

ЦЕНТР ПОЛІТИКО-ПРАВОВИХ РЕФОРМ

ДОСТУП ДО ІНФОРМАЦІЇ ТА ЕЛЕКТРОННЕ УРЯДУВАННЯ

Факт
Київ 2004

*Рекомендовано до друку
Науково-програмною радою Центру політико-правових реформ*

Відповідальний редактор:

І.Б. Колишко, голова Центру політико-правових реформ

Доступ до інформації та електронне урядування / Автори-упорядники М.С. Демкова, М. В. Фігель. — К.: Факт, 2004. — 336 с.

Книга присвячена проблемам правового регулювання доступу до публічної інформації та запровадження в Україні електронного урядування. До праці увійшли аналітичні матеріали, концепції Закону «Про доступ до інформації», законодавчі акти міжнародного права. Особливу увагу приділено висвітленню дискусійних питань щодо доцільності виокремлення інформаційного права в окрему галузь права, правовим режимом доступу до інформації, законодавчій регламентації захисту персональних даних тощо. У праці використано зарубіжний досвід правового регулювання доступу до інформації та функціонування електронного урядування.

Видання буде корисним для всіх, хто на теоретичному і практичному рівні займається питаннями доступу до інформації, проблемами розбудови інформаційного суспільства, а також юристам, які працюють та здійснюють дослідження у сфері інформаційного права, ЗМІ, державним службовцям, викладачам, студентам і всім, хто цікавиться проблематикою інформаційного та адміністративного права.

**Це видання здійснено завдяки фінансовій підтримці
Програми Добросусієства Міністерства закордонних справ
Данії і партнерства між Центром політико-правових реформ
і Датським Інститутом з прав людини**

**«The development of this publication was supported by
Neighborhood Program of the Danish Ministry of Foreign
Affairs and the partnership between the Centre for Legal and
Political Reform and the Danish Institute for Human Rights».**

ISBN

ЗМІСТ

ПЕРЕДМОВА.....5

ЧАСТИНА І ДОСТУП ДО ІНФОРМАЦІЇ

1. Інформація як об'єкт правового регулювання	11
1.1. Правова природа інформації.....	11
1.2. Інформаційне право: стан та перспективи розвитку в Україні.....	17
2. Теоретико-правові та практичні засади доступу до інформації	19
2.1. Теоретичні основи правового регулювання доступу до інформації.....	20
2.1.1. Право на доступ до інформації: європейські стандарти та конституційні гарантії.....	20
2.1.2. Правові режими доступу до інформаціїКласифікація інформації.....	27
2.1.3. Правове регулювання інформації персонального характеру.....	36
2.2. Процедура реалізації права на доступ до інформації	51
2.2.1. Активне право на доступ до інформації.....	51
2.2.2. Пасивне право на доступ до інформації.....	56
2.2.3. Оскарження і відповідальність за порушення права на доступ до інформації.....	59
Замість висновків. Перспективи розвитку законодавства України про доступ до інформації.....	63
<i>Додаток. Проект Концепції закону України «Про доступ до інформації»</i>	67

ЧАСТИНА ІІ ЕЛЕКТРОННЕ УРЯДУВАННЯ: СВІТОВИЙ ДОСВІД І УКРАЇНСЬКІ РЕАЛІЇ

1. Поняття і суть електронного урядування	93
2. Світова практика запровадження та функціонування систем електронного урядування.....	100
3. Правове забезпечення електронного урядування	116
Замість висновків. Завдання електронного урядування та перспективи його запровадження в Україні.....	124
<i>Додаток. Електронні предстелитства урядів світу</i>	129

ЧАСТИНА ТРЕТЯ МІЖНАРОДНЕ ПРАВО У СФЕРІ ІНФОРМАЦІЇ

Конвенція Ради Європи № 108 про захист осіб стосовно автоматизованої обробки даних особистого характеру.....	135
Додатковий протокол № 181 до Конвенції про захист осіб стосовно автоматизованої обробки даних особистого характеру.....	145
Конвенція Ради Європи № 185 про кіберзлочини.....	155
Декларація про європейську політику у галузі нових інформаційних технологій.....	182
Рекомендація № R (81) 19 Комітету міністрів державам-членам Ради Європи про доступ до інформації, що перебуває в розпорядженні державних органів.....	188

Рекомендація № R (89) 9 Комітету міністрів державам-членам

Ради Європи щодо комп'ютерних правопорушень.....

193

Рекомендація № R (91) 10 Комітету міністрів державам-членам

Ради Європи щодо передачі третім особам інформації

персонального характеру, яка знаходиться в органах влади.....

194

Рекомендація № R (95) 13 Комітету міністрів державам-членам

Ради Європи стосовно проблеми кримінально-процесуального права

щодо інформаційних технологій.....

200

Рекомендація № R (99) 5 Комітету міністрів державам-членам

Ради Європи щодо захисту недоторканності приватного життя в Інтернеті,

якою затверджено Керівні принципи захисту особи стосовно збору

і обробки персональних даних на інформаційних магністралях.....

204

Рекомендація № R (2001) 8 Комітету міністрів державам-членам

Ради Європи щодо саморегулювання змісту електронної інформації

(саморегулювання та захист споживачів від нелегального

або шкідливого змісту інформації у нових комунікаційних

та інформаційних послугах).....

210

Рекомендація № R (2002) 2 Комітету міністрів державам-членам

про доступ до офіційних документів.....

215

Рекомендації Ради з економічного співробітництва та розвитку,

що стосуються основних положень про захист недоторканності

приватного життя і міжнародних обмінів персональними даними.....

220

Окінська хартія глобального інформаційного суспільства.....

225

Директива 95/46/ЄС Європейського парламенту та Ради ЄС

«Про захист фізичних осіб при обробці персональних даних

та про вільне переміщення таких даних».....

233

Директива 96/9/ЄС Європейського парламенту та Ради ЄС

«Про правовий захист баз даних».....

264

Директива 97/66/ЄС Європейського парламенту та Ради ЄС

«Стосовно обробки персональних даних і захисту права

на невтручання в особисте життя в телекомунікаційному секторі».....

277

Директива 99/93/ЄС Європейського парламенту та Ради ЄС

про електронний підпис.....

290

Декларації принципів. Побудова інформаційного суспільства — глобальне

завдання нового тисячоліття. Документ WSIS-03/GENEVA/DOC/4-R,

прийнятий на Всесвітній зустрічі на вищому рівні з питань

інформаційного суспільства.....

