. Таке зростання кількості недоступних URL підтверджує ризики втрати правової інформації, що створюється у вигляді веб-сторінок.

В роботі [5] розглядається заява ряду правових бібліотек про відкритий доступ до цифрових матеріалів правової освіти та припинення публікації правових видань у друкованому вигляді. Для забезпечення довготермінового доступу запропоновано оцінити слідуючи альтернативні рішення: архів правової інформації, заснований у 2010 р.; зберігання правового контенту в базах HeinOnline, LexisNexis та Westlaw; використання програмного забезпечення електронних архівів, таких як Portico та LOCCKS; використання можливостей Бібліотеки Конгресу США, яка вже приймає копії усіх правових журналів у друкованому або електронному форматі; створення інституаційних репозитарієв.

Таким чином, проведений аналіз показує актуальність рішень для забезпечення довготермінового зберігання правової інформації та її доступності, а також зменшення витрат. Світові тенденції останніх років полягають у тому, що для вирішення цієї проблеми і зменшення витрат на зберігання недостатньо розвитку традиційного апаратного і програмного забезпечення. Необхідно створення нових засобів – математичних моделей зберігання і побудованих на їх основі інструментальних засобів, програмних пакетів для вибору стратегій, правил для планування та оптимізації процесу зберігання.

Ця тенденція проявилася ще в моделі відкритої архівної інформаційної системи, рекомендованої міжнародним стандартом (Reference Model for an Open Archival Information System – OAIS). Відповідно до моделі при довготерміновому зберіганні даних необхідно враховувати вплив зміни технологій, підтримку нових видів носіїв та форматів, зміну спільнот користувачів тощо. Стандарт забезпечує основу для порівняння різних стратегій та технологій довготермінового зберігання. Серед функцій OAIS передбачається функція планування зберігання, яка забезпечує моніторинг середовища архівного зберігання, рекомендації та плани зберігання для гарантії того,

щоб інформація, яка зберігається в OAIS, залишалася доступною та зрозумілою для користувачів у довготерміновій перспективі, навіть якщо обчислювальне середовище застаріє. Функції планування зберігання включають оцінку контенту архіву та періодичні рекомендації щодо оновлення архівної інформації, рекомендації по міграції поточних запасів архіву, розробку рекомендацій стосовно архівних стандартів та політиків, забезпечення періодичних звітів з аналізу ризиків та моніторингу змін в технологічному середовищі та вимог до обслуговування користувачів.

Метою статті є дослідження загроз, негативних впливів на живучість інформаційних об’єктів при довготерміновому зберіганні для розробки методів планування довготермінового зберігання.

Виклад основних положень. Особливість запропонованого підходу [6, 7] полягає в тому, що при плануванні зберігання з метою забезпечення доступності розглядається живучість інформаційних об’єктів (ІО), тобто властивість виконувати основні функції в умовах негативних впливів (НВ), тимчасово відмовляючись від виконання деяких другорядних функцій [8].

До основних НВ (загроз) при довготерміновому зберіганні відносять: відмови обладнання; старіння програмного забезпечення (ПЗ), форматів, обладнання; атаки; помилки операторів; катастрофи; економічні помилки і т. ін. Для підвищення живучості ІО в даній роботі досліджуються закономірності, будуються моделі різних видів НВ, загроз: множинних відмов, стану обчислювальних ресурсів, помилок на носіях даних, старіння ПО / форматів, мережевих атак [6, 7, 9] .

Модель множинних відмов. Для аналізу впливу близьких у часі відмов на живучість ІО у розподілених мережах зберігання даних було розроблено імітаційну модель множинних відмов [7].

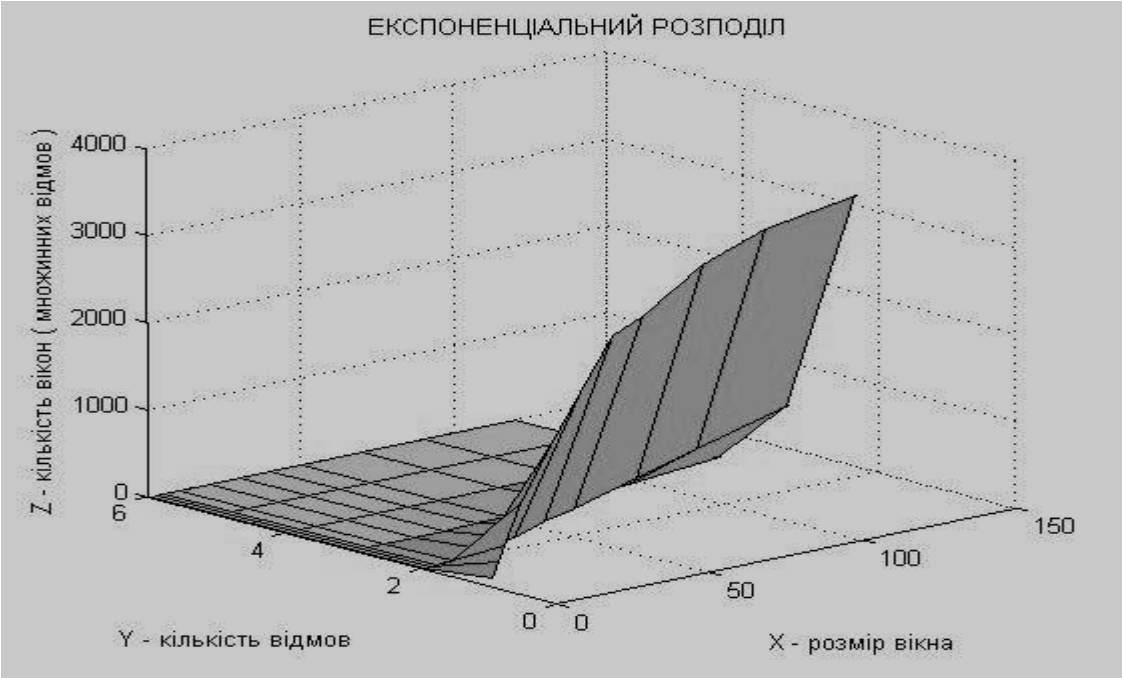


Рис. 1. Оцінка кількості множинних відмов при експоненційному розподілі.

Близькі за часом відмови у великій кількості вузлів можуть зменшити ефективність реплікації і, відповідно, живучість ІО. Характеристики корельованих відмов аналізувалися за допомогою вікна спостереження (часового вікна). Результати

показують, що при експоненційному розподілі відмов більшість часових вікон припадає на вікна з максимальним значенням часу спостереження (Рис. 1.), а при ступеневому розподілі – на вікна з малим значенням часу (Рис. 2). Вікна з малим значенням часу спостереження (в які потрапляють близькі у часі відмови) і відповідні їм значення кількості близьких у часі відмов (а також відповідні кількості вікон) характеризують найбільш складні для забезпечення доступності даних та живучості ІО періоди.

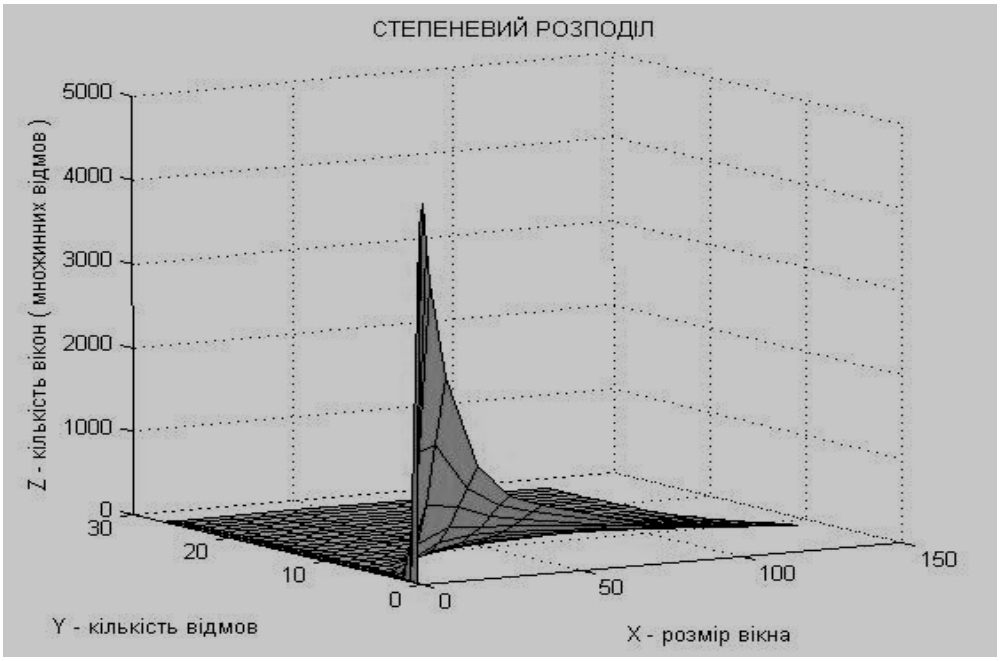


Рис. 2. Оцінка кількості множинних відмов при ступеневому розподілі.

Модель стану обчислювальних ресурсів у розподілених комп’ютерних системах. Для надійного функціонування у складі розподілених комп’ютерних систем передбачаються засоби моніторингу стану обчислювальних ресурсів. Ця інформація може відображати нормальний стан ресурсів; стан, що потребує уваги; критичний стан. Крім того, може бути представлена більш детальна інформація про результати виконання окремих тестів у процесі моніторингу. Модель стану обчислювальних ресурсів у розподілених комп’ютерних системах може використовуватися для опосередкованої оцінки загроз, негативних впливів на інформаційні об’єкти, що зберігаються в таких системах, планування довготермінового зберігання та забезпечення живучості. З цією метою розробляються програмні засоби накопичення результатів моніторингу для їх подальшого аналізу.

Модель відмов на носіях даних. Для дослідження живучості ІО при довготерміновому зберіганні на носіях даних було зібрано статистику на основі показника помилок PI Sum 8 для DVD-дисків [9]. Дані були проранжировані за кількістю помилок та апроксимовані з допомогою ступеневої функції. Цей та інші отримані результати обґрунтовують можливість використання моделі із ступеневим розподілом помилок.

Модель мережевих атак. При розробці моделі в якості опосередкованої оцінки статистики мережевих атак при довготерміновому зберіганні даних у розподілених мережах використовувалася статистика повідомлень про кібератаки, зібрана в новинах Інтернет-ресурсів. Тобто, для оцінки загроз, що створюються мережевими атаками, в якості емпіричних даних моделі використовувались результати пошуку по ретроспективній базі Рунета, створеній за допомогою технології моніторингу новин

системи InfoStream. По датах за період 2010 – 2013 рр. було отримано блізько півтори тисячі значень кількостей повідомлень про кібератаки. Розглядається апроксимація розподілу дат, ранжируваних за кількістю повідомлень про кібератаки за допомогою логарифмічної або степеневої функцій.

Модель старіння ПЗ / форматів. Для оцінки статистики старіння ПЗ / форматів при довготерміновому зберіганні (і відповідних загроз) досліджувалася статистика розвитку проектів розробки ПЗ. З цією метою розглядалися проекти ПЗ з відкритим вихідним кодом, а саме – статистика розподілу часу між публікаціями чергових версій ПЗ або чергових пакетів розширень.

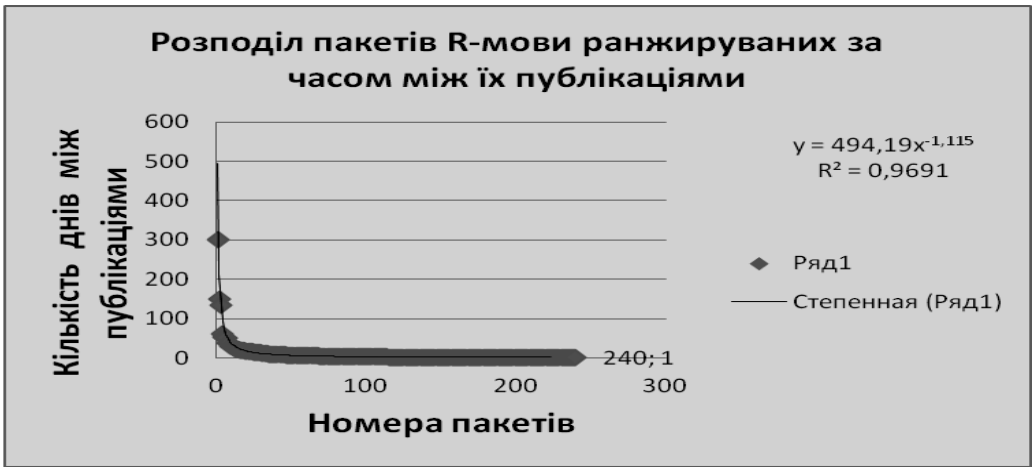


Рис. 3. Розподіл пакетів R–мови, ранжируваних за часом між їх публікаціями з апроксимацією степеневою функцією.

Рис. 4. Розподіл пакетів R-мови, ранжируваних за часом між їх публікаціями у подвійній логарифмічній шкалі.

У результаті аналізу дат публікації пакетів розширень із загального мережевого архіву (CRAN) R-мови програмування було побудовано розподіл пакетів, ранжируваних за часом між їх публікаціями. Він може бути апроксимований за допомогою ступеневої функції з достовірністю апроксимації майже 0,97, що дозволяє припустити ступеневий характер статистики старіння ПЗ (Рис. 3). При представленні отриманого розподілу у подвійній логарифмічній шкалі графік приблизно відповідає прямій лінії, що підтверджує наявність ступеневого закону (Рис. 4).

Аналіз статистики про інші проекти відкритого ПЗ (GCC – набір компіляторів, Ruby – мова програмування) показав більший коефіцієнт достовірності при апроксимації експоненційною функцією, що може пояснюватися недостатнім обсягом зібраної статистики.

Моніторинг загроз. Забезпечення живучості ІО в умовах негативних впливів передбачає оцінку цих впливів з метою вибору адекватної реакції, відмови від деяких функцій. Тобто однією з важливих задач забезпечення живучості є моніторинг негативних впливів [10, 11], загроз довготерміновому зберіганню. Моніторинг щодо виявлення загроз повинен здійснюватися з використанням запропонованих моделей загроз. Як зазначалося вище, планування зберігання відповідно до моделі OAIS теж передбачає моніторинг змін у технологічному середовищі та у вимогах користувачів як одну з основних функцій.

У роботі [12] наголошується, що в довготерміновому зберіганні моніторинг є ключовою функцією, яка забезпечує раннє виявлення загроз. Проте, так як обсяг та різноманітність загроз зростають, стає неможливим ручний моніторинг усіх аспектів середовища, які можуть заважати зберіганню. Більше того, моніторинг повинен виявляти не тільки ризики зберігання, а й сприятливі можливості (наприклад, зменшення витрат) та гарантувати, що дії по зберіганню, визначені процесами керування, досягають цілей та виправдовують сподівання.

Оскільки запропоновані вище моделі теж направлені на виявлення загроз, то розробка таких моделей може розглядатися як складова частина моніторингу загроз. Тобто не тільки виявлення загроз, а й удосконалення, оновлення та розробка нових моделей загроз повинні здійснюватися протягом всього життєвого циклу довготермінового зберігання. Таку діяльність доцільно організовувати на основі мережі відповідних центрів компетенції, які обмінюються інформацією між собою.

Висновки.

Зібрано значний статистичний матеріал, на базі якого побудовано моделі основних видів загроз, негативних впливів при довготерміновому зберіганні великих обсягів даних. Показано важливе місце ступеневого розподілу в цих моделях.

Побудовані моделі, особливості статистики їх розподілів є основою розробки методів планування довготермінового зберігання для забезпечення живучості інформаційних об’єктів.

Оновлення, удосконалення моделей загроз (як і безпосередньо моніторинг загроз) повинні здійснюватися протягом всього життєвого циклу зберігання на основі відповідних центрів компетенції.

Використана література

1. About LexisNexis. – Режим доступу : //www.lexisnexis.com/en-us/about-us/about-us.page

2. США : Основные положения Типового закона о правовых актах, публикуемых в электронном виде. – Режим доступу : //www.rusrim.blogspot.com/2013/04/blog-post_7303.html

3. Rodes S., Neacsu D. Preserving and ensuring long-term access to digitally born legal information // Information and Communication Technology Law – 2009. – Vol. 18. – No.1. – P. 39-74.

4. Rhodes S. Breaking Down Link Rot: The Chesapeake Project Legal Information Archive’s Examination of URL Stability // Law Library Journal. – 2010. – Vol. 102 – No. 33. – P. 581-597.

5. Danner R. A., Leong K., Miller W. V. The Durham Statement Two Years Later: Open Access in the Law School Journal Environment // Law Library Journal. – 2011. – Vol. 103. – No. 2. – P. 39-54.

6. Ланде Д.В., Березін Б.О. Живучість інформаційних об’єктів при довготерміновому зберіганні великих об’ємів даних // Інформація та безпека. – 2012. – № 3-4 (11-12). – С. 13-15.

7. Березін Б.О., Ланде Д.В. Оцінка живучості інформаційних об’єктів при довготерміновому зберіганні великих обсягів даних : *материалы международной научной конференции ИТБ-2013 [“Информационные технологии и безопасность. Оценка состояния”]* : – К. : ИПРИ НАН Украины, 2013. – С. 21-27.

8. Додонов А.Г., Ландэ Д.В. Живучесть информационных систем. – К. : Наук. думка, 2011. – 256 с.

9. Березін Б., Ланде Д. Дослідження стану оптичних носіїв при довготерміновому зберіганні цифрової інформації // Студії з архів. справи та документознавства. – 2012. – Т. 20. – С. 133-139.

10. Додонов А.Г., Флейтман Д.В. Технологические аспекты обеспечения живучести информационных систем // Известия Таганрогского государственного университета. – 2005. – Т. 48. – № 4. – С. 5-7.

11. Бойченко А.В. Вимоги до систем моніторингу факторів впливу на живучість // Реєстрація, зберігання і обробка даних. – 2008. – № 1. – С. 103-115.