304

План дій. Документ WSIS-03/GENEVA/DOC/5-R,

прийнятий на Всесвітній зустрічі на вищому рівні

з питань інформаційного суспільства.....

317

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ.....340

ПЕРЕДМОВА

Однією з найважливіших засад функціонування Європейського адміністративного простору є відкритість та прозорість публічної адміністрації (органів державної влади та органів місцевого самоврядування). У державах з демократичним режимом діють відповідні політико-правові механізми, спрямовані на досягнення максимальної прозорості в діяльності органів влади. Прозора влада повинна належним чином забезпечувати діалог з громадськістю на всіх етапах прийняття рішень та постійний доступ до повної, об'єктивної, точної, зрозумілої інформації про діяльність органів державної влади та її посадових осіб відповідно до законодавства. Від прозорості влади, від якості інформування громадянської про діяльність її органів у демократичній державі також залежить ефективність діяльності публічної адміністрації.

На етапі становлення української держави проблема забезпечення прозорості в діяльності органів влади є однією з основних перешкод, які стоять на шляху розвитку демократичного суспільства. Прозорість влади є необхідною умовою забезпечення передбачених Конституцією України прав громадян на інформацію та участь в управлінні державними справами. Ці конституційні права порушуються, а витіток суспільство втрачає довіру до уряду, до влади. Зрозуміло, що на даному етапі про існування в Україні «здорового» демократичного суспільства говорити ще рано. На жаль, ми все ще переживаємо наслідки радянської системи, при якій панувала ідеологія «підкорення людини державою», а не служіння держави інтересам громадян, як це існує у розвинутих демократичних державах.

Отже, основою права на свободу інформації є відкритість, під якою розуміється відсутність перешкод в одержанні інформації і можливості інформувати інших, тобто можливість шукати, запитувати, одержувати, а також передавати і поширювати інформацію. Це — можливість людини одержувати інформацію не тільки щодо себе самої (якщо така інформація є в певних організаціях чи установах), але також щодо соціальних, політичних та інших питань. Це правило руйнує бар'єр між потребою в інформації і реальному доступі до неї.

На сьогодні в нашій державі існують труднощі у сфері доступу громадян до публічної інформації (якою володіють органи державної влади та органи місцевого самоврядування). Органи влади фактично безпідставно відмовляють у наданні інформації, відносячи її до інформації з обмеженим доступом; непрапомірно застосовуються грифи

¹ Gotzyska Tereza. Prawo do informacji I zasada jawnosci administracyjnej. — Krasow, Zaslupcze, 1999. — С. 27—28.

обмеження доступу до інформації «опублікуванню не підлягає», «не для друку», «для службового користування»; існують перешкоди в отриманні громадянами нормативно-правових актів, виданих місцевими органами виконавчої влади та органами місцевого самоврядування, не кажучи вже про проекти таких актів.

Органи влади не повною мірою виконують вимогу оприлюднювати інформацію про свою діяльність (в тому числі через мережу Інтернет). Не всі внутрішньовідомчі акти публікуються в офіційних виданнях, і, таким чином, державні органи стають подібними до власників інформації, які на власний розсуд приймають рішення про надання або відмову в наданні інформації. Достовірна і повна інформація про внутрішню структуру державного органу, закріплене за ним майно, витрати на його діяльність практично недоступні для звичайних громадян. Можна констатувати, що існуюча державно-правова практика з питань надання інформації громадянам не відповідає стандартам демократичної держави.

Особливої актуальності сьогодні набула проблема захисту персональних даних (інформації персонального характеру), яка полягає у визначенні оптимальної межі між правом на доступ до інформації персонального характеру та правом на захист такої інформації. Усі ці проблеми прямо пов'язані, по-перше, із відсутністю ефективних правових механізмів реалізації права на доступ до інформації, залишаючи закріплення цього права лише на рівні декларації.

У нашій праці також значну увагу приділено одному з ефективних засобів забезпечення прозорості влади — електронному урядуванню, що передбачає можливість будь-якої фізичної або юридичної особи через Інтернет звертатися із запитом до державних органів для одержання необхідної інформації та здійснення юридичних операцій. За такої схеми відносин «громадянин — держава» можна розраховувати на зростання ефективності діяльності публічної адміністрації та зняття рівня корупції. Електронне урядування здатне змінити саму природу влади, зробити її більш прозорою і підконтрольною громадськості, зокрема, шляхом забезпечення реальної участі громадян у політичних процесах.

Отже, мета нашої праці полягає у дослідженні та вирішенні проблем, які виникають на шляху забезпечення прозорості влади, а саме — щодо забезпечення доступу до публічної інформації (інформації, якою володіють органи державної влади та місцевого самоврядування), з'ясування проблем правового регулювання персональних даних, а також шляхів забезпечення функціонування в Україні системи електронного урядування як засобу реалізації права громадян на доступ до інформації.

Як уже згадувалося, для досягнення максимальної прозорості в діяльності публічної адміністрації необхідно розробити, в першу чер-

гу, ефективні правові механізми. Очевидно, що певні нормативно-правові акти в цій сфері вже існують. Проте багато з них були прийняті ще до набрання чинності Конституцією України, а тому не повною мірою відповідають сучасному стану розвитку інформаційних відносин в Україні, не узгоджені між собою та містять інші недоліки, про які йтиметься у даній праці. Ще важкою є проблема запровадження в Україні електронного урядування, законодавство про яке ще досить нове, не апробоване й очевидно не цілком достатнє.

Автори даної праці проаналізували правову базу України, міжнародний досвід, перспективи розвитку законодавства про доступ до інформації, визначили поняття «правове забезпечення електронного урядування», дослідили світову практику його запровадження та функціонування, визначили перспективи запровадження та розвитку електронного урядування в Україні. Як кінцевий етап проведеного дослідженнями експерти ЦППР підготували концепцію Закону про доступ до інформації, що є певним правовим механізмом вирішення існуючих у цій сфері проблем.

У праці було використано відповідні міжнародні документи, законодавство зарубіжних країн, аналітичні матеріали Міжнародної організації «Article 19», Харківської правозахисної групи, проекту ДФІД та ін.

Особливу увагу звернуто на незалежному експертів з питань публічної адміністрації та свободи інформації Н. Гнідюк — за корисні поради, експертам Т. Березі та Н. Блажівській — за збір та надання цікавих матеріалів про світовий досвід функціонування електронного урядування, Л. Щербанюк — за переклад міжнародних документів про інформацію, колегам із Центру політико-правових реформ, а також усім, хто надавав творчу і технічну допомогу в підготовці книги.

Для написання роботи особливо корисними були погляди, рекомендації та пропозиції учасників Круглого столу «Інформаційне право: стан та перспективи розвитку в Україні».

Сподіваємось, наша праця буде корисною для подальшого розвитку правової бази про доступ до інформації, а також для втілення і функціонування електронного урядування у нашій державі.

ЧАСТИНА I

ДОСТУП ДО ІНФОРМАЦІЇ

1. ІНФОРМАЦІЯ ЯК ОБ'ЄКТ ПРАВОВОГО РЕГУЛЮВАННЯ

1.1. Правова природа інформації

Для того щоб дослідити місце конституційного права людини на доступ до публічної інформації серед інших прав, його взаємозв'язок та вплив на прозорість діяльності органів влади, необхідно визначити поняття самої інформації та з'ясувати її правову природу.

Інформація виступає основним об'єктом інформаційного суспільства, і її роль сьогодні важко переоцінити. Відображаючи реальну дійсність, вона інтегрується у всі напрямки діяльності держави, суспільства, громадянина. З появою нових інформаційних технологій, основою яких є впровадження засобів обчислювальної техніки, зв'язку, систем телекомунікації, інформація стає постійним і необхідним атрибутом забезпечення діяльності держави, юридичних осіб, громадських організацій та громадян.

Інформаційний вплив на державу, суспільство, громадянина зараз є ефективнішим, ніж політичний, економічний і навіть військовий. Інформація стає реальною, майже фізично відчутною силою².

Поняття «**інформація**» використовується в усіх галузях науки, зокрема в правовій. Воно набуло багатозначності й інтерпретується залежно від сфери вживання. У перекладі з латинської мови «інформація» (information) — це роз'яснення, виклад³, тобто йдеться про відомості (або їх сукупність), про предмети, явища й процеси навколишнього світу. Сьогодні немає усталеного й вичерпного тлумачення цього терміна; його можна розглядати, виходячи з досліджень філософів.

Поняття інформації неодноразово змінювалось, його межі то розширювалися, то звужувалися. Спочатку під цим словом розуміли «уявлення», «поняття», потім — «відомості», «передачу повідомлень». Уперше термін «інформація» знайшов своє відображення у математичній теорії інформатики і теорії передачі даних каналами зв'язку Клода Шеннона (1948), у якій він під «інформацією» розумів усі види повідомлень. К. Шеннон разом з У. Уївером запропонували ймовірні методи для визначення кількості інформації, що передається. Однак такі методи описують лише знакову структуру інформації, не торкаючись її змісту.

Н. Вінер запропонував «інформаційне бачення» кібернетики як науки про управління в живих організамах та технічних системах. Під інформацією почали розуміти вже не будь-які відомості, а лише ті,

² Черешкин Д.С. Оружие, которое может быть описано ядерного // Независимая газета. — 1995. — № 123.

³ Юрилична енциклопедія: В 6 т. / Редкол.: Ю.С. Шемшученко (голова редкол.) та ін. — К.: Укр. енцикл., 1998. — Т. 2. — С. 717.

які є новими та корисними для прийняття такого рішення, що забезпечить досягнення мети управління. Інші відомості не вважались інформацією.

У свою чергу, Л. Веккер, як і Н. Вінер, підкреслює у цьому понятті ознаку впорядкованості і зазначає: «Інформація може бути охарактеризована як збереження і відновлення її носієм упорядкованості станів і її джерела, яке впливає на цього носія»⁴.

Розглядаючи інформацію як предмет правовідносин у правовій системі, предмет взаємовідносин між державою та юридичними і фізичними особами, доводиться повертатися до вихідних визначень інформації. Прикладом може стати визначення, яке запропонував С. Ожегов. На його думку, інформація — це: 1) відомості про навколишній світ і процеси, що в ньому відбуваються; 2) повідомлення про стан справ, про стан чого-небудь⁵. І це правильно, адже більшість суспільних відносин виникає саме з приводу інформації як відомостей і повідомлень під час її створення, розповсюдження, перетворення та споживання.

Схожі визначення давали й інші науковці. Так, В. Ровенський, А. Уемов, Є. Уємова під інформацією розуміли «повідомлення про події, що відбуваються як у зовнішньому щодо системи середовищі, так і в самій системі»⁶. С. Анісімов вважає, що «інформацією можна назвати будь-яке повідомлення або передачу відомостей про будь-що, яке заздалегідь не було відоме»⁷.

Однак були і більш витончені ідеалістичні інтерпретації поняття інформації. Відомий дослідник К. Фон Вайцекер у своїх працях розкриває його за допомогою іншого поняття — форми, тобто стверджує, що маса й енергія еквівалентні інформації. На думку А. Блока, Г. Гунтера, П. Снайдера, інформація є взагалі чимось третім, «нейтральним», «проміджним» між духом і матерією⁸.

Узагальнюючи, можна виділити **дві концепції інформації**. Прихильники **першої** концепції зробили спробу співвіднести інформацію з поняттям «відображення», розкриваючи водночас необхідність єдності відображення й взаємодії як діалектичної єдності полярних категорій.

Друга концепція інформації, на думку багатьох учених, є більш плідним підходом до вирішення проблеми інформації, — «різноманітність» концентрації інформації. У рамках даного підходу інформацію

можна трактувати як «зняту нерозрізненість», як розмаїтість. «Інформація, — підкреслює Б. Бірюков, — існує там, де є розмаїття, неоднорідність. Інформація «виявляється» тоді, коли хоча б два «елементи» у сукупності різняться, і вона «зникає», якщо об'єкти «склеюються», «ототожнюються»⁹. Багато авторів використовують у своїх дослідженнях ті визначення інформації, які наведені в енциклопедичному словнику: «Інформація — це відомості, що передаються людьми усним, письмовим або іншим способом»¹⁰. Одночасно розглядається і більш узагальнене системне визначення: «Інформація — це загальнонаукове поняття, що включає обмін відомостями між людьми, людиною й автоматом, автоматом і автоматом; обмін сигналами у тваринному й рослинному світі; передачу ознак від клітини, від організму до організму»¹¹. Зазначено, що для цих двох визначень характерна єдина внутрішня сутність, що дає підставу застосовувати їх для різноманітних систем.