12. Faria L., Petrov P., Duretec K., Becker C., Ferreira M., Ramalho J. Design and architecture of a novel preservation watch system // In International Conference on Asia-Pacific Digital Libraries, 2012. – P. 168-178.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

Інформаційні ресурси з інших спеціальностей юридичних наук

УДК 343.365:343.237(091)(477)

БЕНІЦЬКИЙ А.С., *кандидат юридичних наук, доцент,*
Луганський державний університет
внутрішніх справ ім. Е.О. Дідоренка

ВІДПОВІДАЛЬНІСТЬ ЗА ПРИЧЕТНІСТЬ ДО ЗЛОЧИНУ ТА СПІВУЧАСТЬ У ЗЛОЧИНІ ЗГІДНО З КРИМІНАЛЬНИМ ЗАКОНОДАВСТВОМ РОСІЙСЬКОЇ ІМПЕРІЇ (ДРУГА ПОЛОВИНА XIX – ПОЧАТОК XX СТОЛІТТЯ)

Анотація. *Про норми Уложення про покарання кримінальні та виправні у ред. 1885 р., Кримінального уложення 1903 р. та інших кримінально-правових документів Російської імперії, які передбачали відповідальність за причетність до злочину та співучасть у злочині.*

Ключові слова: *причетність до злочину, приховування злочину, недонесення, потурання, співучасть у злочині.*

Аннотация. *О нормах Уложения о наказаниях уголовных и исправительных в ред. 1885 г., Уголовного уложения 1903 г. и других уголовно-правовых документов Российской империи, предусматривающих ответственность за причастность к преступлению и соучастие в преступлении.*

Ключевые слова: *причастность к преступлению, укрывательство преступления, недонесение, попустительство, соучастие в преступлении.*

Summary*. About the norms of Code of criminal and correctional penalties (ed. 1885), Criminal Code of 1903 and other criminal and legal documents of the Russian Empire, which provided responsibility for implication and complicity in the crime.*

Keywords: *implication in a crime, concealment of a crime, misprision, connivance, complicity in a crime.*

Постановка проблеми. Основними джерелами кримінального права на українських землях, які були у складі Російської імперії, від другої половини XIX століття до встановлення радянської влади були Уложення про покарання кримінальні та виправні в редакції 1885 року, Статут про покарання, що накладаються мировими суддями 1864 р., Статут про засланих у редакції 1909 року, Кримінальне уложення 1903 р. та військово-морське кримінальне законодавство. Тому їх дослідження становить інтерес для визначення впливу російського законодавства на становлення законодавства українських державних утворень у період 1917 – 1920 рр., а також кримінального законодавства Радянської України щодо причетності до злочину та співучасті у злочині.

Проблеми історичного розвитку кримінального законодавства Російської імперії XIX – XX століть досліджувалися в роботах таких учених, як С.І. Баршев, Л.С. Білогриць-Котляревський, П.Й. Бобровський, В.В. Єсипов, О.С. Жиряєв, О.Ф. Кістяковський, О.В. Лохвицький, А.В. Наумов, М.А. Неклюдов, П.П. Пусторослев, М.Д. Сергієвський, В.Д. Спасович, М.С. Таганцев, І.Я. Фойницький, П.Л. Фріс та інші. Між тим, питанням співвідношення кримінально-правових норм Уложення 1845 р. у редакції 1885 р. та інших російських законодавчих документів XIX – початку XX століття, які містили положення про інститут причетності до злочину та співучасті у злочині, приділялася недостатня увага.

Метою статті є визначення основних ознак приховування злочину, недонесення, потурання, а також видів та форм співучасті у злочині, які містились у правових документах Російської імперії XIX – початку XX століття.

Виклад основного матеріалу. У 1845 році Державною Думою Російської імперії було прийнято Уложення про покарання кримінальні та виправні (Далі – Уложення). 15 серпня 1845 року воно було затверджене російським імператором Миколою I, а набрало сили 1 травня 1846 року. З 1845 до 1885 року редакція цього Уложення змінювалася, а в редакції 1885 р. воно діяло до революції 1917 р. Уложення 1885 р. закріплювало низку положень про причетність до злочину та співучасть. Так, наприклад, у ст. 11 Уложення 1885 р. передбачалося дві форми співучасті: 1) співучасть без попередньої змови та 2) співучасть за попередньою змовою. Для кожної з цих форм був характерним свій перелік видів співучасників.

Відповідно до ст. 12 Уложення 1885 р. за співучасті без попередньої змови виділялися такі види, як: 1) головні винуватці; 2) учасники. До головних винуватців відносилися: 1) особи, які розпоряджалися діями інших учасників; 2) особи, які керували діями інших учасників; 3) особи, які стали до дії раніше за інших, від самого її початку; 4) особи, які безпосередньо вчинили злочин. До кола учасників входили: 1) особи, які надавали допомогу головним винуватцям у скоєнні злочину; 2) особи, які доставляли засоби на місце злочину; 3) особи, які усували перешкоди для вчинення злочину.

У разі співучасті за попередньою змовою вирізнялися такі види: 1) призвідники; 2) спільники; 3) підмовники або підбурювачі; 4) пособники.

До призвідників відносилися: 1) особи, які керували діями інших при вчиненні злочину або замаху на злочин; 2) особи, які перші розпочали вчиняти злочин (ті, хто подає приклад іншим учасникам вчинення злочину – *А.Б.*). Спільниками вважалися: 1) особи, які погодилися з призвідниками вчинити спільними зусиллями умисний злочин; 2) особи, які погодилися з учасниками вчинити спільними зусиллями умисний злочин. До підмовників і підбурювачів належали особи, які не брали участі в злочині, але проханнями, переконаннями, підкупом, обіцянням вигод, спокушанням, обманом, примусом чи погрозами схилили інших до вчинення злочину. До пособників відносились особи, які не брали участі у вчиненні злочину, але з корисливості чи інших особистих спонукань: 1) допомагали або зобов’язали допомагати тим, хто замислив злочин: а) порадами, указівками, повідомленням інформації; б) доставлянням яких-небудь засобів для вчинення злочину; в) усуненням перешкод; 2) заздалегідь, перед вчиненням злочину, надавали в себе притулок учасникам злочину; 3) заздалегідь обіцяли сприяти після скоєного, переховати злочинців чи приховати злочин.

Формулюючи ознаки пособництва, російський законодавець виділив критерії, які дозволяють відмежувати співучасть від причетності до злочину. В Уложенні 1885 р. указується на те, що пособником визнається особа, яка завідомо перед вчиненням злочину обіцяла сприяти переховуванню злочинців або прихованню злочину після скоєного. Отже, якщо таке сприяння заздалегідь не обіцяне, то пособництвом воно не охоплювалось би. Згідно з Уложенням 1885 р. така діяльність вважалася причетністю до злочину.

Відповідальність для перелічених видів співучасників була різною залежно від ступеня їх участі у вчиненому злочині. Так, згідно зі ст. 117 Уложення 1885 р. в разі вчинення злочину без попередньої змови головні винуватці засуджувалися до “найвищої міри покарання, за той злочин у законах належного” [10], а учасники злочину каралися на ступінь чи два нижче за те, що чекало на головних винуватців.

За вчинення злочину за попередньою згодою призвідники, якщо в законі не визначався особливий рід або особлива міра покарання, а також підмовники й

підбурювачі засуджувалися до найвищої міри покарання, передбаченої за злочин, у якому вони брали участь (ст.ст. 118 і 120 Уложення 1885 р.).

Для спільників у злочині відповідно до ст. 119 Уложення 1885 р. міра відповідальності визначалася залежно від міри сприяння призвідникам у підготуванні до злочину, у підшуканні учасників злочину, а також залежно від сприяння у вчиненні злочину. Пособники, дії яких були необхідні для вчинення злочину, згідно зі ст. 121 Уложення 1885 р. несли відповідальність нарівні з тими, хто його вчинив, а решта – на ступінь нижче у разі сприяння у вчиненні злочину.

В Уложення 1885 року було включено норми, які передбачали відповідальність за причетність до злочину (“причастных к делу и преступлению”). У ст.ст. 14 та 15 визначались особи, які були причетні до злочину: 1) потурачі, ті, хто, маючи владу або можливість попередити злочин, цілеспрямовано або свідомо допустили його вчинення; 2) переховувачі, ті, хто не брав участі у вчиненні злочину, а після скоєного: а) приховав або знищив сліди злочину; б) сховав злочинців; в) узяв до себе або прийняв на зберігання, або передав чи продав іншим викрадене або відняте у кого-небудь, або іншим протизаконним способом здобуті речі; 3) особи, які завідомо знали про умисний (мається на увазі підготовлюваний або вчинюваний злочин – *А.Б.*) або вже вчинений злочин, мали можливість повідомити про це владу, але не виконали цього обов’язку.

Відповідальність за причетність до злочину передбачалась у різних розділах Уложення 1885 р. залежно від того, які було порушено суспільні відносини особами, що скоїли первинний злочин (напр., ст.ст. 822, 930, 931-1, 931-2, 1210, 1670-1, 1701 та 1702).

Згідно з Уложенням 1885 р. за приховування несли відповідальність не тільки фізичні особи, а й громади. Так, статтею 530 встановлювалося: “з єврейської громади, у якій переховувався військовий втікач із євреїв, стягується…” [10]. Цією нормою в російському кримінальному праві того періоду закріплювався принцип колективної відповідальності за вчинення злочину. Такий репресивний підхід законодавця Російської імперії був зумовлений, імовірно, тим, що дуже складно було змінити звичаї та традиції релігійних або етнічних груп населення Росії, щоб особи сприяли виявленню та видачі органам влади розшукуваних осіб.

Як слушно зазначав Н.Д. Сергієвський, інститут групової відповідальності завжди існував у російському кримінальному праві і “найпевніше, завжди існуватиме, видається у письменників немовби однією суцільною, безперервною помилкою… – положення, очевидно, неслушне” [9, с. 41].

В Особливій частині Уложення 1885 р. пропонується такий різновид причетності, як заздалегідь не обіцяне придбання або збут майна, завідомо здобутого злочинним шляхом (ст.ст. 822, 930, 931-1, 931-2, 1210, 1670-1, 1701, 1702).

За вчинення деяких злочинів передбачалась однакова відповідальність для співучасників (призвідників, спільників, пособників, підмовників або підбурювачів) і причетних осіб (потурачів, переховувачів або недоносителів). Так, наприклад, згідно зі ст. 243 Уложення 1885 р. всі учасники посягання на особу імператора або його владу у вигляді спільників, підмовників, підбурювачів або потурачів, а так само переховувачів і недоносителів засуджуються “до того ж покарання”.

В Особливій частині Уложення 1885 р. мовиться про такі форми злочинної діяльності, як скоп, змова, зграя, злочинне співтовариство. За вчинення злочину в складі таких злочинних об’єднань передбачалася спеціальна відповідальність.

В окремих кримінально-правових нормах Уложення 1885 р. містилися ознаки потурання злочину. Так, відповідно до відділення 1 (“О преступлениях и проступках

чиновников при следствии и суде, ст. 426 – 434”) глави XI (“О преступлениях и проступках чиновников по некоторым особым родам службы, ст.ст. 426 – 505”) розділу 5 (“О преступлениях и проступках по службе государственной и общественной, ст.ст. 329 – 505”) Уложення 1885 р. до відповідальності притягувалися слідчі: за порушення своїх посадових обов’язків (ст. 426), за придбання майна, що є “предметом справи” (ст. 427), за невідкриття провадження в справі, коли були достатні підстави для проведення слідства (ст. 429), за тяганину при веденні слідства (ст. 431), за примушення до дачі показань (ст. 432). Згідно з відділенням 3 (“О преступлениях и проступках чиновников полиции, ст.ст. 446 – 459”) глави XI розділу 5 Уложення 1885 р. до відповідальності притягувалися чиновники поліції за потурання злочину (ст. 446).

У 1864 році Державною Думою Російської імперії було прийнято Статут про покарання, що накладаються мировими суддями (далі – Статут про покарання 1864 р.) [11]. Цей документ вміщував кримінально-правові норми, виділені з Уложення 1885 р., про злочинні діяння, підвідомчі мировим суддям. Статут про покарання 1864 р. передбачав відповідальність за менш тяжкі протиправні діяння (проступки).

У статті 15 Статуту про покарання 1864 р. містилося положення про співучасть: “За участі двох чи більше осіб у вчиненні проступку ті з винних, які його самі вчинили або підготували до того інших, караються суворіше, ніж їхні співучасники”. Таким чином, можна було б виокремити три види співучасників: 1) особи, які вчинили діяння (виконавці), 2) особи, які підбурювали до вчинення проступку (підбурювачі), 3) інші особи, які брали участь у вчиненні проступку.

В Особливій частині Статуту про покарання 1864 р. встановлювалася відповідальність за окрему форму незаконної діяльності – участь у збіговиську (напр., ст. 42-1 Статуту про покарання 1864 р.). Крім того, документ містив норми, які визначали відповідальність за деякі види причетності до злочину (приховування злочинця або майна, здобутого злочинним шляхом, а також придбання або збут майна, здобутого злочинним шляхом). Наприклад, відповідно до ст. 172 Статуту про покарання 1864 р. приховувачі злочину та учасники злочину несли однакову відповідальність: “за участь у крадіжці та за приховування викраденого винні підлягають покаранням, визначеним за крадіжку”. Однак мировий суддя міг зменшити покарання до половини для цих осіб.

До початку XX століття на території Російської імперії, крім Уложення про покарання кримінальні та виправні 1885 р., Статуту про покарання, що накладаються мировими суддями 1864 р., Статуту про засланих 1909 р., діяло військово-морське кримінальне законодавство. Воно було закріплено у Військовому та Морському статутах. Військово-морське кримінальне право на території Російської імперії почало діяти від часів Петра I. З моменту прийняття Військового статуту 1716 р. й Морського статуту 1720 р. воно періодично змінювалося. У 1797 році було прийнято Статут військового флоту, який у 1853 році замінено на Морський статут. У 1812 році Військовий статут 1716 року доповнено Польовим уложенням, що містило військово-кримінальні закони, які діяли у воєнний час. У 1839 році було прийнято Військово-кримінальний статут. У 1867 році введено в дію Загальну частину, а в 1868 році – Особливу частину Військового статуту про покарання, який замінив Військово-кримінальний статут 1839 р. У 1869 році прийнято Дисциплінарний статут, у 1868 році – Морський статут про покарання (у 1885 році його редакцію було змінено). Прийнятий у 1874 році Статут військовий про повинність зумовив прийняття в 1875 році Військово-кримінального кодексу.

Окремі кримінально-правові норми, що містилися в узаконеннях по військово-морському відомству, наприкінці XIX століття були зведені у Військово-Морський статут про покарання. У період першої світової війни було посилено кримінальну

відповідальність за військові злочини. Так, наприклад, згідно з наказом № 29 від 14 січня 1916 року за підбурювання до дезертирства могла бути призначена смертна кара [8, с. 86]. У зв’язку з цим до військово-морського кримінального законодавства було внесено відповідні зміни.

У Статуті про засланих кримінально-правові норми містилися в главі шостій “Про кримінальну і дисциплінарну відповідальність засланих” [12]. Документ цей було затверджено 22 липня 1822 року Олександром I. Редакція статуту час від часу змінювалася, оновлені видання його виходили в 1857, 1890, 1906 й у 1909 роках. Деякі з кримінально-правових норм цього документа визначали ознаки переховування злочинця. Так, відповідно до статті 249 Статуту про засланих 1909 р. за обмін іменами та прізвищами заслані (каторжани, заслані поселенці) підлягали певним видам покарань.

22 березня 1903 року Державною Думою Російської імперії було прийнято Кримінальне уложення. Однак у повному обсязі його не було введено в дію. Від 1904 року й до жовтневої революції 1917 року на території Російської імперії поетапно вводилися в дію окремі глави Кримінального уложення.

У ст. 51 Кримінального уложення закріплюються ознаки співучасті, із яких можна визначити, що співучастю є діяльність кількох осіб, які погодилися вчиняти злочинні діяння або діяли спільно. Ця норма пропонує три види співучасників: 1) особи, які безпосередньо вчинили злочинне діяння або брали участь у його виконанні (виконавці); 2) особи, які підбурили іншого до співучасті в злочинному діянні (підбурювачі); 3) особи, які були пособниками, що доставляли засоби або усували перешкоди, надали допомогу у вчиненні злочинного діяння порадою, указівкою чи обіцянням не зашкоджувати його вчиненню або приховати його (пособники).

Кримінальне уложення містило положення, згідно з яким знижувалася міра відповідальності для деяких видів співучасників злочину. За ч. 2 ст. 51 Кримінального уложення співучасники тяжкого злочину або злочину підлягають покаранню за вчинене злочинне діяння, але для пособника покарання пом’якшується за умови, що його допомога була неістотною.

У розгляданому документі було передбачено диференціацію відповідальності співучасників проступку. Виходячи з положень ч. 3 ст. 51 Кримінального уложення за вчинення проступку карається лише той, хто безпосередньо його вчинив або брав участь у його вчиненні, а підбурювач і пособник підлягають покаранню тільки у випадках, які визначено в законі.

Кримінальне уложення в Загальній та Особливій частинах вирізняє форми співучасті. Так, у ст. 52 Кримінального уложення, яка встановлювала правила кваліфікації діянь учасників злочинного співтовариства, зазначалося, що особа, яка погодилася взяти участь у співтоваристві для вчинення тяжкого злочину або злочину і не відмовилася від подальшої співучасті, але не була співучасником тяжкого злочину або злочину, відповідає тільки за участь у співтоваристві. У ч. 2 ст. 52 Кримінального уложення визначено, що участь у співтоваристві для вчинення тяжкого злочину або злочину в зграї, створеній для вчинення кількох тяжких злочинів або злочинів, карається у випадках, окремо законом указаних.

Таким чином, у Загальній частині Кримінального уложення вбачаються дві форми співучасті: злочинне співтовариство взагалі й злочинне співтовариство у вигляді зграї. В Особливій частині Кримінального уложення, крім співтовариства і зграї, указується на такий вид злочинного об’єднання, як скопище.

Кримінальне уложення не згадує про причетність до злочину. Однак, незважаючи на це, деякі види причетності наводяться в Особливій частині Кримінального уложення,

у якій передбачалася відповідальність за недонесення про злочин (ст.ст. 163 і 644) та учасника тяжкого злочину (ст. 164), а також за переховування злочинця (ст.ст. 168 і 644), майна (ст. 279) і речових доказів (ст. 166).

Слід зазначити, що ст. 170 Кримінального уложення закріплювала правило, за яким до осіб, які вчинили злочини, передбачені ст.ст. 162 – 169 Кримінального уложення (не повідомили владу про достеменно відомий злочин, а також вчинили приховування), не застосовувалося покарання. Це відбувалось у випадку, коли: 1) повідомлення про злочин було б звинуваченням члена сім’ї недоносителя у вчиненні ним тяжкого злочину або злочину; 2) приховувався злочин, вчинений членами сім’ї приховувача; 3) переховуваним був член сім’ї переховувача. Цікаво зазначити, що ст. 170 Кримінального уложення закріплювала такі правила: 1) до недоносителя не застосовувалося покарання за неповідомлення про злочин, який він вчинив; 2) до осіб не застосовувалося покарання за приховування вчиненого ними злочину.