Категорія «інформація» виступає одним із найважливіших факторів системи суспільних відносин. У зв'язку з цим у сучасній філософії, теоретичних та прикладних науках не можуть підібрати однозначного трактування (змісту) категорії «інформація».

Під інформацією розуміють також корисний зміст про річ, явище, факт, людину, суспільство, державу тощо, тобто вилучені із них, чи про них дані. При цьому категорія «дані» розглядається як абстрактна категорія. Їх конкретний зміст визначається з прив'язкою до сфери пізнання¹².

Існує думка що з точки зору праксеологічного аспекту, на практиці дуже часто неправомірно (нерационально) встановлюють однозначність між даними та інформацією. На думку прихильників цієї теорії, дані реєструють явища і події, що відбуваються, а інформація — результати переробки та аналізу даних на рівні індивідуального інтелекту, тобто, їх усвідомлення конкретною людиною¹³.

Для того щоб окреслити інформацію у правовому контексті, ми повинні виділити такі юридично значимі ознаки, які зумовлюють специфіку інформації як об'єкта правового регулювання. До таких ознак найчастіше відносять¹⁴:

⁹ Там само. — С. 10

¹⁰ Советский энциклопедический словарь. — М., 1983. — С. — 498.

¹¹ Там само. — С. 498.

¹² Информатизация, право, управление: организационно-правовые вопросы / Р. А. Калужный, О. Д. Круглан, В. Д. Павловский, М. В. Гуалюк, В. С. Цимбалюк, М. Я. Швец. — К., 2002.

¹³ Там само.

¹⁴ Международное информационное право: Методические материалы к дисциплинарному спецкурсу / Сост. Т. М. Смыслова. — М.: СТЭНСИ, 2002. — 192 с.

⁴ Веккер Л. М. Воспитание и основы его моделирования. — М., 1964. — С. 44.

⁵ Копылов В. А. Информационное право // М.: Юрист, 1997. — С. 22.

⁶ Ровенский В., Уемов А., Уємова Е. Машина и мысль. — М., 1960. — С. 69.

⁷ Анисимов С. Ф. Человек и машина. — М.: 1959. — С. 8.

⁸ Аристова І. В. Державна інформаційна політика: організаційно-правові аспекти / За ред. О. М. Бандурки. — Харків: Вид-во Університету внутрішніх справ, 2000. — С. 9.

— нематеріальний характер («самостійність щодо носія», тобто цінність інформації полягає в її суті, а не в матеріальному носії, на якому вона зафіксована);

— суб'єктивний характер («інформація виникає внаслідок діяльності суб'єкта, який наділений свідомістю», тобто вона є результатом інтелектуальної діяльності);

— необхідність об'єктивації для включення у правовий обіг;

— кількісна визначеність;

— неспоживчість, можливість багаторазового використання;

— зберігання інформації у суб'єкта, який її передає;

— здатність до відтворення, копіювання, збереження і накопичення.

Отже, інформація — це багатофункціональний об'єкт. Вона створюється й застосовується в усіх сферах діяльності і забезпечує виконання багатоманітних функцій і завдань, що постають перед найрізноманітнішими суб'єктами — органами державної влади, місцевого самоврядування, перед фізичними і юридичними особами, іншими соціальними утвореннями. Саме тому Закон України «Про інформацію» від 2 жовтня 1992 року розуміє інформацію як «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі»¹⁵. Проте таке визначення потребує суттєвого уточнення.

Розуміння інформації як відомостей лише про події та явища (статичні поняття) залишає поза увагою відомості про процеси (шось триває у часі). Адаже під інформацією слід розуміти і створювані в процесі інтелектуальної діяльності відомості (дані) про навколишній світ, і процеси, що в ньому відбуваються, або відомості про стан справ.

Закон України «Про інформацію» визначає перелік сфер, де інформація має місце. Це — суспільство, держава та навколишнє природне середовище. Обсяг кожної з цих сфер можна розуміти по-різному. Одночасно не має визначення термінів «суспільство» чи «держава». Швидше за все, цей перелік не є вичерпним.

Отже, краще чітко конкретизувати й розширити дію Закону, зазначивши в статті 1 весь перелік сфер діяльності, які існують, а також ті, які можуть виникнути. Але з огляду на недоцільність такого викладу не слід обмежувати Закон вищезаданим переліком, а вказати, що інформація — це відомості про осіб, предмети, факти, події, явища й процеси, незалежно від форм їх вираження.

Тому слід зв'язати на те, що порівняно з філософським підходом законодавча дефініція є недосконалою, а тому провокує термінологічні

конфлікти. Однак 11 січня 2001 року було прийнято Закон України «Про захист економічної конкуренції», у п. 1 ч. 2 статті першої якого подано визначення терміна «інформація», яке використовується для цілей даного Закону, а саме під інформацією тут розуміються «відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості». Аналізуючи це визначення, можна побачити значний поступ законодавства в інформаційній сфері.

Що ж до інформації органів виконавчої влади, то, згідно з Принципами законодавства про свободу інформації міжнародної організації «Article 19. Всесвітня кампанія за свободу слова», «інформація» включає всі записи, які знаходяться в органах виконавчої влади, незалежно від форми, в якій інформація зберігається (документи, магнітофонна стрічка, електронний запис тощо), їхні джерела (чи її було створено публічним органом, чи якимось іншою організацією) і дату створення. Законодавство повинно також застосовуватися до записів, які були засекречені, піддаючи їх такій самій перевірці, як і всю іншу інформацію»¹⁶.

Однак варто зауважити, що доступ до інформації не є тим самим, що доступ до документів. Перше поняття є значно ширшим. Для того щоб мати доступ до документів, спочатку треба отримати інформацію про їхнє існування. Отож для повноцінного доступу до інформації необхідно, щоб хтось був зобов'язаний надавати таку інформацію. Таким чином, природа права на доступ до інформації є подвійною. З одного боку, влада мусить утримуватися від обмеження дії суб'єкта інформаційних правовідносин, зацікавленого в отриманні інформації, а з іншого — сама повинна сприяти поширенню такої інформації, сповіщаючи про факти та події, які є предметом громадського інтересу»¹⁷.