В Особливій частині Кримінального уложення було вказано на такий вид причетності, як придбання, прийняття на зберігання й збут чужого майна, здобутого завідомо злочинним шляхом. Так, відповідно до п. 4 ч. 1 ст. 279 Кримінального уложення покаранню піддавалися винні в участі в грає, утвореній для придбання, прийняття на зберігання, приховання, застави або збуту чужого майна, здобутого завідомо злочинним шляхом. Крім того, за ч. 1 ст. 279 Кримінального уложення покарання зазнавала особа, винна в наданні пристановища завідомо учасникові грає. Однак у нормі не вказувалося, чи має воно бути заздалегідь обіцяним.

27 лютого 1918 року відбулася Лютнева буржуазно-демократична революція. Органи управління державою перейшли до Тимчасового уряду. 1 вересня 1917 року постановою Тимчасового уряду було проголошено Російську Республіку. У період дії Тимчасового уряду на території російської держави продовжували бути чинними Уложення про покарання кримінальні та виправні 1885 р., Статут про покарання, що накладаються мировими суддями, 1864 р., Статут про засланих 1909 р., Військовий і Морський статути. Судами в той час не застосовувалися лише кримінально-правові норми, які стосувалися посягання на імператора і членів його сім’ї.

На території України після зречення російського імператора Миколи ІІ від престолу почалось формування національних органів влади. У березні 1917 року в Києві була створена Центральна Рада, куди увійшли представники українських політичних партій, громадських організацій та різних верств суспільства. У квітні 1917 року на Всеукраїнському національному конгресі Центральна Рада отримала статус виконавчого органу, який діяв на українських землях. 25 жовтня (7 листопада) 1917 року Тимчасовий уряд було скинуто більшовиками. 7 (20) листопада 1917 року Українська Центральна Рада у своєму Третьому універсалі оголосила створення Української Народної Республіки (далі – УНР) у складі Російської Республіки [1].

25 листопада (7 грудня) 1917 року УНР приймає Закон “Про правонаступництво”, яким було визначено, що до сформування Федеративної Російської Республіки всі закони і постанови, які мали силу на території Української Народної Республіки до 27 жовтня 1917 року, оскільки вони не змінені і не скасовані універсалами, законами і постановами Української Центральної Ради, мають силу і надалі як закони і постанови Української Народної Республіки [6]. Дане положення було підтверджено Законом УНР “Про порядок видання законів” від 8 (21) грудня 1917 р. [5] Таким чином, на території України продовжувало діяти кримінальне законодавство Російської імперії.

9 (22) січня 1918 року IV універсалом Української Центральної Ради було проголошено, що Українська Народна Республіка стає самостійною державою [2].

3 березня 1918 р. у Брест-Литовську між Росією, з одного боку, і Німеччиною та її союзниками, з іншого, був укладений мирний договір, за яким радянський уряд визнавав незалежність України. 29 квітня 1918 року на Всеукраїнському землеробському конгресі в Києві було проголошено Гетьманат під керівництвом Павла Скоропадського. Його уряд у документах мав назву – Українська держава. Державні органи УНР було скасовано. Урядом П. Скоропадського також було скасовано нормативно-правові документи, які було прийнято за часів Тимчасового уряду, а також Центральної Ради. Так, П. Скоропадський у Грамоті до всього українського народу від 29 квітня 1918 року вказував, що “усі розпорядження колишнього українського уряду, а також тимчасового Російського уряду відміняються і знищуються” [3].

У період правління П. Скоропадського на українських землях де-факто діяло законодавство Російської імперії. Так, у пункті 23 Закону Української держави “Закони про тимчасовий державний устрій України” від 29 квітня 1918 року було вказано, що “Українська Держава керується на твердих основах законів, виданих в установленій черзі” [4]. Між тим, урядом П. Скоропадського не було прийнято нормативного документа, який би визначав порядок застосування законодавства Російської імперії. На думку В.М. Іванова, тою мірою, як затверджувалися відповідні закони Української держави, скасовувались попередні законодавчі акти, про що, як правило, вказувалося в тексті того чи іншого закону [7, с. 19]. У період Гетьманату не було прийнято кримінального законодавства, тому на землях Української держави продовжувало діяти кримінальне законодавство Російської імперії.

14 грудня 1918 року П. Скоропадський відрікся від влади. Державні гілки влади на окремих українських земелях перейшли до Директорії Української Народної Республіки (далі – Директорія УНР). У період правління Директорії УНР було прийнято низку законодавчих актів щодо протидії окремим видам злочинів. Між тим, Директорія УНР застосовувала кримінальне законодавство Російської імперії. Так, наприклад, у червні 1919 року Надзвичайний Військовий Суд при Штабі Дієвої Армії пред’явивши обвинувачення отаману Петру Болбочану у скоєнні злочину, передбаченого артикулом 246 Зводу військових постанов 1869 р., зазначив, що отаман Петро Болбочан “злочинно захопив владу – посаду Командуючого Запорізькою групою і тим дезорганізував військовий фронт під час щасливого наступу проти ворога” [14]. 10 червня 1919 року Надзвичайний Військовий Суд позбавив Петра Болбочана всіх прав стану і призначив покарання до страти [13].

У період із кінця грудня 1918 року до кінця 1920 року на землях України розгорнулася із нової силою Громадянська війна. Директорія УНР змушена була вести бойові дії з радянськими військами, повстанською армією під керівництвом Нестора Махна, Збройними силами Півдня Росії під керівництвом генерала А.І. Денікіна та іншими військовими формуваннями, які існували в цей період на території України. Директорія УНР фактично проіснувала до кінця 1920 року.

Уряди УНР, Української держави та Директорії УНР у зв’язку із малим періодом свого існування, а також через постійні військові сутички із внутрішніми та зовнішніми ворогами не змогли утворити кримінального законодавства незалежної України.

18 березня 1921 року в Ризі був підписаний мирний договір між Польщею, з одного боку, та РРФСР й УСРР, з іншого боку. Згідно з умовами договору основна частина українських земель опинилась під радянською владою, а частина західних українських земель увійшли до складу Польської Республіки (Друга Річ Посполита). На території західних українських земель, що опинилися під владою Польщі, діяло кримінальне законодавство цієї країни. Слід зазначити, що на території Польщі, яка

раніше входила до складу Російської імперії, діяло Кримінальне уложення 1903 р. 1 вересня 1932 р. у Польщі було прийнято Кримінальний кодекс та Закон про проступки.

Висновки.

Основним кримінально-правовим документом на українських землях, які були у складі Російської імперії, з другої половини XIX століття до приходу радянської влади було Уложення про покарання кримінальні та виправні 1845 р. У ньому вперше було зафіксовано положення про причетність до злочину, які послужили основою для формування його в самостійний кримінально-правовий інститут. У кримінально-правових нормах Уложення 1845 р. (в редакції 1885 р.) було передбачено види причетності до злочину, які відрізнялися від видів та форм співучасті в злочині. Для співучасників та причетних до злочину осіб установлювалася різна система покарань. При кваліфікації діянь приховувачів злочину необхідно було встановлювати момент дачі ними згоди виконавцеві та іншим учасникам злочину на вчинення відповідних діянь із приховування їхньої злочинної діяльності. Разом із тим, за злочини проти членів імператорської сім’ї, державну зраду, а також інші особливо небезпечні злочини недоносителі та приховувачі несли таку ж відповідальність, як і основні виконавці злочинів.

Використана література

1. III універсал Української Центральної Ради від 7 (20) листопада 1917 р. // ЦДАВО України. Ф. 1115. Оп. 1. Спр. 4. Арк. 9.

2. IV універсал Української Центральної Ради від 9 (22) січня 1918 р. // Вісник Ради Народних Міністрів Української Народної Республіки. – 1917. – № 3. – 13 січня.

3. Грамота ко всему украинскому народу от 29 апреля 1918 г. – Режим доступу : //www.cn.archives.gov.ua/expos/temat/independ/4.html

4. Закони про тимчасовий державний устрій України : Закон Української держави від 29 квітня 1918 р. // Українська суспільно-політична думка в XX ст. – Документи і матеріали в 2- х. Т. І. / [упор. Т. Гунчак і Р. Сольчаник]. – К. : Сучасність, 1983. – С. 386-389.

5. Про порядок видання законів : Закон УНР від 8 (21) грудня 1917 р. – Режим доступу : //www.textbooks.net.ua/ content/ view/998/17

6. Про правонаступництво : Закон УНР від 25 листопада (7 грудня) 1917 р. – Режим доступу : //www.textbooks.net.ua/ content/ view/993/17

7. Іванов В.М. Історія держави і права : навч. посіб. : у 2-х частинах / В.М. Іванов – К. : МАУП, 2002. – Ч. 2. – 2003. – 224 с.

8. Приказ по Военному ведомству № 29 от 14 января 1916 г. // Разведчик. – 1916. – № 1318. – С. 86.

9. Сергеевский Н.Д. Наказание в русском праве XVII века / Н.Д. Сергеевский. – СПб. : Изд. книжн. маг. А.Ф. Цинзерлинга, 1887. – С. 41.

10. Уложение о наказаниях уголовных и исправительных 1845 г. – Режим доступу : //www.civil. consultant.ru/reprint/books/229/2. html#img3

11. Устав о наказаниях, налагаемых мировыми судьями, 1864 г. – Режим доступу : //www.civil. consultant.ru/reprint/books/229/2. html#img3

12. Устав о ссыльных // Свод законов Российской империи. Т. XIV. – СПб. : Деятель, 1912. – Ст. 3427.

13. ЦДАВО України. Ф. 2279. Оп. 1. Спр. 3. Арк. 13.

14. ЦДАВО України. Ф. 2279. Оп. 1. Спр. 3. Арк. 21.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

Європейські правові стандарти

Офіційний переклад
засвідчено Міністерством закордонних справ України від 01.07.02 р.

Конвенція Ради Європи від 28 січня 1981 року № 108

“Про захист осіб у зв’язку з автоматизованою обробкою персональних даних”

(Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Amendment to Convention ETS No. 108 allowing the European Communities to accede).

Преамбула

Держави-члени Ради Європи, які підписали цю Конвенцію,

враховуючи, що метою Ради Європи є досягнення більшого єднання між її членами на основі поваги до верховенства права, а також прав людини і основоположних свобод;

зважаючи на доцільність поширення гарантій прав і основоположних свобод кожної людини, і зокрема, права на повагу до особистого життя, з огляду на зростання транскордонного потоку персональних даних, які піддаються автоматизованій обробці;

підтверджуючи в той же час свою відданість свободі інформації незалежно від кордонів;

визнаючи необхідність узгодження основоположних цінностей поваги до особистого життя та безперешкодного обміну інформацією між народами;

погодились про таке:

Глава I - Загальні положення

Стаття 1 - Предмет і мета

Метою цієї Конвенції є забезпечення на території кожної Сторони для кожної особи, незалежно від її громадянства або місця проживання, поваги її прав і основоположних свобод, і зокрема її права на особисте життя, у зв’язку з автоматизованою обробкою персональних даних, що її стосуються (“захист даних”).

Стаття 2 - Визначення

Для цілей цієї Конвенції:

a) “персональні дані” означають будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною (“суб’єкт даних”);

b) “файл даних для автоматизованої обробки” означає будь-який масив даних, що піддається автоматизованій обробці;

c) “автоматизована обробка” включає такі операції, що здійснюються повністю або частково за допомогою автоматизованих засобів: зберігання даних, виконання логічних та/або арифметичних операцій з цими даними, їх зміни, знищення, вибірка або поширення;

d) “контролер файлу” означає фізичну чи юридичну особу, державний орган, установу або будь-який інший орган, що уповноважений відповідно до внутрішнього законодавства вирішувати, якими повинні бути цілі файлу даних для автоматизованої обробки, які категорії персональних даних мають зберігатися та які операції мають здійснюватися з ними.

Стаття 3 - Сфера застосування

1. Сторони зобов’язуються застосовувати цю Конвенцію до файлів персональних даних для автоматизованої обробки та до автоматизованої обробки персональних даних у державному та приватному секторах.

2. Будь-яка держава або Європейські співтовариства під час підписання або здачі на зберігання своїх ратифікаційних грамот або своїх документів про прийняття, затвердження чи приєднання або в будь-який інший час після цього можуть повідомити заявою на ім’я Генерального секретаря Ради Європи про те, що вони:

а) не застосовуватимуть цю Конвенцію до певних категорій файлів персональних даних для автоматизованої обробки, перелік яких буде зданий на зберігання. Однак у цей перелік вони не включають категорій файлів даних для автоматизованої обробки, які згідно з їх внутрішнім правом підпадають під дію положень про захист даних. Відповідним чином, вони вносять поправки до цього переліку новою заявою у випадках, коли згідно з їх внутрішнім правом під дію положень про захист даних підпадають нові категорії файлів персональних даних для автоматизованої обробки;

б) застосовуватимуть також цю Конвенцію до інформації, яка стосується груп осіб, асоціацій, фундацій, компаній, корпорацій та будь-яких інших установ, що безпосередньо чи опосередковано складаються з окремих осіб, незалежно від того, чи мають такі установи правосуб’єктність, чи ні;

в) застосовуватимуть також цю Конвенцію до файлів персональних даних, які не піддаються автоматизованій обробці ***(Поправки Комітету Міністрів Ради Європи від 15.06.99 р. “Про умови приєднання держав-членів Європейських Співтовариств до Конвенції Ради Європи № 108 від 28.01.1981 р.” (далі – Поправки КМ РЄ від 15.06.99 р.)).***

3. Будь-яка держава або Європейські співтовариства, що поширили сферу застосування цієї Конвенції будь-якою із заяв, передбачених у підпункті 2в або е) вище, можуть повідомити у згаданій заяві, що таке поширення дії Конвенції стосується лише певних категорій файлів персональних даних, перелік яких буде зданий на зберігання ***(Поправки КМ РЄ від 15.06.99 р.).***

4. Будь-яка Сторона, яка шляхом заяви, передбаченої у підпункті 2.а вище, виключила зі сфери застосування цієї Конвенції певні категорії файлів персональних даних для автоматизованої обробки, не може вимагати застосування Конвенції до таких категорій Стороною, яка не виключила їх зі сфери застосування цієї Конвенції.

5. Відповідним чином, Сторона, яка не поширила сферу застосування Конвенції, як це передбачено у підпунктах 2.b і с вище, не може вимагати застосування цієї Конвенції по цих пунктах стосовно Сторони, яка у такий спосіб поширила сферу її застосування.

6. Заяви, передбачені у пункті 2 вище набирають чинності з моменту набрання чинності Конвенцією стосовно держави чи Європейських Співтовариств, які їх зробили, якщо такі заяви були зроблені під час підписання або здачі на зберігання їх ратифікаційних грамот або документа про прийняття, затвердження чи приєднання, або через три місяці після їхнього отримання Генеральним секретарем Ради Європи, якщо вони були зроблені в будь-який інший час після цього. Такі заяви можуть бути відкликані повністю або частково шляхом подання відповідного повідомлення на ім’я Генерального секретаря Ради Європи. Відкликання набирають чинності через три місяці від дати отримання такого повідомлення ***(Поправки КМ РЄ від 15.06.99 р.).***

Глава II - Основоположні принципи захисту даних

Стаття 4 - Обов’язки Сторін

1. Кожна Сторона в межах свого законодавства вживає необхідних заходів з метою запровадження основоположних принципів захисту персональних даних, викладених у цій главі.

2. Такі заходи вживаються не пізніше моменту набрання чинності цією Конвенцією для відповідної Сторони.

Стаття 5 - Якість даних

Персональні дані, що піддаються автоматизованій обробці:

a) отримуються та обробляються сумлінно та законно;

b) зберігаються для визначених і законних цілей та не використовуються у спосіб, несумісний з цими цілями;

c) мають бути адекватними, відповідними і не надмірними з точки зору цілей, для яких вони зберігаються;

d) мають бути точними та у разі необхідності мають поновлюватися;

e) зберігаються у форматі, який дозволяє ідентифікувати суб’єктів даних не довше, ніж це необхідно для цілі, для якої такі дані зберігаються.

Стаття 6 - Особливі категорії даних

Персональні дані, що свідчать про расову приналежність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров’я або статевого життя, не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство не забезпечує відповідних гарантій. Це правило застосовується також до персональних даних, що стосуються засудження у кримінальному порядку.

Стаття 7 - Безпека даних

Для захисту персональних даних, що зберігаються у файлах даних для автоматизованої обробки, вживаються відповідні заходи безпеки, спрямовані на запобігання випадковому чи несанкціонованому знищенню або випадковій втраті, а також на запобігання несанкціонованому доступу, зміні або поширенню.

Стаття 8 - Додаткові гарантії для суб’єкта даних

Будь-якій особі надається можливість:

a) встановлювати існування файлу персональних даних для автоматизованої обробки, його головні цілі, а також особу та постійне місце проживання чи головне місце роботи контролера файлу;

b) отримувати через розумні проміжки часу та без надмірної затримки або витрат підтвердження або спростування факту зберігання персональних даних, що її стосуються, у файлі даних для автоматизованої обробки, а також отримувати такі дані у доступній для розуміння формі;

c) вимагати у відповідних випадках виправлення або знищення таких даних, якщо вони оброблялися всупереч положенням внутрішнього законодавства, що запроваджують основоположні принципи, визначені у статтях 5 і 6 цієї Конвенції;

d) використовувати засоби правового захисту у разі невиконання передбаченого у пунктах b і c цієї статті прохання про підтвердження або у відповідних випадках про надання, виправлення або знищення персональних даних.

Стаття 9 - Винятки та обмеження

1. Винятки з положень статей 5, 6 і 8 цієї Конвенції дозволяються лише в межах, визначених цією статтею.

2. Відхилення від положень статей 5, 6 і 8 цієї Конвенції дозволяється у випадках, коли таке відхилення передбачається законодавством Сторони та є у демократичному суспільстві необхідним заходом, спрямованим на:

a) захист державної та громадської безпеки, фінансових інтересів Держави або на боротьбу із кримінальними правопорушеннями;

b) захист суб’єкта даних або прав і свобод інших людей.

3. Обмеження щодо здійснення прав, визначених у пунктах b, c і d статті 8, можуть встановлюватися законодавством стосовно файлів персональних даних для автоматизованої обробки, що використовуються для цілей статистики або наукових досліджень, у випадках явної відсутності небезпеки порушення недоторканості особистого життя суб’єктів даних.

Стаття 10 - Санкції та засоби правового захисту

Кожна Сторона зобов’язується передбачити відповідні санкції та засоби правового захисту від порушень положень внутрішнього права, що запроваджують основоположні принципи захисту персональних даних, визначені у цій главі.

Стаття 11 - Розширення захисту

Жодне з положень цієї глави не тлумачиться як таке, що обмежує або іншим чином перешкоджає можливості Сторони забезпечувати суб’єктам даних більший ступінь захисту, ніж передбачений цією Конвенцією.

Глава III - Транскордонні потоки даних

Стаття 12 - Транскордонні потоки персональних даних та внутрішнє законодавство

1. Стосовно передачі через національні кордони за допомогою будь-яких засобів персональних даних, що піддаються автоматизованій обробці або зібраних з метою їхньої автоматизованої обробки, застосовуються наступні положення.