Існують різні підходи до того, що слід вважати **документом**. Ми знаємо, що існують певні ознаки, за якими можна визначити традиційні паперові документи. Але значно складніше з'ясувати подібні ознаки стосовно електронної документалізації. Стрімке зростання такого виду документалізації, включно з легалізацією електронних документів у багатьох країнах світу шляхом ухвалення законів про цифровий підпис,

¹⁶ Міжнародні стандарти забезпечення свободи слова.: Збірник публікацій міжнародних організацій «Article 19». — К.: Мільніум, 2003. — С. 8.

¹⁷ Право на приватність: *conditio sine qua non* / Харківська правозахисна група. — Харків: Фоліо, 2003. — С. 117.

вимагає врахування багатьох нових елементів, необхідних для подальшого розвитку законодавства про доступ до інформації. Цікавим, наприклад, є шведський підхід, де документом вважається будь-яка інформація, записана на будь-якому носії, тому поняття доступу до інформації та доступу до документів майже збігаються за своїм змістом. Проте такий підхід може створювати й певні складнощі. Так, Державний архів Швеції свого часу був змушений копіювати розміщену й доступну інформацію з усіх шведських сайтів в Інтернеті. Адже за новим законодавством країни кожен автономний шматок подібної інформації визнається документом, а останній підлягає зберіганню в архіві. Для цього був створений спеціальний робот, що копіює інформацію та записує її на електронні носії. Враховуючи стрімкий розвиток технічних засобів і зростаючі обсяги інформації, така робота вимагає великих фінансових витрат і може перетворити архів на музей комп'ютерної техніки. Але в такий спосіб держава гарантує реалізацію права на доступ до інформації¹⁸.

Якщо розглядати інформацію в контексті інформаційного суспільства, то вона (інформація) разом із знаннями виступає головним продуктом і основою його функціонування. Функціонування інформаційного суспільства забезпечується розвитком інформаційної інфраструктури, одним з основних елементів якої є інформаційні ресурси. Інформаційні ресурси становлять собою документи та масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, депозитаріях, музейних сховищах та ін.)¹⁹, тобто вони виступають джерелами інформації.

Інформаційне суспільство у правовому відношенні функціонує на основі нормативних актів, які регламентують **інформаційні відносини** (особлива однорідна група суспільних відносин, що виникають під час руху інформації в інформаційній сфері в результаті здійснення інформаційних процесів у порядку реалізації кожним інформаційних прав і свобод, а також у порядку виконання обов'язків органами державної влади і місцевого самоврядування щодо забезпечення гарантій інформаційних прав і свобод)²⁰ і процеси, у тому числі відносини власності на інформаційні ресурси та авторські права, доступ до публічної інформації, захист інформації, права на інтелектуальну власність, використання інформаційних технологій у державному управлінні. З точки зору функціонування інформаційного суспільства, цікавим є питання саме використання інформації (задоволення інфор-

маційних потреб суб'єктів інформаційних відносин), проблема доступу до неї. Право на доступ до інформації та недоторканності особистості є загальними правами людини, їх законодавче оформлення створює правовий фундамент інформаційного суспільства.

Таким чином, інформація виступає об'єктом інформаційних відносин — відносин, які пов'язані з реалізацією права на інформацію та інформаційною діяльністю у галузі створення, збирання, отримання, використання, поширення та зберігання інформації. Виходячи з цього, виникає питання про існування інформаційного права як самостійної галузі або ж галузі інформаційного законодавства.

1.2. Інформаційне право: стан та перспективи розвитку в Україні

З правової точки зору, інформація виступає об'єктом інформаційних правовідносин. Чимало дискусій точиться навколо питання, чи можна відносити «інформаційне право» до самостійної галузі права. Розглянемо це питання детальніше.

Право, виконуючи економічні та соціально-політичні функції і взаємодіючи з державою в особі уповноважених на правотворчість органів, постійно розвивається, удосконалюється і змінюється. Це слід пов'язувати з різноманітними стратегічними завданнями і цілями, які ставляться в той чи інший історичний період. Право як єдина система правил поведінки регулює суспільні відносини, що відрізняються за об'єктом, змістом, суттю, суб'єктним складом та іншими критеріями. Зазначена позиція передбачає поділ системи права на галузі та інститути.

У свою чергу, під галуззю права, як правило, розуміють відокремлену сукупність правових норм, що регулюють певну сферу суспільних відносин специфічним методом правового регулювання. Об'єднання правових норм у галузь права зумовлене об'єктивною законністю.

Зважаючи на те, що особливої актуальності на сьогодні набули проблеми формування інформаційного суспільства, стрімко зростає кількість спеціалістів, зайнятих у цій сфері, у суспільстві виникають процеси трансформції багатьох державно-правових інститутів у зв'язку з підвищенням соціальної ролі інформації і розвитком глобальних мереж. Постають нові правові проблеми, пов'язані з використанням глобальних інформаційно-комунікативних систем в інфраструктурі ресурсів економіки, політики, інших соціальних сфер. Під впливом цих факторів формується особлива, комплексна галузь законодавства — інформаційне законодавство. Це не лише виділення особливої структури в системі комплексних галузей, а й відображення процесу значних змін у вже сформованих галузях права і законодавства.

¹⁸ Там само.

¹⁹ Голобуцький О. П., Шевчук О. Б. Електронний уряд. — К., 2002.

²⁰ Копылов В.А. Информационное право: Учебник. — 2-е изд., перераб. и доп. — М.: Юрист, 2002. — С. 99.

У науковій літературі останніх років можна виділити цілий спектр понять, за допомогою яких автори намагаються назвати цю нову галузь права. До таких термінів можна віднести: «програмане право», «програмна інформатика», «право інформатики», «комп'ютерне право», «інформаційно-комп'ютерне право», «право знати», «право на доступ до інформації», «право на інформацію», а також «телекомунікаційне право» і «інформаційне право» (див. роботи А.Б. Агапова, Ю.М. Батуріна, І.Л. Бачило, А.Б. Венрова, М.М. Расолова, Ю.А. Ти-хомирова та інших).