2. Сторона не може лише з метою захисту недоторканості особистого життя забороняти або зумовлювати спеціальними дозволами транскордонні потоки персональних даних, що передаються на територію іншої Сторони.

3. Незважаючи на це, кожна Сторона має право відступати від положень пункту 2:

a) якщо її законодавство містить конкретні положення для певних категорій персональних даних або файлів персональних даних для автоматизованої обробки, у зв’язку з особливостями цих даних або файлів, за винятком випадків, коли положення іншої Сторони забезпечують аналогічний захист;

b) якщо передача даних здійснюється з її території на територію Держави, що не є Договірною Державою, через територію іншої Сторони, для запобігання порушенню такою передачею законодавства Сторони, згаданої на початку цього пункту.

Глава IV - Взаємна допомога

Стаття 13 - Співробітництво між Сторонами

1. Сторони погоджуються надавати одна одній взаємну допомогу з метою імплементації цієї Конвенції.

2. Для цього:

a) кожна Сторона призначає один або більше органів, назву та адресу яких вона повідомляє Генеральному секретарю Ради Європи;

b) кожна Сторона, яка призначила більше одного органу, зазначає у своєму повідомленні, згаданому в попередньому підпункті, сферу повноважень кожного з них.

3. Орган, призначений однією Стороною, на прохання органу, призначеного іншою Стороною:

a) надає інформацію про своє законодавство та адміністративну практику у галузі захисту даних;

b) відповідно до свого внутрішнього законодавства та виключно з метою захисту недоторканості особистого життя, вживає всіх відповідних заходів для надання фактичної інформації щодо конкретної автоматизованої обробки, яка здійснюється на його території, але за винятком персональних даних, що обробляються.

Стаття 14 - Допомога суб’єктам даних, які проживають за кордоном

1. Кожна Сторона надає допомогу будь-якій особі, яка постійно проживає за кордоном, у здійсненні прав, наданих її внутрішнім законодавством, що запроваджує принципи, визначені у статті 8 цієї Конвенції.

2. Якщо така особа проживає на території іншої Сторони, їй надається можливість подати своє прохання за посередництвом органу, призначеного цією Стороною.

3. Прохання про надання допомоги має містити всі необхідні відомості, що стосуються, між іншим:

a) прізвища, адреси та будь-яких інших відповідних відомостей, які встановлюють особу, що звертається із проханням;

b) файлу персональних даних для автоматизованої обробки, якого стосується прохання, або його контролера;

c) мети прохання.

Стаття 15 - Гарантії стосовно допомоги, що надається призначеними органами

1. Орган, призначений Стороною, який отримав від органу, призначеного іншою Стороною, інформацію, що супроводжує прохання про надання допомоги, або інформацію у відповідь на його власне прохання про надання допомоги, використовує цю інформацію лише для цілей, зазначених у проханні про надання допомоги.

2. Кожна Сторона забезпечує, щоб особи, які працюють у призначеному органі або діють від його імені, мали відповідні зобов’язання щодо збереження таємності або конфіденційності такої інформації.

3. Призначеному органу на свій власний розсуд і без ясно вираженої згоди суб’єкта даних, що проживає за кордоном, у жодному випадку не дозволяється звертатися згідно з пунктом 2 статті 14 із проханням про надання допомоги від імені відповідної особи.

Стаття 16 - Відхилення прохань про надання допомоги

Призначений орган, до якого направлено прохання про надання допомоги згідно зі статтями 13 або 14 цієї Конвенції, може відмовитися задовольняти таке прохання, тільки якщо:

a) прохання є несумісним із повноваженнями, якими наділені у галузі захисту персональних даних органи, що відповідають за виконання прохання;

b) прохання не відповідає положенням цієї Конвенції;

c) виконання прохання може порушити суверенітет, безпеку або громадський порядок Сторони, якою він був призначений, або права та основні свободи осіб, які знаходяться під юрисдикцією цієї Сторони.

Стаття 17 - Витрати на допомогу та порядок її надання

1. Взаємна допомога, яку Сторони надають одна одній згідно зі статтею 13, та допомога, яку вони надають згідно зі статтею 14 суб’єктам даних, що проживають за кордоном, не може бути підставою для сплати жодних витрат або зборів, за винятком тих, що сплачуються у зв’язку з діяльністю експертів і тлумачів. Витрати або збори у зв’язку з діяльністю останніх сплачуються Стороною, яка призначила орган, що звертається із проханням про надання допомоги.

2. На суб’єкта даних не може покладатися сплата витрат або зборів, пов’язаних із заходами, що були вжиті від його імені на території іншої Сторони, крім витрат або зборів, які на законних підставах сплачуються резидентами такої Сторони.

3. Інші деталі положення щодо надання допомоги, що стосуються, зокрема, форм і процедур, а також використання мов, визначаються безпосередньо між відповідними Сторонами.

Глава V - Консультативний комітет

Стаття 18 - Склад Комітету

1. Консультативний комітет створюється після набрання чинності цією Конвенцією.

2. Кожна Сторона призначає в Комітет одного представника та заступника представника. Будь-яка Держава-член Ради Європи, яка не є Стороною Конвенції, має право бути представленою в Комітеті спостерігачем.

3. Консультативний комітет одностайним рішенням може запропонувати будь-якій Державі, яка не є членом Ради Європи і не є Стороною Конвенції, бути представленою на тому чи іншому засіданні в якості спостерігача.

Стаття 19 - Функції Комітету

Консультативний комітет:

a) може вносити пропозиції з метою сприяння або покращення застосування Конвенції;

b) може вносити пропозиції щодо внесення змін та доповнень до цієї Конвенції відповідно до статті 21;

c) надає свій висновок щодо будь-якої пропозиції про внесення змін та доповнень до цієї Конвенції, які передаються йому на розгляд відповідно до пункту 3 статті 21;

d) на прохання Сторони може робити висновок з будь-якого питання, що стосується застосування цієї Конвенції.

Стаття 20 - Процедура

1. Консультативний комітет скликається Генеральним секретарем Ради Європи. Його перше засідання відбувається протягом дванадцяти місяців після набрання чинності цією Конвенцією. У подальшому він збирається щонайменше один раз на два роки і у будь-якому разі, коли одна третина представників Сторін вимагає його скликання.

2. Кворум засідання Консультативного комітету складає більшість представників Сторін.

3. Кожна сторона має право голосувати. Кожна держава, яка є Стороною для Конвенції, має один голос. Стосовно питань у межах їх повноважень Європейські Співтовариства здійснюють своє право голосувати і підраховувати кількість голосів, що дорівнює числу держав-членів, які є Сторонами цієї Конвенції і передали свої повноваження Європейським Співтовариствам у цій сфері. В такому разі ці держави-члени Співтовариства не голосують, а інші держави-члени можуть це робити. Європейські Співтовариства не голосують, коли розглядаються питання, які не входять до їх повноважень ***(Поправки КМ РЄ від 15.06.99 р.).***

4. Після кожного свого засідання Консультативний комітет подає Комітету Міністрів Ради Європи доповідь про свою роботу та про стан виконання Конвенції.

5. Відповідно до положень цієї Конвенції, Консультативний комітет складає свій власний регламент.

Глава VI - Зміни

Стаття 21 - Зміни

1. Зміни та доповнення до цієї Конвенції можуть пропонуватися Стороною, Комітетом Міністрів Ради Європи або Консультативним комітетом.

2. *Будь-яка пропозиція про внесення поправки надсилається Генеральним секретарем Ради Європи державам-членам Ради Європи, Європейським Співтовариствам та кожній державі, що не є членом Ради, яка приєдналася до цієї Конвенції або якій було запропоновано приєднатися до неї у відповідності до положень Статті 23* ***(Поправки КМ РЄ від 15.06.99 р.)***

3. Будь-які зміни, запропоновані Стороною або Комітетом Міністрів, надсилається Консультативному комітету, який подає Комітету Міністрів свої висновки щодо цих запропонованих змін.

4. Комітет Міністрів розглядає запропоновані зміни та будь-які висновки, подані Консультативним комітетом, і може затвердити зміни.

5. Текст будь-якої зміни, затверджений Комітетом Міністрів відповідно до пункту 4 цієї статті, надсилається Сторонам для прийняття.

6. Будь-які зміни, затверджені відповідно до пункту 4 цієї статті, набирають чинності на тридцятий день після того, як усі Сторони поінформували Генерального секретаря про їх прийняття.

Глава VII - Заключні положення

Стаття 22 - Набуття чинності

1. Ця Конвенція відкрита для підписання Державами-членами Ради Європи. Вона підлягає ратифікації, прийняттю або схваленню. Ратифікаційні грамоти або документи про прийняття чи схвалення здаються на зберігання Генеральному секретарю Ради Європи.

2. Ця Конвенція набуває чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати, на яку п’ять Держав-членів Ради Європи висловили свою згоду на обов’язковість для них цієї Конвенції відповідно до положень попереднього пункту.

3. Для будь-якої Держави-члена, яка згодом висловить свою згоду на обов’язковість для неї цієї Конвенції, вона набирає чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати здачі на зберігання ратифікаційної грамоти або документа про прийняття чи схвалення.

Стаття 23 - Приєднання Держав, що не є членами Ради Європи

1. Після набрання цією Конвенцією чинності Комітет Міністрів Ради Європи може запропонувати будь-якій державі, яка не є членом Ради Європи, приєднатися до цієї Конвенції у рішенні, що приймається більшістю голосів, передбаченою у статті 20 d Статуту Ради Європи та одностайним голосуванням представників Договірних держав, які мають право засідати в Комітеті.

2. Європейські Співтовариства можуть приєднатися до цієї Конвенції.

3. Стосовно будь-якої держави, що приєдналася до цієї Конвенції, чи Європейських Співтовариств, що можуть приєднатися, Конвенція набирає чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати здачі на зберігання документа про приєднання Генеральному секретарю Ради Європи ***(Поправки КМ РЄ від 15.06.99 р.)***

Стаття 24 – Територіальні положення

1. Будь-яка держава або Європейські Співтовариства під час підписання або здачі на зберігання своїх ратифікаційних грамот або своїх документів про прийняття, затвердження чи приєднання можуть визначити територію чи території, до яких застосовуватиметься ця Конвенція.

2. Будь-яка держава чи Європейські Співтовариства можуть в будь-який інший час після цього заявою на ім’я Генерального секретаря Ради Європи поширити дію цієї Конвенції на будь-яку іншу територію, визначену в цій заяві. Щодо такої території Конвенція набирає чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати отримання такої заяви Генеральним секретарем ***(Поправки КМ РЄ від 15.06.99 р.)***

Стаття 25 - Застереження

Жодне застереження щодо положень цієї Конвенції не дозволяється.

Стаття 26 - Денонсація

1. Будь-яка Сторона може в будь-який час денонсувати цю Конвенцію шляхом подання відповідного повідомлення на ім’я Генерального секретаря Ради Європи.

2. Така денонсація набирає чинності в перший день місяця, що настає після закінчення шестимісячного періоду від дати отримання такого повідомлення Генеральним секретарем.

Стаття 27 - Повідомлення

Генеральний секретар Ради Європи повідомляє держави-члени Ради Європи, Європейські Співтовариства та будь-яку державу, що приєдналася до цієї Конвенції, про:

а) будь-яке підписання;

б) здачу на зберігання ратифікаційної грамоти або будь-якого документа про прийняття, затвердження чи приєднання;

в) будь-яку дату набрання чинності цієї Конвенції відповідно до статей 22, 23 та 24;

г) будь-яку іншу дію, будь-яке повідомлення або сповіщення, які стосуються цієї Конвенції ***(Поправки КМ РЄ від 15.06.99 р.)***

Вчинено у Страсбурзі 28 дня січня місяця 1981 року, англійською та французькою мовами, причому обидва тексти є однаково автентичними, в одному примірнику, який зберігатиметься в архівах Ради Європи. Генеральний секретар Ради Європи надсилає завірені копії цієї Конвенції кожній Державі-члену Ради Європи та будь-якій Державі, якій було запропоновано приєднатися до цієї Конвенції.

Рада Європи, Страсбург, 28 січня 1981 року.

*** * * * * * ***

Офіційний переклад
засвідчено Міністерством закордонних справ України від 01.07.02 р.

Додатковий протокол до Конвенції Ради Європи № 108 від 8 листопада 2001 року “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних”

(Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows).

Преамбула

Сторони в цьому Додатковому протоколі до Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних, відкритої для підписання в Страсбурзі 28 січня 1981 року (далі – “Конвенція”),

переконані у тому, що органи нагляду, виконуючи свої функції у повній незалежності, є елементом ефективного захисту осіб у зв’язку з обробкою персональних даних,

виходячи із важливості обміну інформацією між народами,

вважаючи, що із збільшенням обміну персональними даними через національні кордони, необхідно гарантувати ефективний захист прав людини та фундаментальних свобод, зокрема, право на недоторканість особистого життя стосовно таких обмінів персональними даними,

погодились із наступним:

Стаття 1 - Органи нагляду

1. Кожна Сторона призначає один або більше органів нагляду, відповідальний за забезпечення принципів, які містяться у її внутрішньодержавному праві, що втілюють принципи, викладені у Розділах II та III Конвенції, та в цьому Протоколі.

2. a. З цією метою вищезазначений 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, що втілюють принципи, викладені у пункті 1 статті 1 цього Протоколу.

b. Кожний орган нагляду розглядає та приймає рішення щодо заяв будь-якої особи відносно захисту його/її прав і основоположних свобод відносно обробки персональних даних, в межах своєї компетенції.

3. Органи нагляду виконують свої функції у повній незалежності.

4. Рішення органу нагляду можна оскаржити у суді у разі, якщо вони викликали скарги.

5. Відповідно до положень Розділу IV, та не впливаючи на положення Статті 13 Конвенції, органи нагляду співробітничаю між собою в тій мірі, наскільки це необхідно для виконання їхніх обов’язків, зокрема, шляхом обміну будь-якою корисною інформацією.

Стаття 2 - Транскордонні потоки персональних даних до користувачів, які не підпадають під юрисдикцію Сторони Конвенції

1. Кожна Сторона передбачає, що передача персональних даних користувачеві, що знаходиться під юрисдикцією Держави чи організації, які не є Стороною Конвенції, може відбуватися, тільки якщо така Держава чи організація забезпечує адекватний рівень захисту відповідної передачі даних.

2. Відходячи від положень пункту 1 статті 2 цього Протоколу, кожна Сторона може дозволити передачу персональних даних:

a. якщо внутрішньодержавне право забезпечує це у зв’язку з:

- специфічними інтересами суб’єкту даних, або
- перевагою законних інтересів, в особливості важливих суспільних інтересів, або

b. якщо гарантії, що, зокрема, можуть походити з договірних положень, надаються контролером, відповідним за передачу, та визнаються достатніми компетентними органами відповідно до внутрішньодержавного права.

Стаття 3 - Заключні положення

1. Сторони вважають положення статей 1 та 2 цього Протоколу додатковими статтями Конвенції, і усі положення Конвенції застосовуються відповідно.

2. Цей Протокол відкритий для підписання Державами, що підписали Конвенцію. Після приєднання до Конвенції на умовах, передбачених нею, Держави-члени Європейських Співтовариств можуть підписати цей Протокол. Цей Протокол підлягає ратифікації, прийняттю або затвердженню. Сторона, яка підписала цей Протокол, не може його ратифікувати, прийняти або схвалити, якщо вона раніше чи одночасно ратифікувала, прийняла, схвалила чи приєдналася до Конвенції. Документи про ратифікацію, прийняття, затвердження чи приєднання до цього Протоколу передаються на зберігання Генеральному секретарю Ради Європи.

3. a. Цей Протокол набуває чинність в перший день місяця, що настає після закінчення тримісячного періоду від дати, на яку п’ять Держав, що підписали його, висловили свою згоду на обов’язковість для них цього Протоколу відповідно до положень пункту 2 статті 3.

b. Для будь-якої Держави, що підписала цей Протокол, і згодом висловила свою згоду на обов’язковість для неї цього Протоколу, він набуває чинність в перший день місяця, що настає після закінчення тримісячного періоду від дати передачі на зберігання документу про ратифікацію, прийняття чи затвердження.

4. a. Після набуття чинності цим Протоколом будь-яка Держава, що приєдналася до Конвенції, може також приєднатися до Протоколу.

b. Приєднання відбувається шляхом передачі на зберігання Генеральному секретарю Ради Європи документа про приєднання, який набуває чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати його передачі на зберігання.

5. a. Будь-яка Сторона може в будь-який час денонсувати цей Протокол шляхом відповідного повідомлення на ім’я Генерального секретаря Ради Європи.

b. Така денонсація набирає чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати отримання такого повідомлення Генеральним секретарем.

6. Генеральний секретар Ради Європи повідомляє Держави-члени Ради Європи, Європейських Співтовариств та будь-яку іншу Державу, що приєдналась до цього Протоколу, про:

a. будь-яке підписання;

b. здачу на зберігання або будь-якої документа про ратифікацію, прийняття, затвердження;

c**.** будь-яку дату набуття чинності цим Протоколом відповідно до статті 3;

d. будь-яку іншу дію або повідомлення, які стосуються цього Протоколу.

На посвідчення чого нижчепідписані, належним чином на те уповноважені представники підписали цей Протокол.

Вчинено в Страсбурзі 8 дня листопада місяця 2001 року, англійською та французькою мовами, причому обидва тексти є однаково автентичними, в одному примірнику, який зберігатиметься в архівах Ради Європи. Генеральний секретар Ради Європи надсилає завірені копії кожній Державі-члену Ради Європи, Європейських Співтовариств та будь-якій іншій Державі, якій було запропоновано приєднатися до Конвенції.

Рада Європи, Страсбург, 8 листопада 2001 року.