В.А. Копылов²¹ у своїх працях зазначає, що всі вищезазначені терміни можна поділити на дві групи. Терміни першої групи, швидше за все, виникають завдяки об'єктам, у зв'язку з якими виникають суспільні відносини (це програми для ЕОМ; комп'ютери; інформатика як наука, що вивчає інформацію; одночасно «інформатик» і «комп'ютери» як пов'язані поняття; телекомунікації як засіб отримання, передачі і знищення зв'язку). Друга група термінів ґрунтується на застосуванні понять, що уособлюють інформаційні права та свободи, які мають гарантуватися інформаційним правом, — «право знати», «право на доступ до інформації» та ін.²²

Незважаючи на різноманітність цих понять, усіх їх можна об'єднати в один клас через поняття «інформаційна сфера» (сфера діяльності, пов'язана зі створенням, поширенням, перетворенням і використанням інформації), у якій вони застосовуються або як її складові частини, або як асоційовано пов'язані з нею. Вважаємо, що інформаційну сферу слід розглядати в сукупності, а не зупинятись на її окремих складових — інформатика, програмні засоби, комп'ютери, їх системи, засоби зв'язку, телекомунікації та ін.²³

На думку деяких науковців²⁴, **повноцінність галузі права** може бути визначена при наявності **трьох її складових**, а саме: 1) самостійності предмета і метода стосовно інших галузей права; 2) самостійності нормативно-правової основи галузі, достатньої для формування окремої галузі законодавства; 3) самостійності її доктрини і навчальної дисципліни.

Під **предметом** права зазвичай розуміють певні види суспільних відносин, що регулюються правом.

Під **предметом** інформаційного права слід розуміти інформаційні відносини як відокремлену групу суспільних відносин, що виника-

ють у процесі обігу інформації в інформаційній сфері в результаті здійснення інформаційних процесів шляхом реалізації кожним інформаційних прав і свобод, а також шляхом виконання обов'язків органами державної влади і місцевого самоврядування щодо забезпечення гарантій інформаційних прав і свобод²⁵.

Проблематичним залишається питання про самостійність **методу даної галузі** права. Незважаючи на явно виражену самостійність предмета правового регулювання, інформаційне право не може мати власного методу, на зразок цивільного чи кримінального права, оскільки є **комплексною галуззю**. Тут реалізуються методи усіх класичних галузей права: конституційного, адміністративного, цивільного і кримінального. За цією ознакою інформаційне право є галуззю другого рівня, яка реалізує методи базових галузей права, що не заважає розвитку її теоретичної і нормативної основи²⁶.

Даючи інші індикатори для галузі інформаційного права — наявність **законодавства і навчальних курсів** з окремих напрямків і всього комплексу проблем себе вже проявляють. За останні 5—7 років сформовано значний масив українського законодавства і прийнято велику кількість підзаконних актів, які регулюють різноманітні напрямки діяльності в інформаційній сфері. Щодо навчальних курсів, то їх лише почали вводити в навчальні програми вищих навчальних закладів. Слід згадати також і те, що згідно з Наказом Вищої атестаційної комісії України від 03.06.2003 № 291, зареєстрованого в Міністерстві юстиції України 1 липня 2003 р. за № 532/7853 «Про внесення змін і доповнень до Переліку спеціальностей, за якими проводиться захист дисертацій на здобуття наукових ступенів кандидата наук і доктора наук, присудження наукових ступенів і присвоєння вчених звань», до галузей науки, за якими присуджується науковий ступінь під шифром 12.00.07, додано «інформаційне право».

Проте, на нашу думку, ще рано говорити про інформаційне право як галузь права, хоча, без сумніву, є перспективи для виділення **інформаційного права** в нову комплексну галузь права, яку можна буде розглядати як **сукупність** **однорідних правових норм, що регулюють суспільні відносини, які виникають в інформаційній сфері**.

²¹ Копылов В.А. Информационное право. Учебник. — 2-е изд., перераб. и доп. — М.: Юрист, 2002.

²² Там само.

²³ Там само.

²⁴ Бачило И.Л., Копылов В.А. Есть ли основания для создания отрасли «Информационное право» // <http://di.iis.ru:82/arc/infosoc/etag.nsf/0/95b72be27308f4fc256904002b0108?>

²⁵ Копылов В.А. Информационное право...

²⁶ Бачило И.Л., Копылов В.А. Есть ли основания для создания отрасли «Информационное право»...

2. ТЕОРЕТИКО-ПРАВОВІ ТА ПРАКТИЧНІ ЗАСАДИ ДОСТУПУ ДО ІНФОРМАЦІЇ

2.1. Теоретичні основи правового регулювання доступу до інформації

2.1.1. Право на доступ до інформації: європейські стандарти та конституційні гарантії

Конституція України закріпила право людини на свободу інформації. Стаття 34 Конституції України гарантує кожному право на свободу думки і слова, на вільне вираження своїх поглядів і переконань; право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб і на свій вибір. Поняття «свобода інформації» охоплює цілу групу прав і свобод: свободу слова (свободу вираження думок), свободу преси і інших засобів масової інформації, право на одержання інформації, що має суспільне значення, свободу поширення інформації будь-яким законним способом. Свобода інформації гарантується заборонаю цензури. Водночас Конституція України містить обмеження свободи інформації. Головним обмеженням свободи інформації є заборона будь-якої пропаганди й агітації, що збуджують соціальну, національну, расову, релігійну ненависть і ворожнечу, а також пропаганди соціальної, расової, національної, релігійної або мовної перекрутки.

Конституцією України також передбачено, що свобода інформації може бути обмежена лише законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримки авторитету й неупередженості правосуддя.

Свобода інформації не є абсолютним правом і не може бути обмежена в період дії надзвичайного або воєнного стану.

Отже, з вищевикладеного випливає, що право на доступ до інформації є складовою закріпленого Конституцією України права на свободу інформації. Дана норма Конституції ґрунтується на положеннях Конвенції про захист прав людини та основних свобод (стаття 10), Міжнародного пакту про громадянські і політичні права (статті 18, 19) тощо.

Україна нині перебуває на шляху формування і розвитку в ній інформаційного суспільства, існування якого можливе у демократичній, правовій державі, де панує принцип верховенства права і максимально забезпечується реалізація прав людини. Право на доступ до інформації є одним із невід'ємних прав людини і громадянина, а тому

знаходить своє закріплення як на міжнародному рівні, так і в національному законодавстві.

В умовах сучасного рівня світової глобалізації розвиток нашої держави не може відбуватися сепаративно від інших країн. Тому для ефективного функціонування і розвитку інформаційних відносин з метою забезпечення доступу до публічної інформації необхідно враховувати норми міжнародного та європейського права.