*** * * * * * ***

Неофіційний переклад

Директива 95/46/ЄС Європейського Парламенту і Ради Європейського Союзу від 24 жовтня 1995 року

“Про захист осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних”

Європейський Парламент і Рада Європейського Союзу,

Беручи до уваги Договір про заснування Європейського Співтовариства, зокрема його статтю 100 a,

Беручи до уваги пропозицію Комісії [1],

Беручи до уваги висновок Економічного і Соціального Комітету [2],

Діючи відповідно до процедури, викладеної в статті 189 b Договору [3],

(1) Враховуючи, що цілі Співтовариства, викладені в Договорі, з поправками, внесеними Договором про Європейський Союз, полягають у створенні дедалі тіснішого союзу серед народів Європи, заохоченні більш тісних відносин між державами, що входять до Співтовариства, забезпеченні економічного і соціального прогресу шляхом спільних дій, спрямованих на усунення бар’єрів, що розділяють Європу, підтримку постійного поліпшення умов життя його народів, збереження і зміцнення миру та свободи, а також на розвиток демократії, яка базується на правах, визнаних конституціями і законами держав-членів та Європейською Конвенцією про захист прав людини і основоположних свобод;

(2) Враховуючи, що системи обробки даних створені для служіння людині; враховуючи, що вони, незалежно від національності чи місця проживання фізичних осіб, повинні поважати їхні основні права і свободи, особливо право на невтручання в особисте життя, і сприяти економічному і соціальному прогресу, розширенню торгівлі і добробуту людей;

(3) Враховуючи, що створення і функціонування внутрішнього ринку, у якому згідно зі статтею 7(a) Договору гарантується вільне пересування товарів, осіб, послуг і капіталів, вимагає не тільки можливості вільного переміщення персональних даних з однієї держави-члена в іншу, але й захисту прав людей;

(4) Враховуючи дедалі частіше застосування обробки персональних даних у Співтоваристві в різних сферах соціальної та економічної діяльності; враховуючи, що прогрес, досягнутий у сфері інформаційних технологій, значно полегшує обробку та обмін такими даними;

(5) Враховуючи, що економічна і соціальна інтеграція, досягнута в результаті створення і функціонування внутрішнього ринку в розумінні статті 7(a) Договору, неминуче призведе до істотного збільшення транскордонних потоків персональних даних між усіма тими, хто бере участь в економічному і соціальному житті держав-членів, як у приватному, так і в державному статусі; враховуючи, що обмін персональними даними між підприємствами різних держав-членів має розвиватися; враховуючи, що відповідно до права Співтовариства державні органи різних держав-членів повинні співпрацювати та обмінюватися персональними даними для того, щоб виконувати свої обов’язки і завдання від імені органів влади в іншій державі-члені в контексті простору без внутрішніх кордонів, який створюється внутрішнім ринком;

(6) Враховуючи, крім того, що збільшення науково-технічного співробітництва і узгоджене введення нових телекомунікаційних мереж у Співтоваристві роблять необхідним і полегшують здійснення транскордонних потоків персональних даних;

(7) Враховуючи, що розходження в рівні захисту прав і свобод фізичних осіб, що надають держави-члени, в особливості права на невтручання в особисте життя, при обробці персональних даних, може перешкоджати передачі таких даних з території однієї держави-члена на територію іншої держави-члена; враховуючи, що такі розходження до того ж можуть стати перешкодою в здійсненні певних видів економічної діяльності на рівні Співтовариства, негативно відбитися на конкуренції, перешкоджати владі у виконанні її зобов’язань згідно з правом Співтовариства; враховуючи, що такі розходження в рівні захисту викликані існуванням великої різноманітності національних законів, постанов і адміністративних положень;

(8) Враховуючи, що для усунення перешкод на шляху передачі персональних даних рівень захисту прав і свобод фізичних осіб при обробці цих даних повинен бути однаковим у всіх державах-членах; враховуючи, що ця мета, будучи життєво необхідною для внутрішнього ринку, не може бути досягнута державами-членами поодинці, особливо з урахуванням ступеня існуючих у даний час розходжень між відповідним законодавством держав-членів і необхідністю узгодження законів держав-членів для забезпечення єдиного підходу до регулювання транскордонних потоків персональних даних, тобто, дотримуючись цілей внутрішнього ринку, передбачених статтею 7(a) Договору; враховуючи, що в зв’язку з цим необхідні дії Співтовариства, спрямовані на зближення такого законодавства;

(9) Враховуючи, що при однаковому рівні захисту внаслідок зближення національних законодавств держави-члени більше не зможуть перешкоджати вільному пересуванню персональних даних між собою, посилаючись на обмеження, пов’язані із захистом прав і свобод фізичних осіб, а особливо права на невтручання в особисте життя; враховуючи, що державам-членам буде наданий певний ступінь свободи маневрування, який в контексті виконання Директиви може також використовуватись діловими і соціальними партнерами; враховуючи, що держави-члени в такий спосіб зможуть уточнити у своєму національному законодавстві загальні умови, що регулюють законність обробки даних; враховуючи, що при цьому держави-члени будуть прагнути поліпшити систему захисту, передбачену в їхньому законодавстві в даний час; враховуючи, що в межах певного ступеня свободи маневрування та відповідно до права Співтовариства можуть виникнути розбіжності в процесі здійснення Директиви, і це може вплинути на пересування даних як у державі-члені, так і в Співтоваристві;

(10) Враховуючи, що метою національного законодавства про обробку персональних даних є захист прав і свобод, а особливо права на невтручання в особисте життя, що визнається як статтею 8 Європейської конвенції про захист прав і основоположних свобод, так і загальними принципами права Співтовариства; враховуючи, що з цієї причини зближення згаданих законодавств не повинне призвести до зниження рівня наданого ними захисту, а навпаки, повинне прагнути забезпечити високий рівень захисту в Співтоваристві;

(11) Враховуючи, що принципи захисту прав і свобод фізичних осіб, а особливо права на невтручання в приватне життя, викладені в цій Директиві, уточнюють і посилюють принципи, викладені в Конвенції Ради Європи від 28 січня 1981 року “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних”;

(12)Враховуючи, що принципи захисту повинні застосовуватися до усіх випадків обробки персональних даних, здійснюваних будь-якою особою, чия діяльність регулюється правом Співтовариства; враховуючи, що ці принципи не поширюються на обробку даних, створених фізичною особою в процесі діяльності виняткового особистого чи домашнього характеру, такої як переписування і ведення адресних книг;

(13) Враховуючи, що діяльність, згадана в Розділах V і VI Договору про Європейський Союз, щодо суспільного порядку, оборони, державної безпеки чи діяльності держави в сфері кримінального законодавства, не входить до сфери дії права Співтовариства, без шкоди для зобов’язань, покладених на держави-члени згідно з параграфом 2 статті 56, статті 57 чи статті 100 Договору, що засновує Європейське Співтовариство; враховуючи, що обробка персональних даних, необхідна для захисту економічного добробуту держави, не входить до сфери дії цієї Директиви, у випадках, коли така обробка пов’язана з питаннями державної безпеки;

(14) Враховуючи, що з урахуванням важливості розвитку технологій, використовуваних для прийому, передачі, маніпуляцій, реєстрації, збереженні чи повідомленні звукових і візуальних даних, які стосуються фізичних осіб, який відбувається в інформаційному суспільстві, ця Директива повинна застосовуватися до обробки, що використовує такі дані;

(15) Враховуючи, що обробка таких даних підпадає під дію цієї Директиви лише в тих випадках, коли обробка є автоматизованою або коли оброблені дані розміщуються чи призначені для розміщення в картотеках, структурованих за визначеними критеріями, що стосуються фізичних осіб, таким чином, щоб забезпечити легкий доступ до відповідних персональних даних;

(16) Враховуючи, що обробка звукових і візуальних даних, таких як, наприклад, відеоспостереження, не відноситься до сфери дії цієї Директиви, якщо вона проводиться з метою суспільного порядку, оборони, державної безпеки чи в ході державної діяльності, що відноситься до сфери кримінального права, чи іншої діяльності, що не відноситься до сфери дії права Співтовариства;

(17) Враховуючи, що до випадків, коли обробка звукових і візуальних даних провадиться з метою журналістики чи літературної або художньої творчості, принципи Директиви повинні застосовуватися з обмеженнями відповідно до положень, викладених у статті 9;

(18) Враховуючи, що для того, щоб уникнути втрати фізичною особою захисту, на який вона має право згідно з цією Директивою, будь-яка обробка персональних даних у Співтоваристві повинна відбуватися відповідно до законодавства однієї з держав-членів; враховуючи, що в зв’язку з цим обробка, здійснена в межах юрисдикції контролера, створеного в державі-члені, повинна регулюватися законодавством цієї держави;

(19) Враховуючи, що створення такого органу на території держави-члена передбачає ефективне і реальне ведення діяльності на основі постійних домовленостей; враховуючи, що правова форма такої установи, незалежно від того є воно простою філією чи представництвом – суб’єктом права, не є вирішальним чинником у цьому відношенні; враховуючи, що при створенні єдиного контролера на території декількох держав-членів, зокрема, шляхом створення представництв, для запобігання порушення національних правил, він повинен забезпечити виконання своїми установами зобов’язань, накладених на них національним законодавством, що застосовується до його діяльності;

(20) Враховуючи той факт, що обробка даних проводиться особою, яка перебуває в третій країні, не повинен перешкоджати захисту фізичних осіб, передбаченому цією Директивою; враховуючи, що в таких випадках обробка даних повинна регулюватися законами держави-члена, у якому розташовані використовувані засоби, і повинні існувати гарантії для забезпечення дотримання на практиці прав і обов’язків, передбачених цією Директивою;

(21) Враховуючи, що ця Директива не завдає шкоди правилам територіальності, застосовуваним у кримінальних справах;

(22) Враховуючи, що держави-члени більш точно визначають у законах, що приймаються, а також при здійсненні заходів на виконання цієї Директиви, загальні умови, за яких обробка даних є законною; враховуючи, що, зокрема, стаття 5 у сполученні зі статтями 7 і 8 дозволяє державам-членам незалежно від загальних правил передбачати особливі умови обробки даних для певних секторів і для різних категорій даних, зазначених у статті 8;

(23) Враховуючи, що держави-члени уповноважені забезпечити здійснення захисту фізичних осіб шляхом прийняття як загального закону про захист фізичних осіб при обробці персональних даних, так і галузевих законів, таких як ті, що стосуються, наприклад, статистичних установ;

(24) Враховуючи, що законодавство про захист юридичних осіб при обробці даних, що їх стосуються, не зачіпається цією Директивою;

(25) Враховуючи, що принципи захисту повинні бути відображені, з одного боку, у зобов’язаннях, що накладаються на осіб, на державні органи влади, підприємства, агентства чи інші органи, які відповідають за обробку, зокрема в тому, що стосується якості даних, технічної безпеки, повідомлення наглядових органів, і обставин, при яких може проводитися обробка, та, з іншого боку, у праві, яким наділені фізичні особи, чиї дані підлягають обробці, знати, що обробка дійсно проводиться, звертатися до даних, вимагати внесення змін і навіть заперечувати проти обробки за певних обставин;

(26) Враховуючи, що принципи захисту повинні застосовуватися до будь-яких даних, що стосується встановленої особи чи особи, яку можна встановити; враховуючи, що для визначення того, чи можна особу встановити, повинні враховуватися всі засоби, використання яких контролером чи якою-небудь іншою особою ймовірно очікувати для встановлення вище згаданої особи; враховуючи, що принципи захисту не застосовуються до даних, що надані анонімно таким чином, що суб’єкт даних не може бути встановлений; враховуючи, що кодекси поведінки в значенні статті 27 можуть бути корисним знаряддям для забезпечення керівництва

щодо способів анонімного надання даних і їхнього збереження у формі, що забезпечує неможливість встановлення особи суб’єкта даних;

(27) Враховуючи, що захист фізичних осіб повинен застосовуватися як до автоматизованої обробки даних, так і до ручної обробки; враховуючи, що масштаби захисту не повинні залежати від використовуваних методів, бо інакше це створить загрозу обходу закону; враховуючи, що, незважаючи на це, у тому що стосується ручної обробки, ця Директива охоплює тільки картотеки даних, але не неструктуровані справи; враховуючи, що, зокрема, зміст картотеки повинен бути структурований відповідно до визначених критеріїв щодо фізичних осіб, що забезпечувало б легкий доступ до персональних даних; враховуючи, що, відповідно до визначення в статті 2 (c), різні критерії визначення складових частин структурованої сукупності персональних даних і різні критерії управління доступом до такої сукупності можуть бути встановлені кожною державою-членом; враховуючи, що справи чи зібрання справ, як і їхні титульні аркуші, що не розроблені відповідно до визначених критеріїв, за жодних обставин не входять до сфери дії цієї Директиви;

(28) Враховуючи, що будь-яка обробка персональних даних повинна бути законною і справедливою по відношенню до фізичних осіб, яких вона безпосередньо стосується; враховуючи, що, зокрема, дані повинні бути достовірними, відповідними і не надмірними з точки зору цілей, заради яких проводиться їхня обробка; враховуючи, що ці цілі повинні бути чіткими і законними і повинні бути визначені на час збору даних; враховуючи, що цілі обробки даних, яка проводиться після збору даних, не повинні бути несумісними із цілями, визначеними спочатку;

(29) Враховуючи, що подальша обробка персональних даних в історичних, статистичних чи наукових цілях не повинна розглядатися як несумісна з цілями, заради яких дані були зібрані раніше, за умови, що держави-члени забезпечать відповідні гарантії; враховуючи, що ці гарантії повинні, зокрема, виключати використання даних на підтримку заходів чи рішень відносно будь-якої конкретної особи;

(30) Враховуючи, що для забезпечення законності обробки персональних даних, вона повинна, крім іншого, проводитися з дозволу суб’єкта даних чи бути необхідною для укладання чи виконання договору, обов’язкового для суб’єкта даних, або в якості правової вимоги, або для виконання завдання, яке здійснюється в інтересах суспільства чи при виконанні офіційних повноважень, або в законних інтересах фізичної чи юридичної особи, за умови, що враховуються інтереси чи права і свободи суб’єкта даних; враховуючи, що, зокрема, для того, щоб зберегти рівновагу між інтересами, які зачіпаються, в той же час гарантуючи ефективну конкуренцію, держави-члени можуть визначити обставини, при яких персональні дані можуть використовуватися чи надаватися третій стороні в контексті законної звичайної ділової діяльності компаній і інших органів; враховуючи, що держави-члени можуть аналогічним чином визначити умови, за яких персональні дані можуть надаватися третій стороні з метою маркетингу, здійснюваного або в комерційних цілях, або благодійною організацією чи будь-якою іншою асоціацією чи фондом, наприклад, політичного характеру, за умови дотримання положень, що дозволяють суб’єкту даних безкоштовно і без зазначення причин заперечувати проти обробки даних, які його стосуються;

(31) Враховуючи, що обробка персональних даних повинна розглядатися законною, якщо вона проводитися з метою захисту інтересу, який є надзвичайно важливим для життя суб’єкта даних;

(32) Враховуючи, що питання про те, чи повинен контролер, який виконує завдання в інтересах суспільства чи при виконанні офіційних повноважень, бути державним органом або іншою фізичною чи юридичною особою, що регулюється публічним правом чи приватним правом, такою як професійне об’єднання, повинне визначатися національними законодавствами;

(33) Враховуючи, що дані, які за своєю природою можуть порушити основні свободи і таємницю приватного життя, не повинні оброблятися доти, доки суб’єкт даних не дасть своєї згоди; враховуючи, що, незважаючи на це, відступ від даної заборони повинен бути чітко викладений з огляду на особливі потреби, зокрема, якщо обробка цих даних проводиться у певних цілях, пов’язаних із здоров’ям, особами, які зв’язані правовим зобов’язанням зберігати професійну таємницю, або під час законної діяльності певних асоціацій чи фондів, метою яких є дозволити здійснення свобод;

(34) Враховуючи, що держави-члени повинні бути також уповноважені, якщо це виправдовується важливим суспільним інтересом, відступати від заборони обробляти конфіденційні категорії даних, якщо це пов’язано із суспільними інтересами в таких сферах, як охорона суспільного здоров’я і соціальний захист, особливо з метою гарантування якості і рентабельності процедур, що використовуються під час врегулювання позовів про виплату допомоги і надання послуг у системі страхування здоров’я, а також у сфері наукових досліджень і урядової статистики; враховуючи, що, незважаючи на це, вони зобов’язані забезпечувати особливі і відповідні гарантії, спрямовані на захист прав і приватного життя людей;

(35) Враховуючи, що, крім того, обробка персональних даних, яка здійснюється офіційними органами для досягнення цілей, встановлених у конституційному праві чи в міжнародному публічному праві, офіційно визнаних релігійних об’єднань здійснюється на важливих підставах суспільного інтересу;

(36) Враховуючи, що якщо в ході виборчої діяльності функціонування демократичної системи в деяких державах-членах вимагає від політичних партій збору даних про політичні погляди людей, обробка таких даних може бути дозволена на важливих підставах суспільного інтересу, за умови створення відповідних гарантій;

(37) Враховуючи, що обробка персональних даних для цілей журналістики чи художньої або літературної творчості, зокрема в аудіовізуальному секторі, повинна підлягати звільненню від вимог, викладених у деяких положеннях цієї Директиви, у тій мірі, в якій це необхідно для узгодження прав людини зі свободою інформації і особливо з правом одержувати і передавати інформацію, яке гарантується, передусім, статтею 10 Європейської Конвенції про захист прав і основоположних свобод; враховуючи, що, виходячи з цього, держави-члени повинні визначити винятки і відступи, необхідні для досягнення балансу між правами в тому, що стосується загальних заходів щодо законності обробки даних, заходів для передачі даних третім країнам і повноважень наглядового органу; враховуючи, однак, що це не повинно призвести до того, що держави-члени встановлять винятки відносно заходів із забезпечення безпеки обробки; враховуючи, що, принаймні, наглядовий орган, відповідальний за цю галузь, повинен також бути наділений певними апостеріорними повноваженнями, наприклад, видавати регулярний звіт чи передавати справи судовим органам;

(38) Враховуючи, що для того, щоб обробка даних була справедливою, суб’єкт даних повинен мати змогу дізнатися про існування факту обробки і, якщо дані отримані від нього, повинен одержати точну і повну інформацію з урахуванням обставин збору даних;

(39) Враховуючи, що деякі випадки обробки стосуються даних, які контролер одержав не від суб’єкта даних безпосередньо; враховуючи, крім того, що дані можуть бути відкриті законним шляхом третій стороні, навіть якщо це не було передбачено під час збору даних у суб’єкта; враховуючи, що у всіх цих випадках суб’єкт даних повинен бути проінформований про це тоді, коли дані записуються чи пізніше, коли вони вперше розкриваються третій стороні;

(40) Враховуючи, однак, що дане зобов’язання не обов’язково накладати, якщо суб’єкт даних вже має необхідну інформацію; враховуючи, що, крім того, дане зобов’язання не накладається, якщо запис чи розкриття третій стороні будуть чітко передбачені законом або якщо надання інформації суб’єкту даних виявиться неможливим чи зажадає непропорційних зусиль, що може відбутися у випадку, коли обробка даних проводитися в історичних, статистичних чи наукових цілях; враховуючи, що при цьому може враховуватися число суб’єктів даних, вік даних і будь-які затверджені компенсаційні заходи;

(41) Враховуючи, що будь-яка особа повинна мати можливість використати право доступу до даних, які стосуються і перебувають в обробці, з метою їхньої перевірки, особливо перевірки точності і законності обробки; враховуючи, що з тих же причин кожен суб’єкт даних повинен також мати право знати логіку, застосовувану при автоматизованій обробці даних, які його стосуються, принаймні у випадку з автоматизованими рішеннями, про які йде мова в пункті 1 статті 15; враховуючи, що це право не повинне негативно впливати на торгові секрети чи інтелектуальну власність і, зокрема, на авторське право, що захищає програмне забезпечення; враховуючи, що, незважаючи на це, врахування цих факторів не повинне призвести до відмови суб’єкту даних у наданні всієї інформації;

(42) Враховуючи, що держави-члени можуть в інтересах суб’єкта даних чи з метою захисту прав і свобод інших осіб обмежити права на доступ і на інформування; враховуючи, що вони, наприклад, можуть прийняти рішення, що доступ до медичних даних може бути отриманий тільки через медичного працівника;

(43) Враховуючи, що обмеження прав на доступ і інформування та обмеження інших зобов’язань контролера можуть бути встановлені державами-членами в тій мірі, в якій вони необхідні для захисту, наприклад, національної безпеки, оборони, суспільної безпеки чи важливих економічних і фінансових інтересів держави-члена, а також у карних розслідуваннях, переслідуваннях і діях у зв’язку з порушенням етики встановлених професій; враховуючи, що перелік винятків і обмежень повинен включати задачі моніторингу, інспекції чи регулювання, що необхідні в трьох останніх із згаданих сфер відносно суспільної безпеки, економічних чи фінансових інтересів і попередження злочинності; враховуючи, що перерахування задач у цих трьох сферах не впливає на законність винятків чи обмежень, встановлених із причин державної безпеки чи оборони;

(44) Враховуючи, що держави-члени можуть бути змушені, на підставі положень права Співтовариства, відступати від положень цієї Директиви в тому, що стосується права доступу, зобов’язання інформувати фізичних осіб, якості даних; з метою виконання вищезгаданих цілей;

(45) Враховуючи, що у випадках, коли дані можуть оброблятися законним шляхом на підставі суспільного інтересу, офіційних повноважень чи законних інтересів фізичної або юридичної особи, будь-який суб’єкт даних повинен, незважаючи на це, мати право на законних і незаперечних підставах, що стосуються його конкретної ситуації, опротестувати обробку будь-яких даних, які його стосуються; враховуючи, що, незважаючи на це, держави-члени можуть передбачити протилежні національні положення;

(46) Враховуючи, що захист прав і свобод суб’єктів даних при обробці персональних даних вимагає прийняття відповідних технічних й організаційних заходів як при розробці системи обробки, так і під час самої обробки, зокрема для забезпечення безпеки і, таким чином, запобігання будь-якій незаконній обробці; враховуючи, що держави-члени повинні забезпечити дотримання контролерами таких заходів; враховуючи, що ці заходи повинні забезпечити відповідний рівень безпеки, з огляду на існуюче положення речей і вартість їхньої реалізації з урахуванням пов’язаного з обробкою ризику і характеру даних, що підлягають захисту;

(47) Враховуючи, що, у тих випадках, коли повідомлення, що містить персональні дані, передається за допомогою телекомунікацій чи електронної пошти, єдиною метою яких є передача таких повідомлень, контролером у відношенні персональних даних, які містяться в повідомленні, буде вважатися особа, від якої виходить це повідомлення, а не особа, що надає послуги з передачі повідомлень; враховуючи, що, незважаючи на це, особи, що надають ці послуги, будуть, як правило, вважатися контролерами у зв’язку з обробкою додаткових персональних даних, необхідних для надання цієї послуги;

(48) Враховуючи, що процедури повідомлення наглядового органу покликані забезпечити розкриття цілей і принципів будь-якого процесу обробки для перевірки того, що процес здійснюється відповідно до національних заходів, прийнятих відповідно до цієї Директиви;

(49) Враховуючи, що для того, щоб уникнути непотрібних адміністративних формальностей, звільнення від зобов’язання повідомляти і спрощення необхідного повідомлення можуть бути передбачені державами-членами у випадках, коли обробка навряд чи може завдати шкоди правам і свободам суб’єктів даних, і за умови, що вона проводиться відповідно до прийнятої державою-членом міри, що визначає її рамки; враховуючи, що звільнення чи спрощення можуть бути передбачені державами-членами за умови, що особа, призначена контролером, гарантує, що здійснена обробка даних навряд чи може завдати шкоди правам і свободам суб’єктів даних; враховуючи, що такий службовець із захисту даних незалежно від того, чи є він співробітником інституту контролера чи ні, повинен мати можливість виконувати свої функцій абсолютно незалежно;

(50) Враховуючи, що звільнення чи спрощення може бути передбачене у випадках із процесами обробки, єдиною метою яких є ведення реєстру, що відповідно до національного законодавства, призначений для надання інформації населенню і є відкритим для звертань населення чи будь-якої особи, що демонструє законний інтерес;

(51) Враховуючи, що, незважаючи на це, спрощення чи звільнення від зобов’язання повідомляти не звільняє контролера від жодних інших зобов’язань, що випливають з цієї Директиви;

(52) Враховуючи, що в цьому контексті апостеріорна перевірка компетентними органами в цілому повинна розглядатися як достатній захід;

(53) Враховуючи, що, незважаючи на це, при деяких процесах обробки існує ймовірність певних ризиків для прав і свобод суб’єктів даних в силу їхньої природи, їхнього обсягу чи їхніх цілей, як, наприклад, позбавлення фізичних осіб права, допомоги чи контракту, або через особливе використання нових технологій; враховуючи, що держави-члени за власним бажанням визначають ці ризики у своєму законодавстві;

(54) Враховуючи, що з урахуванням усіх процесів обробки, що здійснюються в суспільстві, кількість процесів, які створюють такий особливий ризик, повинна бути обмеженою; враховуючи, що держави-члени повинні передбачити, що наглядовий орган чи службовець із захисту даних разом з органом перевіряють таку обробку до її виконання; враховуючи, що після проведення такої попередньої перевірки наглядовий орган у відповідності із своїм національним законодавством дає свій висновок чи дозвіл на здійснення обробки; враховуючи, що така перевірка може в однаковій мірі відбуватися в ході підготовки або законодавчого заходу національного парламенту, або заходу, що базується на такому законодавчому заході, що визначає природу обробки і встановлює відповідні гарантії;

(55) Враховуючи, що у випадку порушення контролером прав суб’єктів даних, національне законодавство повинне передбачити судовий спосіб захисту; враховуючи, що будь-яка шкода, що може бути завдана людині в результаті незаконної обробки даних, повинна відшкодовуватися контролером, який може бути звільнений від відповідальності, якщо доведе, що він не є відповідальним за цю шкоду, зокрема у випадках, коли він встановлює наявність провини суб’єкта даних чи за форс-мажорних обставин; враховуючи, що санкції повинні застосовуватися до будь-якої особи, незалежно від того, керуються вони приватним чи публічним правом, якщо вона не виконує національних заходів, прийнятих відповідно до цієї Директиви;

(56) Враховуючи, що транскордонні потоки персональних даних необхідні для розширення міжнародної торгівлі; враховуючи, що захист фізичних осіб, гарантований у Співтоваристві цією Директивою, не перешкоджає передачі персональних даних третім країнам, що забезпечують адекватний рівень захисту; враховуючи, що адекватність рівня захисту, наданого третіми країнами, повинна оцінюватися у світлі всіх обставин, пов’язаних із процесом передачі чи сукупністю процесів передачі;

(57) Враховуючи, що з одного боку, передача персональних даних третій країні, що не забезпечує адекватний рівень захисту, повинна бути заборонена;

(58) Враховуючи, що повинні бути прийняті положення, які передбачають винятки з такої заборони при визначених обставинах: коли суб’єкт даних дав свою згоду, коли передача даних необхідна для контракту чи права вимоги, коли того вимагає захист важливого суспільного інтересу, наприклад, у випадках міжнародної передачі даних між податковими і митними органами чи між службами, що відповідають за питання соціального забезпечення, або коли передача даних здійснюється з реєстру, що створений відповідно до закону і призначений для консультацій населення чи осіб, що мають законний інтерес; враховуючи, що в цьому випадку така передача даних не повинна включати всі дані чи всі категорії даних, що містяться в реєстрі, і оскільки реєстр призначений для звертання осіб, що мають законний інтерес, передача даних повинна здійснюватися тільки на прохання цих осіб чи у випадку, якщо вони будуть одержувачами даних;

(59) Враховуючи, що можуть бути застосовані особливі заходи, спрямовані на компенсацію відсутності захисту в третій країні, у випадках, коли контролер пропонує відповідні гарантії; враховуючи, що, крім того, повинні бути передбачені положення відносно порядку переговорів між Співтовариством і такими третіми країнами;

(60) Враховуючи, що, в будь-якому випадку передача даних третій країні може здійснюватися тільки в повній відповідності до положень, прийнятих державами-членами відповідно до цієї Директиви, зокрема її статті 8;

(61) Враховуючи, що держави-члени і Комісія в межах своїх повноважень повинні заохочувати профспілкові об’єднання та інші зацікавлені представницькі організації до складання кодексів поведінки для того, щоб сприяти в застосуванні цієї Директиви, беручи до уваги особливі характеристики обробки даних, що проводиться у визначених галузях, і дотримуючись національних положень, прийнятих з метою виконання цієї Директиви;

(62) Враховуючи, що створення в державах-членах наглядових органів, що наділені повною незалежністю у виконанні своїх функцій, є істотним елементом захисту фізичних осіб при обробці персональних даних;

(63) Враховуючи, що такі органи повинні мати необхідні засоби для виконання своїх обов’язків, включаючи повноваження із розслідування і втручання, зокрема у випадках скарг фізичних осіб, і повноваження брати участь у судових розглядах; враховуючи, що такі органи повинні сприяти забезпеченню прозорості обробки в державах-членах, до юрисдикції яких вони належать;

(64) Враховуючи, що органи влади різних держав-членів повинні допомагати одна одній у виконанні своїх обов’язків для того, щоб забезпечити дотримання правил захисту на належному рівні на всій території Європейського Союзу;

(65) Враховуючи, що на рівні Співтовариства повинна бути створена Робоча група із захисту фізичних осіб при обробці даних, що буде абсолютно незалежною у виконанні своїх функцій; враховуючи, що беручи до уваги її особливий характер, вона повинна консультувати Комісію і сприяти однаковому застосуванню національних правил, прийнятих відповідно до цієї Директиви;

(66) Враховуючи, що в питаннях передачі даних третім країнам застосування даної Директиви робить необхідним надання Комісії виконавчих повноважень і встановлення процедури, передбаченої Рішенням Ради 87/373/ЄЕС [4];

(67) Враховуючи, що 20 грудня 1994 року було досягнуто тимчасової згоди між Європейським Парламентом, Радою та Комісією про заходи із виконання актів, прийнятих відповідно до процедури, викладеної в статті 189 b Договору ЄС;

(68) Враховуючи, що викладені в цій Директиві принципи щодо захисту прав і свобод фізичних осіб, особливо їхнього права на невтручання в приватне життя, при обробці персональних даних, можуть бути доповнені чи уточнені, зокрема, це стосується певних галузей, визначених правилами, що базуються на цих принципах;

(69) Враховуючи, що державам-членам повинен надаватися період часу, що не перевищує трьох років з моменту набуття чинності національними заходами, що впроваджують цю Директиву, для послідовного застосування таких нових національних правил до всіх процесів обробки, що уже ведуться; враховуючи, що для полегшення їхньої рентабельної реалізації державам-членам надаватиметься подальший період, що закінчується через 12 років з дати прийняття цієї Директиви, для забезпечення відповідності існуючих неавтоматизованих картотек до деяких положень Директиви; враховуючи, що, якщо дані, що містяться в таких картотеках, обробляються вручну в період цього подовженого перехідного періоду, ці картотеки повинні приводитись у відповідність до цих положень під час такої обробки;

(70) Враховуючи, що суб’єкту даних не потрібно повторно давати свою згоду для того, щоб дозволити контролеру після набуття чинності національними положеннями, прийнятими відповідно до цієї Директиви, продовжити обробку будь-яких чутливих даних, необхідних для виконання контракту, укладеного на основі вільної та поінформованої згоди до набуття чинності такими положеннями;

(71) Враховуючи, що ця Директива не перешкоджає державам-членам у регулюванні маркетингової діяльності, орієнтованої на споживачів, що проживають на їхній території, у тій мірі, в якій таке регулювання не стосується захисту фізичних осіб при обробці персональних даних;

(72) Враховуючи, що ця Директива дозволяє враховувати принцип громадського доступу до офіційних документів при здійсненні принципів, викладених у цій Директиві,

ПРИЙНЯЛИ ТАКУ ДИРЕКТИВУ:

Розділ I. Загальні положення

Стаття 1. Ціль Директиви

1. Відповідно до цієї Директиви, держави-члени захищають основні права і свободи фізичних осіб і, особливо, їхнє право на невтручання в особисте життя при обробці персональних даних.

2. Держави-члени не обмежують і не забороняють вільну передачу персональних даних між державами-членами на підставах, пов’язаних із захистом, що надається згідно з пунктом 1.

Стаття 2. Визначення

В цілях цієї Директиви:

(a) “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 опосередковано, зокрема, за допомогою ідентифікаційного коду або одного чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості;

(b) “обробка персональних даних” (“обробка”) означає будь-яку операцію чи сукупність операцій, здійснюваних з персональними даними (за допомогою чи без допомоги автоматизованих засобів), таких як збір, реєстрація, організація, зберігання, адаптація чи зміна, пошук, консультація, використання, розкриття за допомогою передачі, поширення чи іншого надання, упорядкування чи комбінування, блокування, стирання чи знищення;

(c) “картотека персональних даних” (“картотека”) означає будь-який структурований масив персональних даних, що є доступними за визначеними критеріями, незалежно від того, чи є такий масив централізованим, децентралізованим або розділеним на функціональних або географічних засадах;

(d) “контролер” означає фізичну чи юридичну особу, державний орган, агентство або будь-який інший орган, який окремо чи разом з іншими визначає цілі та засоби обробки персональних даних; якщо цілі та засоби обробки визначені законодавчими чи нормативними положеннями держави чи Співтовариства, контролер або особливі критерії його призначення можуть визначатися правом держави чи Співтовариства;

(e) “оператор обробки даних” означає фізичну чи юридичну особу, державний орган, агентство чи будь-який інший орган, що обробляє персональні дані від імені контролера;

(f) “третя сторона” означає будь-яку фізичну чи юридичну особу, державний орган, агентство чи будь-який інший орган, інший ніж суб’єкт даних, контролер, оператор обробки даних і особи, що, будучи безпосередньо підпорядкованими контролеру чи оператору обробки даних, уповноважені обробляти дані;

(g) “одержувач” означає фізичну чи юридичну особу, державний орган, агентство чи будь-який інший орган, якому надаються дані, незалежно до того, третя особа це чи ні; однак, органи, що можуть одержувати дані в рамках окремого запиту, не розглядаються як одержувачі;

(h) “згода суб’єкта даних” означає будь-яке вільно виражене спеціальне і поінформоване зазначення його бажань, за допомогою якого суб’єкт даних дає свою згоду на обробку персональних даних, які його стосуються.

Стаття 3. Сфера застосування

1. Ця Директива застосовується до обробки персональних даних за допомогою повного чи часткового використання автоматизованих засобів, а також до обробки неавтоматичними засобами персональних даних, що є частиною картотеки чи призначені для внесення в картотеку.

2. Ця Директива не застосовується до обробки персональних даних:

- протягом діяльності, що не входить у сферу дії права Співтовариства такої як діяльність, передбачена Розділами V і VI Договору про Європейський Союз і, у будь-якому випадку, до операцій із обробки даних, що стосуються суспільної безпеки, оборони, державної безпеки (включаючи економічний добробут держави, якщо процес обробки стосується питань державної безпеки) і діяльності держави в сфері кримінального права;
- якщо вона проводиться фізичною особою під час діяльності виключно особистого чи побутового характеру.

Стаття 4. Застосовуване національне законодавство

1. Кожна держава-член застосовує національні положення, які вона приймає до обробки відповідно до цієї Директиви:

(a) обробка здійснюється в контексті діяльності установи контролера на території держави-члена; якщо ж один і той самий контролер заснований на території декількох держав-членів, він повинен вжити всіх необхідних заходів для забезпечення того, що кожна з цих установ дотримується зобов’язань, передбачених відповідним національним законодавством;

(b) контролер заснований не на території держави-члена, а у місці, де його національне законодавство застосовується відповідно до міжнародного публічного права;

(c) контролер не заснований на території Співтовариства, але з метою обробки 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 Співтовариства.

2. За обставин, передбачених у підпункті (c) пункту 1, контролер повинен призначити представника на території цієї держави-члена, без шкоди для судових позовів, що можуть бути подані проти самого контролера.

Розділ II. Загальні правила законності обробки даних

Стаття 5.

Держави-члени в рамках положень цього Розділу більш точно визначають умови, за яких обробка персональних даних є законною.

Підрозділ 1. Принципи, які стосуються якості даних

Стаття 6.

1. Держави-члени передбачають, що персональні дані повинні:

(a) оброблятися чесно і законно;

(b) збиратися для встановлених, чітких і законних цілей і надалі не оброблятися у спосіб, несумісний з цими цілями. Подальша обробка даних в історичних, статистичних чи наукових цілях не розглядається як несумісна, якщо держави-члени забезпечують відповідні гарантії;

(c) бути достовірними, відповідними і не надлишковими відносно цілей, заради яких вони збираються і/або надалі обробляються;

(d) бути точними і, якщо необхідно, обновлятися; слід вжити 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;

(e) 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.

2. Забезпечення дотримання пункту 1 покладається на контролера.

Підрозділ II. Критерії законності обробки даних

Стаття 7.

1. Держави-члени передбачають, що персональні дані можуть оброблятися тільки за умови, що:

(a) суб’єкт даних недвозначно дав свою згоду; чи

(b) обробка необхідна для виконання контракту, стороною якого є суб’єкт даних, чи для вживання заходів на прохання суб’єкта даних до підписання контракту; чи

(c) обробка необхідна для дотримання правового зобов’язання, яким зв’язаний контролер; чи

(d) обробка необхідна для захисту життєво важливих інтересів суб’єкта даних; чи

(e) обробка необхідна для виконання завдання, здійснюваного в суспільних інтересах, чи при виконанні офіційних повноважень, якими наділений контролер або третя сторона, якій надаються дані; чи

(f) обробка необхідна в цілях законних інтересів, що їх переслідують контролер чи третя сторона або сторони, для яких надаються дані, крім випадків, коли над такими інтересами переважають інтереси прав і свобод суб’єкта даних, що вимагають захисту згідно з пунктом 1 статті 1.

Підрозділ ІІІ. Особливі категорії обробки

Стаття 8. Обробка особливих категорій даних

1. Держави-члени забороняють обробку персональних даних, що вказують на расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання, профспілкове членство, і обробку даних, що стосуються здоров’я чи статевого життя людини.