Так, Загальна декларація прав людини (ЗДПЛ)²⁷ є основним загальноприйнятим документом проголошення прав людини, обов'язковим для виконання всіма країнами-учасницями як документ, що відноситься до прецедентного міжнародного права. Стаття 19 Декларації прав людини гарантує не тільки право на свободу вираження поглядів, а й право на доступ до інформації; це положення сформульоване так:

«...Кожний має право на свободу думки і вираження; це право включає також право вільно виражати думки та збирати, отримувати та поширювати інформацію і думки через засоби масової інформації, незважаючи на кордони... Зазначені свободи можуть бути обмежені у випадках, коли «це встановлено законом з метою забезпечення належного визнання і поваги прав та свобод інших осіб, задоволення справедливих вимог моралі, суспільного порядку і загального добробуту в демократичному суспільстві» (стаття 29 Загальної декларації).» У Міжнародному пакті про громадянські та політичні права (МПГПП)²⁸, ратифікованому Україною у 1973 р., гарантії доступу до інформації сформульовані подібно до ЗДПЛ, а саме:

«...Кожен повинен мати право на свободу думки і слова: це право включає свободу збирати, отримувати і поширювати інформацію та думки різних видів усно, письмово чи друком, незважаючи на кордони...»

Свобода слова та думки також забезпечується Конвенцією з прав людини,²⁹ ратифікованою в Україні у вересні 1997 р., та двома регіональними системами захисту прав людини, статтею 13 Американської Конвенції з прав людини³⁰ та статтею 9 Хартії прав людини та народів Африки³¹. Посилаючись на Конвенцію з прав людини, Парламентська Асамблея Ради Європи схвалила Рекомендації закликали до вільного доступу до урядових документів та реалізації права на інформацію. Парламентська Асамблея переконувала країни-члени, які ще

²⁷ Резолюція Генеральної Асамблеї ООН 217A(III), 10 грудня 1948.

²⁸ Резолюція Генеральної Асамблеї ООН 2200A(XXI) від 16 грудня 1966, вступила в силу 23 березня 1976.

²⁹ ETS Series No. 5, прийнята 4 листопада 1950, вступила в силу 3 вересня 1953. На 7 липня 2003 підписана 44 країнами.

³⁰ Прийнята 22 листопада 1969, вступила в силу 18 липня 1978.

³¹ Прийнята 26 червня 1981, вступила в силу 21 жовтня 1986.

не схвалили нормативних актів про інформацію, доповнити національне законодавство відповідним регулюванням.

У статті 10 Конвенції з прав людини чітко зазначено, що в країнах-членах Ради Європи свобода доступу кожного до офіційних документів розглядається як засіб публічного нагляду за діями влади і як показник ступеня розвитку демократії.

Для забезпечення свободи інформації та запровадження принципів вільного доступу до документів у Рекомендаціях Ради Міністрів (81) 19, схвалених у 1987 році, були визначені конкретні заходи щодо доступу до інформації, яка знаходиться у розпорядженні органів державної влади³². Згідно з положеннями згаданого документа, для країн-членів ЄС є обов'язковими такі принципи:

1. Всі громадяни країн-членів мають право складати запит на інформацію, яка знаходиться в розпорядженні органів публічної влади.

2. Заборонено відмовляти у запиті на інформацію лише тому, що інформація, на яку складається запит, не стосується особистих інтересів зацікавленої сторони.

3. Кожен запит на інформацію повинен бути розглянутий у визначений термін, а в разі відмови у наданні документів, повинно бути чітко пояснено (обґрунтовано) причини відмови.

4. Доступ до інформації може бути обмеженим лише у випадках, визначених законом, та які стосуються інтересів національної безпеки, громадського порядку, розслідування кримінальних злочинів, або які можуть порушити право на приватність.

ООН визнає право на доступ до інформації як складову права на свободу думки і слова.

У 2002 році Комітет Міністрів Ради Європи прийняв детальну Рекомендацію стосовно доступу до офіційних документів³³, у якій проголошено:

«Загальний принцип доступу до офіційних документів»

Країни-учасниці повинні забезпечити право особи на доступ за запитом до офіційних документів, що належать органам державної влади. Цей принцип повинен застосовуватися в усіх без винятку випадках, без дискримінації на будь-якій основі, у тому числі на основі національності особи.

Можливі обмеження доступу до офіційних документів

1. Країни-учасниці можуть обмежувати право на доступ до офіційних документів. Ці обмеження повинні бути чітко визначені зако-

ном, служити розвитку демократичного суспільства та відповідати меті захисту. Обмеження допускається стосовно інформації про:

- i) національну безпеку, оборону та міжнародні стосунки;
- ii) громадську безпеку;
- iii) попередження, розслідування та переслідування злочинної діяльності;
- iv) особисте життя та інші законні особисті інтереси;
- v) громадські чи приватні комерційні та інші економічні інтереси;
- vi) рівність сторін судового процесу;
- vii) екологічну безпеку;
- viii) інспекцію, контроль та нагляд органів державної влади;
- ix) економічну, грошову та валютну політику держави;
- x) конфіденційність нарад органів державної влади під час внутрішньої підготовки питань.

2. У доступі до офіційного документа може бути відмовлено, якщо оприлюднення інформації, що в ньому міститься, може зашкодити або, скоріше за все, зашкодить інтересам, зазначеним у пункті 1, якщо тільки користь від оприлюднення не переважає потенційної шкоди.

Рада Європи рекомендувала всім країнам-учасникам керуватися цими принципами як у законодавчій діяльності, так і застосовувати їх на практиці³⁴.

Також слід враховувати два важливих документи Article 19 — Право громадськості знати: принципи законодавства про свободу інформації (Принципи Артика 19)³⁵ та Модельний закон про свободу інформації (Модельний закон АРТИКЛА 19).³⁶ Ці документи ґрунтуються на порівнянні світової практики регулювання питань вільного доступу до інформації та використовуються для аналізу інформаційного законодавства країн світу.

У Європі існує ще один базис для захисту права на інформацію — Заключний акт Конференції Організації з безпеки та співробітництва в Європі (ОБСЄ), прийнятий 1 серпня 1975 року. Цей Акт ще раз підтвердив всі зобов'язання, які були зазначені в Загальній декларації та Міжнародних пактах з прав людини. Новим елементом у цьому документі є створення механізмів співпраці країн на практичному рівні щодо скасування будь-яких бар'єрів та обмежень вільного обігу інформації між суспільствами. Документ також запровадив загальноприйнятні стандарти щодо збору та поширення інформації у сфері комерції та промисловості, захисту довкілля, наукових досліджень та новітніх технологій.