2. Пункт 1 не застосовується, якщо:

(a) суб’єкт даних дав свою недвозначну згоду на обробку цих даних, крім випадків, коли законодавство держав-членів передбачає, що заборона, згадана в пункті 1, не може бути знята при наданні згоди з боку суб’єкта даних; чи

(b) обробка необхідна з метою виконання зобов’язань і особливих прав контролера в області законодавства про працевлаштування, у тій мірі, у якій це дозволено національним законодавством, що передбачає адекватні гарантії; чи

(c) обробка необхідна для захисту важливих інтересів суб’єкта даних чи іншої особи, якщо суб’єкт даних не може дати свою згоду через свою недієздатність чи неправоздатність; чи

(d) обробка проводиться в ході законної діяльності з відповідними гарантіями установою, асоціацією чи будь-яким іншим некомерційним органом у політичних, філософських, релігійних чи профспілкових цілях і за умови, що обробка стосується винятково членів цього органу чи людей, що у зв’язку з цими цілями перебувають у постійному контакті з ним, і що дані не надаються третій особі без згоди суб’єктів даних; чи

(e) обробка стосується даних, що явно оприлюднені суб’єктами даних, чи необхідна для порушення, виконання чи захисту судових позовів.

3. Пункт 1 не застосовується, якщо обробка даних необхідна з метою медичної профілактики, діагностики, надання медичних послуг чи лікування або для керування служб охорони здоров’я, і якщо ці дані обробляються працівником, що, відповідно до національного законодавства чи правил, встановлених національними компетентними органами, зв’язаний зобов’язанням збереження професійної таємниці, чи іншою особою, що зв’язана подібним зобов’язанням.

4. За умови надання відповідних гарантій держави-члени можуть на важливій підставі суспільного інтересу встановлювати винятки на додачу до тих, що передбачені в пункті 2, за допомогою національного закону, або рішення наглядового органу.

5. Обробка даних, що стосуються правопорушень, обвинувачення у кримінальних справах чи засобів безпеки, може проводитися тільки під контролем офіційного органу або якщо національне законодавство передбачає відповідні спеціальні гарантії, з винятками, що можуть бути надані державою-членом відповідно до національних положень, що передбачають відповідні спеціальні гарантії. Однак повний реєстр обвинувачень у кримінальних справах може вестися лише під контролем офіційного органу.

Держави-члени можуть передбачити, що дані про адміністративні санкції чи про судові рішення в цивільних справах також повинні оброблятися під контролем офіційного органу.

6. Відступи від пункту 1, передбачені у пунктах 4 і 5, доводяться до відома Комісії.

7. Держави-члени визначають умови, за яких може оброблятися національний ідентифікаційний код чи будь-який інший ідентифікатор загального застосування.

Стаття 9. Обробка персональних даних і свобода самовираження

Держави-члени передбачають винятки чи відступи від положень цього Розділу, Розділу IV і Розділу VI у тому, що стосується обробки персональних даних, яка проводиться виключно для цілей журналістики або художньої чи літературної творчості за умови, що вони необхідні, для узгодження права на невтручання в особисте життя з нормами, що регулюють свободу самовираження.

Підрозділ IV. Інформація, що надається суб’єкту даних

Стаття 10. Інформація у разі збору даних від суб’єкта даних

Держави-члени передбачають, що контролер чи його представник повинні надати суб’єкту даних, у якого збираються дані щодо нього самого, принаймні наступну інформацію, крім тих випадків, коли в нього вже є ця інформація:

(a) особа контролера і його представника, якщо такий є;

(b) цілі обробки, для якої призначені дані;

(c) будь-яка додаткова інформація, як наприклад:

- одержувачі чи категорії одержувачів даних,
- обов’язковість чи добровільність відповіді на питання, а також можливі наслідки за ненадання відповіді,
- існування права доступу і права на виправлення даних, які його стосуються у тій мірі, в якій така додаткова інформація необхідна з огляду на особливі обставини, за яких дані збираються, для гарантії справедливої обробки у відношенні суб’єкта даних обробки.

Стаття 11. Інформація у разі, якщо дані не були отримані від суб’єкта даних

1. У випадку, якщо дані не були отримані від суб’єкта даних, держави-члени передбачають, що контролер чи його представник повинні 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:

(a) особа контролера і його представника, якщо такий є;

(b) цілі обробки;

(c) будь-яка додаткова інформація, як наприклад:

- категорії використовуваних даних;
- одержувачі чи категорії одержувачів;
- існування права доступу і права на виправлення даних, які його стосуються у тій мірі, в якій така додаткова інформація необхідна з огляду на особливі обставини, за яких дані обробляються, для гарантії справедливої обробки у відношенні суб’єкта даних обробки.

2. Пункт 1 не застосовується в певних випадках, зокрема при обробці 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 цих випадках держави-члени надають відповідні гарантії.

Підрозділ V. Право суб’єкта даних на доступ до даних

Стаття 12. Право доступу

Держави-члени гарантують кожному суб’єкту даних право отримати від контролера:

(a) без обмежень через розумні інтервали часу і без надмірної затримки або витрат:

- підтвердження того, обробляються чи ні дані, які його стосуються, та інформацію, принаймні, про цілі обробки, категорії розглянутих даних і про одержувачів чи категорії одержувачів, яким надаються дані;
- повідомлення йому в зрозумілій формі про те, що дані знаходяться в процесі обробки, і будь-яку іншу доступну інформацію щодо їхнього джерела;

- інформацію про логіку, використану під час автоматизованої обробки даних, що його стосуються, принаймні, у випадку автоматизованих рішень, згаданих у статті 15 (ї);

(b) в залежності від випадку виправлення, стирання чи блокування даних, обробка яких не відповідає положенням цієї Директиви, зокрема через неповноту чи неточність даних;

(c) повідомлення третім сторонам, яким були надані дані, про будь-яке виправлення, стирання чи блокування, виконане відповідно до підпункту (b), якщо це можливо чи не вимагає непропорційних зусиль.

Підрозділ VI. Винятки та обмеження

Стаття 13. Винятки та обмеження

1. Держави-члени можуть вживати законодавчих заходів для обмеження обсягів обов’язків і прав, передбачених у статтях 6 (1), 10, 11 (1), 12 і 21, якщо таке обмеження є необхідним, щоб гарантувати:

(a) національну безпеку;

(b) оборону;

(c) суспільну безпеку;

(d) запобігання розслідування, виявлення і судове переслідування кримінальних злочинів чи порушень етики визначених професій;

(e) важливий економічний чи фінансовий інтерес держави-члена чи Європейського Союзу, включаючи монетарні, бюджетні і податкові питання;

(f) моніторинг, перевірку чи регулятивну функцію, пов’язану, навіть зрідка, з виконанням офіційних повноважень у випадках, вказаних у підпунктах (c), (d) і (e);

(j) захист суб’єкта даних чи прав і свобод інших осіб.

2. За умови виконання відповідних правових гарантій, зокрема того, що дані не використовуються для вживання заходів чи прийняття рішень щодо будь-якої конкретної людини, держави-члени можуть, за явної відсутності якого-небудь ризику втручання в особисте життя, обмежити шляхом законодавчого заходу права, передбачені в статті 12, якщо дані обробляються виключно з метою наукових досліджень чи зберігаються в особовій формі протягом періоду, що не перевищує період часу, необхідного лише для цілі створення статистики.

Підрозділ VII. Право суб’єкта даних на заперечення

Стаття 14. Право суб’єкта даних на заперечення

Держави-члени надають суб’єкту даних право:

(a) принаймні у випадках, передбачених у підпунктах (e) і (f) статті 7, заперечувати в будь-який час на безсумнівних законних підставах, пов’язаних з його конкретною ситуацією, проти обробки даних, які його стосуються, за винятком випадків, коли інше передбачено національним законодавством. За наявності обґрунтованого заперечення в розпочатій контролером обробці більше не можуть використовуватися такі дані;

(b) заперечувати за вимогою і безкоштовно проти обробки персональних даних, що його стосуються і які контролер має намір обробити з метою прямого маркетингу, чи бути проінформованим до того, як персональні дані будуть вперше надаватися третім особам чи використовуватися від їхнього імені з метою прямого маркетингу, при цьому йому чітко пропонується право на безкоштовне заперечення проти такого надання чи використання даних.

Держави-члени вживають необхідних заходів для забезпечення того, щоб суб’єкти даних були інформовані про існування права, про яке йдеться в першій частині підпункту (b).

Стаття 15. Автоматизовані індивідуальні рішення

1. Держави-члени надають кожній особі право на те, щоб стосовно неї не приймалося рішення, що має для неї правові наслідки чи значною мірою зачіпає та яке ґрунтується винятково на автоматизованій обробці даних, призначеній для оцінки деяких його особистісних характеристик, як наприклад, виконання нею професійних обов’язків, кредитоспроможності, надійності поведінки і т. д.

2 . Відповідно до інших статей цієї Директиви держави-члени передбачають, що стосовно особи може бути прийняте рішення, про яке йдеться в пункті 1, якщо це рішення:

(a) прийняте в ході укладання чи виконання контракту, за умови, що прохання про укладання чи виконання контракту, подане суб’єктом даних, було задоволене або існують відповідні заходи для захисту його законних інтересів, як, наприклад, заходи, що дозволяють йому виразити свою точку зору; чи

(b) санкціоноване законом, що також передбачає заходи для захисту законних інтересів суб’єкта даних.

Підрозділ VIII. Конфіденційність і безпека обробки

Стаття 16. Конфіденційність обробки

Будь-яка особа, яка діє у підпорядкуванні контролера чи оператора обробки, включаючи самого оператора обробки, який має доступ до персональних даних, не повинні обробляти їх інакше, як за вказівкою контролера, за винятком тих випадків, коли це вимагається законом.

Стаття 17. Безпека обробки

1. 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 обробка включає передачу даних через мережу, і від усіх інших незаконних форм обробки.

Такі заходи, із урахуванням нинішнього стану речей і вартості їхнього здійснення, повинні забезпечувати рівень безпеки, співвідносний з ризиком, що супроводжує обробку, і з природою даних, що захищаються.

2. Держави-члени передбачають, що контролер повинен, у випадку обробки від свого імені, вибрати оператора обробки, що надає достатні гарантії щодо технічних заходів безпеки і організаційних заходів, що регулюють обробку, яка має проводитись, і повинен забезпечити виконання цих заходів.

3. Здійснення обробки за допомогою оператора обробки даних повинне регулюватися договором чи правовим актом, яким оператор обробки даних підпорядковується контролеру і який передбачає, зокрема, наступне:

- оператор обробки даних повинен діяти тільки за вказівками контролера;
- зобов’язання, викладені в пункті 1 і визначені законодавством держави-члена, у якому призначений оператор обробки даних, повинні також застосовуватися до оператора обробки.

4. З метою збереження доказів розділи договору чи юридичного акту про захист даних і вимоги про заходи, згадані у пункті 1, повинні бути викладені в письмовій формі чи в іншій тотожній формі.

Підрозділ IX. Повідомлення

Стаття 18. Зобов’язання повідомляти наглядовий орган

1. Держави-члени передбачають, що контролер чи його представник, якщо такий існує, повинні повідомити наглядовий орган, згаданий у статті 28, про обробку до проведення будь-якої повної чи часткової автоматизованої операції з обробки даних чи сукупності таких операцій, призначених служити єдиній цілі чи декільком взаємозалежним цілям.

2. Держави-члени можуть передбачити спрощення чи звільнення від повідомлення тільки в наступних випадках і за наступних умов:

- якщо для категорій операцій з обробки, які, беручи до уваги дані, що будуть оброблятися, навряд чи можуть завдати шкоди правам і свободам суб’єктів даних, вони визначають цілі обробки даних, дані чи категорії даних, які проходять обробку, категорію чи категорії суб’єктів даних, одержувачів чи категорії одержувачів, яким будуть надані дані, і період часу, протягом якого дані будуть зберігатися, і/чи

- якщо контролер відповідно до національного права, яким він керується, призначає посадову особу із захисту персональних даних, що, серед іншого, відповідає за наступне:
- забезпечення у незалежний спосіб внутрішнього застосування національних положень, прийнятих на виконання цієї Директиви;
- ведення реєстру операцій із обробки, що проводиться контролером і містить інформацію, згадану в пункті 2 статті 21.

3. Держави-члени можуть передбачити, що пункт 1 не застосовується до обробки, єдиною метою якої є ведення реєстру, що, відповідно до законодавчих чи нормативних положень, призначений для надання інформації громадськості і відкритий для консультування або населення в цілому, або будь-якої особи, що проявляє законний інтерес.

4. Держави-члени можуть передбачити звільнення від зобов’язання щодо повідомлення чи спрощення системи повідомлення у випадку здійснення операцій із обробки, про які йдеться в підпункті (d) пункту 2 статті 8.

5. Держави-члени можуть повідомляти про неавтоматизовані операції із обробки з персональними даними, або передбачити спрощений порядок повідомлення про ці операції.

Стаття 19. Зміст повідомлення

1. Держави-члени визначають інформацію, що повинна міститися в повідомленні. Вона повинна включати, принаймні, наступне:

(a) ім’я та адресу контролера і його представника, якщо такий є;

(b) ціль чи цілі обробки;

(c) опис категорії чи категорій суб’єктів даних або категорій їхніх персональних даних;

(d) одержувачів чи категорії одержувачів, яким можуть надаватися дані;

(e) передачі даних, що передбачаються, третім країнам;

(f) загальний опис, що дозволяє зробити попередню оцінку відповідності заходів, прийнятих згідно із статтею 17, для забезпечення безпеки обробки.

2. Держави-члени встановлюють процедури, згідно з якими наглядовий орган повинен бути сповіщений про будь-яку зміну, що зачіпає інформацію, згадану в пункті 1.

Стаття 20. Попередня перевірка

1. Держави-члени визначають операції із обробки, що можуть мати певний ризик для прав і свобод суб’єктів даних, і перевіряють, щоб ці операції із обробки вивчалися до початку обробки.

2. Такі попередні перевірки здійснюються наглядовим органом після одержання повідомлення від контролера чи посадової особи з питань захисту даних, який при виникненні сумнівів повинні радитися з наглядовим органом.

3. Держави-члени можуть також проводити такі перевірки у зв’язку з підготовкою законодавчого заходу національного парламенту або заходу, що базується на такому законодавчому заході і визначає характер обробки та встановлює відповідні гарантії.

Стаття 21. Оголошення операцій із обробки

1. Держави-члени вживають заходів для забезпечення оголошуються операцій із обробки.

2. Держави-члени передбачають, що наглядовий орган повинен вести реєстр операцій із обробки, повідомлення про які відбувається згідно із статтею 18. Реєстр повинен містити, принаймні, інформацію, перераховану в підпунктах (a) – (e) пункту 1 статті 19. Будь-яка особа може перевірити такий реєстр.

3. Держави-члени передбачають у відношенні операцій із обробки, що контролери чи інші органи, призначені державами-членами, надають після запиту будь-якої особи у відповідній формі, принаймні, інформацію, перераховану в підпунктах (a) – (e) пункту 1 статті 19.

Держави-члени можуть передбачити, що це положення не застосовується до обробки, єдиною метою якої є ведення реєстру, що згідно із законодавчим чи нормативним положенням передбачає надання інформації населенню і який відкритий для консультування або для населення в цілому, або для будь-якої особи, що може довести свій законний інтерес.

Розділ III. Засоби судового захисту, відповідальність та санкції

Стаття 22. Засоби захисту

Без шкоди для будь-якого адміністративного засобу захисту, що може бути передбачений, у тому числі захисту наглядовим органом, згаданому в статті 28, до звертання в судовий орган, держави-члени передбачають право кожної людини на засоби судового захисту від будь-якого порушення прав, гарантованих їй національним законодавством, що застосовується до відповідної обробки.

Стаття 23. Відповідальність

1. Держави-члени передбачають, що будь-яка особа, якій завдано шкоди в результаті незаконної операції з обробки чи будь-якої дії, несумісної із національними положеннями, прийнятими відповідно до цієї Директиви, має право на одержання компенсації від контролера за завдану шкоду.

2. Контролер може бути звільнений від цієї відповідальності цілком чи частково, якщо він доведе, що не є відповідальним за випадок, що став причиною завданої шкоди.

Стаття 24. Санкції

Держави-члени вживають відповідних заходів для забезпечення повного виконання положень цієї Директиви і, зокрема, встановлюють санкції, що повинні накладатися у випадку порушення положень, прийнятих відповідно до цієї Директиви.

Розділ IV. Передача персональних даних третім країнам

Стаття 25. Принципи

1. Держави-члени передбачають, що передача третій країні персональних даних, що проходять обробку чи призначені для проходження обробки після передачі, може відбуватися за умови, що розглянута третя країна гарантує адекватний рівень захисту без шкоди для виконання національних положень, прийнятих відповідно до інших положень цієї Директиви.

2. Адекватність рівня захисту, наданого третьою країною, розглядається у світлі всіх обставин операції з передачі даних чи сукупності операцій з передачі даних; особливу увагу варто звернути на характер даних, ціль і тривалість запропонованої операції чи операцій із обробки, країну походження даних і країну кінцевого призначення даних, загальні і галузеві норми права, що діють у розглянутій третій країні, і професійні правила та заходи безпеки, що виконуються в цій країні.

3. Держави-члени та Комісія інформують одні одного про випадки, коли вони вважають, що третя країна не забезпечує адекватного рівня захисту, передбаченого пунктом 2.

4. Якщо Комісія дійде висновку, відповідно до процедури, передбаченої в статті 31 (2), що третя країна не забезпечує адекватного рівня захисту, передбаченого пунктом 2 даної статті, держави-члени вживають заходів, необхідних для запобігання будь-якій передачі даних цього ж виду відповідній третій країні.

5. У належний час Комісія проводить переговори з метою виправлення ситуації, що склалася в результаті виявлення фактів згідно з пунктом 4.

6. Згідно з процедурою, згаданою в пункті 2 статті 31, Комісія може дійти висновку, що третя країна забезпечує адекватний рівень захисту, передбаченого пунктом 2 цієї статті, керуючись своїм внутрішнім законодавством чи міжнародними зобов’язаннями, які вона взяла на себе, особливо після завершення переговорів, передбачених у пункті 5, щодо захисту особистого життя та прав і основоположних свобод.

Держави-члени вживають заходів, необхідних для виконання рішення Комісії.

Стаття 26. Відступи

1. Шляхом відступу від статті 25 і крім випадків, коли інше передбачено національним законодавством, що регулює особливі випадки, держави-члени передбачають, що передача чи сукупність передач персональних даних третій країні, яка не забезпечує адекватний рівень захисту, згаданий в пункті 2 статті 25, може відбуватися за умови, що:

(a) суб’єкт даних дав свою недвозначну згоду на пропоновану передачу даних; або

(b) передача даних необхідна для виконання контракту між суб’єктом даних і контролером чи для виконання заходів, що передують договору і прийняті у відповідь на прохання суб’єкта даних; або

(c) передача даних необхідна для укладення чи виконання контракту, укладеного в інтересах суб’єкта даних між контролером і третьою стороною; або передача даних необхідна чи юридично обов’язкова на важливих підставах суспільних інтересів, або для встановлення, виконання чи захисту правових вимог; або

(d) передача даних необхідна для захисту життєво важливих інтересів суб’єкта даних; або

(e) передача даних зроблена з реєстру, метою якого, відповідно до законів або положень, є надання інформації населенню і який відкритий для консультацій або населення в цілому, або будь-якої людини, що може продемонструвати законний інтерес, у тому обсязі, за якого умови, передбачені в законодавстві про консультацію, виконуються в особливому випадку.

2. Без шкоди для пункту 1, держава-член може дозволити передачу чи сукупність передач персональних даних третій країні, що не забезпечує адекватного рівня захисту, передбаченого в пункті 2 статті 25, якщо контролер надає відповідні гарантії із захисту невтручання в особисте життя та прав і свобод людей і в тому, що стосується здійснення відповідних прав; такі гарантії можуть, зокрема, стати результатом відповідних умов договору.

3. Держава-член повідомляє Комісію та інші держави-члени про дозволи, які вона дає відповідно до пункту 2.

Якщо член чи Комісія заперечують проти цього на обґрунтованих підставах, що стосуються захисту невтручання в особисте життя та прав і свобод людей, Комісія вживає відповідних заходів згідно з процедурою, передбаченою в пункті 2 статті 31.

Держави-члени вживають необхідних заходів для виконання рішення Комісії.

4. Якщо Комісія відповідно до процедури, передбаченої в пункті 2 статті 31, вирішує, що деякі стандартні умови договору пропонують достатні гарантії, як того вимагає пункт 2, держави-члени вживають необхідних заходів для виконання рішення Комісії.

Розділ V. Кодекси поведінки

Стаття 27.

1. Держави-члени і Комісія сприяють розробці кодексів поведінки, метою яких є сприяння належному виконанню національних положень, прийнятих державами-членами відповідно до цієї Директиви, з урахуванням характерних особливостей різних галузей.

2. Держави-члени передбачають, щоб профспілки та інші органи, що представляють інші категорії контролерів і які розробили проекти національних кодексів або які мають намір змінити чи доповнити існуючі національні кодекси, могли представити їх на розгляд державного органу.

Держави-члени передбачають, що такий орган повинен упевнитися, серед іншого, у тому, чи відповідають представлені проекти національним положенням, прийнятим відповідно до цієї Директиви. Якщо орган вважає це за необхідне, він може поцікавитися думкою суб’єктів даних чи їхніх представників.

3. Проекти кодексів Співтовариства і зміни та доповнення до існуючих кодексів Співтовариства можуть бути надані Робочій групі, згаданій в статті 29. Ця Робоча група визначає, серед іншого, чи відповідають надані проекти національним положенням, прийнятим відповідно до цієї Директиви. Якщо орган вважає це за необхідне, він може поцікавитися думкою суб’єктів даних чи їхніх представників. Комісія може забезпечити відповідне оприлюднення кодексів, схвалених Робочою групою.

Розділ VI. Наглядовий орган та Робоча група із захисту фізичних осіб при обробці персональних даних

Стаття 28. Наглядовий орган

1. Кожна держава-член передбачає, що один чи більше державних органів відповідають за моніторинг застосування в межах її території положень цієї Директиви.

Ці органи діють у повній незалежності при здійсненні функцій, якими вони наділені.

3. Кожна держава-член передбачає, що при розробці адміністративних заходів чи положень, що стосуються захисту прав і свобод фізичних осіб при обробці персональних даних, проводяться консультації з наглядовими органами.

Кожен орган, зокрема, наділений:

- такими слідчими повноваженнями, як право доступу до даних, що є предметом операцій із обробки, і право збирати всю інформацію, необхідну для виконання його обов’язків із здійснення нагляду;

- ефективними повноваженнями на втручання, як-от надання висновків до здійснення операцій із обробки відповідно до статті 20, і забезпечення відповідного опублікування таких висновків, видання розпоряджень про блокування, стирання чи знищення даних, накладення тимчасової чи остаточної заборони на обробку даних, попередження чи винесення догани контролеру, або повноваження звертатися до національних парламентів чи інших політичних інститутів;

- право брати участь у судочинстві, якщо були порушені національні положення, прийняті відповідно до цієї Директиви, чи довести ці порушення до відома судових органів.

Рішення наглядового органу, що викликали скарги, можуть бути оскаржені в суді.

4. Кожен наглядовий орган розглядає запити, зроблені будь-якою особою чи об’єднанням, що представляє інтереси цієї особи, про захист її прав і свобод при обробці персональних даних. Особа, якої це стосується, повинна бути поінформована про результати розгляду запиту.

Кожен наглядовий орган, зокрема, розглядає запити про перевірки законності обробки даних, зроблені будь-якою особою, у випадках, коли застосовуються національні положення, прийняті у відповідності до статті 13 цієї Директиви. Така особа повинна в будь-якому випадку бути поінформована про те, що перевірка мала місце.

5. Кожен наглядовий орган регулярно складає звіт про свою діяльність. Звіт повинен оприлюднюватись.

6. Кожен наглядовий орган має право, незалежно від того, яке національне законодавство застосовується до відповідної обробки, виконувати на території власної держави-члена повноваження, якими він наділений відповідно до пункту 3. Кожен орган може отримати прохання про виконання його повноважень від органу іншої держави-члена.

Наглядові органи співпрацюють один з одним у тій мірі, наскільки це необхідно для виконання їхніх обов’язків, зокрема, шляхом обміну всією корисною інформацією.

7. Держави-члени передбачають, що навіть після звільнення на посадових осіб і персонал наглядового органу поширюється обов’язок зберігати професійну таємницю відносно конфіденційної інформації, до якої вони мають доступ.

Стаття 29. Робоча група із захисту фізичних осіб при обробці персональних даних

1. Цим створюється Робоча група із захисту фізичних осіб при обробці персональних даних, надалі – Робоча група.

Вона має консультативний статус і незалежна у своїй діяльності.

2. Робоча група складається з представника наглядового органу чи органів, призначеного кожною державою-членом, і представника від органа чи органів, створених для установ і органів Співтовариства, а також представника Комісії.

Кожен член Робочої групи призначається установою, органом чи органами, які він представляє. Якщо держава-член створила більш ніж один наглядовий орган, вони призначають спільного представника. Ті ж самі положення повинні застосовуватися до органів, створених для установ і органів Співтовариства.

3. Робоча група приймає рішення простою більшістю представників наглядових органів.

4. Робоча група вибирає свого голову. Термін повноважень голови складає два роки. Він може вибиратися повторно.

5. Секретаріат Робочої групи забезпечується Комісією.

6. Робоча група приймає свій власний регламент.

7. Робоча група розглядає питання, винесені на порядок денний головою або за його власною ініціативою, або на прохання представника наглядового органу чи органів, або на прохання Комісії.

Стаття 30. Завдання робочої групи

1. Робоча група:

(a) розглядає будь-яке питання, що стосується застосування національних заходів, прийнятих відповідно до цієї Директиви, з метою сприяння загальному застосуванню таких заходів;

(b) представляє Комісії висновки щодо рівня захисту в Співтоваристві та в третіх країнах;

(c) повідомляє Комісію про будь-яку запропоновану поправку до цієї Директиви, про будь-які додаткові чи особливі заходи із захисту прав і свобод фізичних осіб при обробці персональних даних і про будь-які інші запропоновані заходи Співтовариства, що стосуються цих прав і свобод;

(d) виносить висновок про кодекси, складені на рівні Співтовариства.

2. Якщо Робоча група виявляє, що між законами чи практикою держав-членів виникають розбіжності, які можуть порушити рівень захисту осіб при обробці персональних даних у Співтоваристві, вона відповідним чином сповіщає про це Комісію.

3. Робоча група може за власною ініціативою давати рекомендації з усіх питань, які стосуються захисту осіб при обробці персональних даних у Співтоваристві.

4. Висновки і рекомендації Робочої групи передаються Комісії і комітету, передбаченому статтею 31.

5. Комісія повідомляє Робочу групу про дії, розпочаті у відповідь на її висновки і рекомендації. Повідомлення робиться у вигляді доповіді, що також подається Європейському Парламенту і Раді. Доповідь повинна бути оприлюднена.

6. Робоча група складає щорічний звіт про ситуацію відносно захисту фізичних осіб при обробці персональних даних у Співтоваристві та в третіх країнах, яку вона надає Комісії, Європейському Парламенту і Раді. Звіт повинен бути оприлюднений.

Розділ VII. Засоби співтовариства з виконання

Стаття 31. Комітет

Комісії допомагає Комітет, що складається з представників держав-членів і очолюється представником Комісії.

Представник Комісії подає Комітету проект заходів, яких слід вжити: Комітет надає свій висновок про проекти в межах строку, який може бути встановлений головою залежно від ступеня невідкладності питання.

Висновок приймається більшістю, встановленою у пункті 2 статті 148 Договору. Голоси представників держав-членів у комітеті підраховуються відповідно до процедури, встановленої даною статтею. Голова не голосує.

Комісія приймає заходи, що повинні застосовуватися негайно. Однак, якщо ці заходи не збігаються з висновком Комітету, Комісія негайно повідомляє про це Раду. У такому випадку:

- Комісія відкладає застосування прийнятих нею засобів на три місяці з моменту повідомлення про них;

- Рада, діючи кваліфікованою більшістю, може прийняти інше рішення в межах строку, передбаченого в першому абзаці.

Заключні положення

Стаття 32.

1. Держави-члени приймають законодавчі, нормативні й адміністративні положення, необхідні для виконання цієї Директиви, не пізніше ніж наприкінці трирічного періоду з моменту її прийняття.

Коли держави-члени приймають такі положення, останні повинні містити посилання на цю Директиву чи супроводжуватися таким посиланням у разі їх офіційної публікації. Методи, за якими робиться таке посилання, встановлюються державами-членами.

2. Держави-члени гарантують, що обробка даних, яка на день набуття чинності національними положеннями, прийнятими відповідно до цієї Директиви, вже відбувається, буде приведена у відповідність до цих положень за трирічний період з цієї дати.

Шляхом відступу від попереднього абзацу держави-члени можуть передбачити, що обробка даних, які на день набуття чинності національними положеннями, прийнятими на виконання цієї Директиви, вже зберігаються в неавтоматизованих картотеках, повинна бути приведена у відповідність до статей 6, 7 і 8 цієї Директиви протягом 12 років з дня її прийняття. Тим не менше, держави-члени надають суб’єкту даних право на його прохання і, зокрема, під час здійснення його права на доступ, виправляти, стирати чи блокувати дані, що є неповними, неточними чи зберігаються у формі, несумісній із законними цілями, переслідуваними контролером.

3. Шляхом відступу від пункту 2, держави-члени можуть передбачати, що за умови наявності відповідних гарантій дані, що зберігаються тільки з метою історичного дослідження, не потрібно приводити у відповідність до статей 6, 7 і 8 цієї Директиви.

4. Держави-члени повинні представити Комісії текст положень внутрішнього законодавства, які вони приймають у сфері, що підпадає під дію цієї Директиви.

Стаття 33.

Комісія регулярно доповідає Раді і Європейському Парламенту, починаючи не пізніше ніж через три роки з дати, зазначеної в пункті 1 статті 32, про виконання цієї Директиви, при необхідності додаючи до своєї доповіді відповідні пропозиції про поправки. Доповідь підлягає оприлюдненню.

Комісія вивчає, серед іншого, застосування цієї Директиви до обробки звукових і візуальних даних, що стосуються фізичних осіб, і подає будь-які відповідні пропозиції, що є необхідними з погляду досягнень в інформаційних технологіях та у світлі рівня прогресу в інформаційному суспільстві.

Стаття 34.

Ця Директива адресована державам-членам.

Вчинено в Люксембурзі 24 жовтня 1995 року.

За Європейський Парламент Президент К. Хенш.

За Раду Президент Л. Атьєнца Сера.

Ссылка по тексту:

1. Офіційний журнал (далі – ОЖ) № С 277, 5.2.1990, с. 3 та
ОЖ № С 311, 27.11.1992, с. 30.
2. ОЖ № 159, 17.6.1991, с. 38.
3. Висновок Європейського Парламенту від 11 березня 1992 р. (ОЖ № С 94, 13.4.1992, с. 198), ратифікований 2 грудня 1993 р. (ОЖ № С 342, 20.12.1993, с. 30); Загальна позиція Ради від 20 лютого 1995 р. (ОЖ № С 93, 13.4.1995 р., с. 1) і Рішення Європейського Парламенту від 15 червня 1995 р. (ОЖ № 166, 3.7.1995, с.).
4. ОЖ № L С 97, 18.7.1987, с. 33.

Джерело: Європейський Парламент і Рада Європейського Союзу. Офіційний журнал № L 281, 23.11.1995, с. 31-50. – Режим доступу : //www.evropa.eu.int/ISPO

*** * * * * * ***

До відома авторів

Журнал “Інформація і право” видається в установленому законодавством порядку для висвітлення результатів фундаментальних і прикладних наукових досліджень, а також дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук, з проблем становлення інформаційного суспільства, історії та філософії інформаційного права, інформаційних технологій та інформатизації, соціальних комунікацій, міжнародного права та інформаційної безпеки в умовах формування глобального інформаційного простору.

Зміст матеріалів статей має бути спрямований на вирішення визначених автором наукових завдань, згідно таких основних напрямів досліджень, як:

ІНФОРМАЦІЙНЕ ПРАВО:

- Філософія та методологія розвитку інформаційного права.
- Інформаційне законодавство України.
- Діяльність в інформаційній сфері.
- Міжнародне співробітництво в інформаційному просторі.
- Інформаційна безпека.

ТЕХНІКО-ТЕХНОЛОГІЧНІ НАУКИ:

- Інформаційно-технологічна діяльність.
- Телекомунікаційні системи та мережі.
- Захист даних та інформаційних ресурсів.
- Моделювання інформаційних процесів та явищ.
- Системи та засоби штучного інтелекту.

СОЦІАЛЬНІ КОМУНІКАЦІЇ:

- Теорія та історія соціальних комунікацій, мас-медіа та видавництва.
- Прикладні соціальні комунікації.
- Соціальна інформатика.
- Документознавство та книгознавство.
- Вплив інформаційних засобів та маніпулювання свідомістю людини.

Вимоги до оформлення:

1) **статтю слід подавати українською мовою, виготовлену у друкарський спосіб, та її електронну версію** (структура та зміст якої повністю відповідають друкованому варіанту) у вигляді файлу:
   - *у редакторі Word, шрифт – Times New Roman, з розширенням .doc, кегль – 13;*
   - *параметри сторінки – формат А-4, розташування тексту (таблиці, діаграми тощо) книжне, береги поля (верхній, нижній, лівий і правий край) – 20 мм;*
   - *відстань між рядками – 1 інтервал;*
   - *кількість матеріалу однієї статті – не більше 10 стор.*

   Стаття має передбачати такі обов’язкові структурні елементи:
   - *УДК, ім’я та прізвище, науковий ступінь, вчене звання автора;*
   - *назва статті, анотація та ключові слова – укр., рос., англ. мовами;*

- ***розв’язання проблеми:***
  - ***постановка проблеми*** *(загальна характеристика) та аналіз досліджень (публікацій), в яких започатковано розв’язання проблеми, виділення не вирішених її частин, котрим присвячується стаття;*
  - ***формування мети*** *(постановка завдання) статті;*
  - ***виклад основних положень – вирішення завдання та обґрунтування результатів;***
- ***висновки, пропозиції за результатами розв’язання проблеми;***
- *перспективи щодо подальших досліджень;*
- ***використана література*** *(згідно з наказом ВАК України від 26.01.08 р. № 63);*
- *підпис, адреса (е-адреса), телефон автора;*

2) подавати письмовий Відгук на статтю, підписаний особою, яка має науковий ступінь.
Відгук в обов’язковому порядку має висвітлювати такі питання:

- *актуальність теми;*
- *новизна та обґрунтованість одержаних результатів;*
- *наукова (практична) цінність результатів;*

3) рукопис статті та Відгук мають бути ретельно вичитаними, виправленими і підписаними відповідними особами;

4) за надання послуг щодо розгляду, форматування, корегування, тиражування та ін. робіт, пов’язаних з публікацією статей та виданням журналу, **пропонується здійснити оплату в розмірі 120 грн. на рахунок Інституту.**

Реквізити для оплати робіт та адреса для отримання автором екземпляра журналу:

– код ЄДРПОУ 25959933, р/р № 31258272210479, МФО 820019 в ГУДСКУ у м. Києві (з приміткою – **за науковий журнал**);

– адреса редакції: 01032, м. Київ, вул. Саксаганського, 110-В. Науково-дослідний інститут інформатики і права НАПрН України.

Копію квитанції прохання направити на е-адресу: **bvm777@ ukr.net**

Д о у в а г и

- Редакційна колегія не завжди поділяє погляди авторів публікацій. Статті видаються в авторській редакції.
- Редакційна колегія залишає за собою право на:
  - відхилення матеріалів статей які не відповідають тематиці Журналу, або таких, які виконані з порушенням зазначених вище Вимог до оформлення статей та експертних відгуків;
  - внесення до статті змін редакційного змісту у зв’язку зі скороченням обсягу матеріалу.
- Листування з читачами – тільки на сторінках журналу.

*** * * * * * ***

Інформація і право

Науковий журнал

Засновники:	- Науково-дослідний інститут інформатики і права Національної академії правових наук України; - Національна бібліотека України ім. В.І. Вернадського Національної академії наук України; - Відкритий міжнародний університет розвитку людини “Україна”.
Видавець журналу –	© Науково-дослідний інститут інформатики і права Національної академії правових наук України.
Адреса редакції –	01032, м. Київ, вул. Саксаганського, 110-В. Науково-дослідний інститут інформатики і права Національної академії правових наук України. Тел.: 234-94-56, 234-91-33.
Веб-сторінки журналу у мережі Інтернет:	//www.ippi.org.ua (НДІІП НАПрН України); //www.nbuv.gov.ua (Нац. бібліотека України ім. В.І. Вернадського).

Наукове редагування, створення оригінал-макета та дизайн – Брижко В.М.
Редагування – Москаленко А.М. (укр.), Майстренко І.А. (англ.).
Формат 70 х 108/16. Папір на внутрішній блок 80 г./м^2, білизна 97 %.
Спосіб друку – ризографія. Ум. друк. арк. 15.2. Тираж 100 прим.
Виготовлено з оригінал-макета в друкарні ТОВ “ПанТот”, м. Київ, вул. Щорса, 29.