³² Recueil des résolutions et recommandations du Comité des Ministres du Conseil de l'Europe relatives au droit administrative avec leurs rapports explicatifs. Document préparé par la Direction des Affaires Juridiques (CJ-DA) (94) Info 1, Strasbourg 1994.

³³ Прийнята 21 лютого 2002.

³⁴ Преамбула.

³⁵ (Лондон: червень 1999.)

³⁶ (Лондон: червень 2001.)

Закріплення права на доступ до інформації широко відображено в Йоганнесбурзьких принципах, які були ухвалені 1 жовтня 1995 року групою експертів з міжнародного права, національної безпеки та прав людини, скликаною Article 19. Цей документ складається з 25 принципів, які визначають право на свободу інформації, обмеження свободи слова, обмеження свободи інформації, засобів правового захисту права на свободу інформації.

Принципом 11 — «Загальні норми доступу до інформації» — передбачено, що «кожна особа має право одержувати інформацію від органів влади, а також інформацію стосовно національної безпеки. На це право не можна накладати жодних обмежень на підставі захисту інтересів національної безпеки, хіба що уряд зможе довести, що це обмеження приписане законом і є необхідним у демократичному суспільстві для захисту законних інтересів національної безпеки».

Міжнародна організація «Article 19» також розробила принципи законодавства про свободу інформації, щоб встановити стандарти, на основі яких будь-хто може визначити, чи насправді закони його країни дозволяють мати доступ до офіційної інформації. До таких принципів відносяться:

1. Принцип максимального оприлюднення: «Законодавство про свободу інформації повинно керуватися принципом максимального оприлюднення». Даний принцип встановлює презумпцію, яка полягає в тому, що вся інформація, яку зберігають державні органи влади, підлягає оприлюдненню і що цю презумпцію може бути подолано тільки в дуже обмеженій кількості випадків. Якщо державна влада намагається заборонити доступ до інформації, вона повинна нести відповідальність щодо обґрунтування відмови на кожному етапі розгляду справи. Інакше кажучи, державна влада повинна довести, що інформація, яку вона бажає приховати, підпадає під сферу режиму винятків.

2. Обов'язок публікувати: «Публічні органи повинні бути зобов'язаними публікувати основну інформацію». Закон повинен встановлювати як загальний обов'язок публікувати інформацію, так і її основні категорії, що підлягають опублікуванню. Публічні органи повинні принаймні бути зобов'язаними опублікувати такі категорії інформації:

- оперативна інформація про те, як публічна адміністрація функціонує, включаючи кошти, цілі, перевірені рахунки, стандарти, досягнення тощо, особливо якщо орган надає безпосередні послуги суспільству;
- інформація на будь-які запити, скарги чи інші безпосередні дії, які члени суспільства можуть здійснити щодо цієї публічної адміністрації;
- інструкції стосовно процедур, через які члени суспільства можуть втрутитися в основну політику чи внести законодавчі пропозиції;

— визначення типів інформації, якими володіє ця інституція і форми, у яких ця інформація зберігається;

— зміст будь-яких адміністративних чи політичних рішень, що впливають на суспільство, разом з причинами прийняття подібних рішень і матеріали щодо обґрунтування їх необхідності.

3. Стимування відкритого уряду: «Публічні органи повинні активно сприяти відкритому уряду». Інформування громадян про їхні права і сприяння культурі відкритості уряду є головним, що має на меті здійснення законодавства про свободу інформації.

4. Обмежена сфера винятків: «Винятки повинні бути зрозумілими, описуватися вузько і підлягати суворому контролю стосовно категорій «шкоди» і «суспільних інтересів». Відмова державних органів оприлюднити інформацію є не виправданою, якщо вони не можуть довести, що інформація пройшла «триєтапний тест», який містить такі вимоги: (1) інформація повинна мати відношення до легітимної мети, передбаченої законом; (2) оприлюднення інформації повинно зарожувати спричиненням суттєвої шкоди вказаній легітимній меті; (3) шкода, яка може бути заподіяною вказаній меті, повинна бути ватомішою, ніж суспільний інтерес в отриманні інформації.

5. Процедура отримання доступу: «Запити стосовно надання інформації повинні опрацьовуватися швидко і справедливо, а перетяг відмов має бути доступним і незалежним». Процес прийняття рішень стосовно інформаційних запитів повинен здійснюватися на трьох різних рівнях: на рівні публічного органу; апеляції до незалежного адміністративного органу; апеляції до суду.

6. Кошти: «Надмірна вартість не повинна перешкоджати особам подавати інформаційні запити». Кошти, які отримують публічні органи за надання доступу до інформації, не повинні бути настільки високими, щоб стримувати потенційних заявників.

7. Відкриті засідання: «Засідання публічних органів повинні бути відкритими для громадськості».

8. Оприлюднення створеного прецеденту: «Закони, які суперечать принципу максимального оприлюднення, повинні бути змінені або скасовані».

9. Захист інформаторів: «Особи, які передають інформацію про правопорушення (інформатори), повинні бути захищеними».

Право на доступ до інформації повинно забезпечуватися, у першу чергу, наявністю відповідного ефективного законодавства, що є правовою підставою забезпечення здійснення конституційного права людини на свободу інформації, а також наявністю реальних механізмів здійснення цього права.

Традиційно право на доступ до інформації асоціюється з досвідом Сполучених Штатів Америки. Однак першими країнами, у яких громадяни одержали право на інформацію, були скандинавські країни:

Швеція (де конституційний Закон про свободу преси був прийнятий Рікстагом у 1766 р.), а потім через два століття Фінляндія (Закон 1951 р.). У 1966 році був прийнятий Закон Сполучених Штатів Америки про свободу інформації, у якому були представлені нові інтерпретації і нові легітимні форми захисту свободи інформації. У 1970 р. аналогічні закони були прийняті в Данії і Норвегії, у 1973 р. — в Австрії, у 1978 р. — у Франції і Нідерландах, 1982 р. — в Австралії, Новій Зеландії і Канаді, у 1990 р. — в Італії, у 1992 р. — в Угорщині, у 1993 р. — у Португалії, у 1994 р. — у Бельгії, у 1997 р. — в Ірландії і Тайланді, у 1998 р. — у Кореї й Ізраїлі, а 1999 р. — у Чеській Республіці і Японії, у 2001 р. — у Польщі. У згаданих країнах відкритість стала законним принципом, а таємність — винятком³⁷.

Після розпаду тоталітарного режиму в країнах Центральної і Східної Європи з'явилися сприятливі умови для запровадження інституційних механізмів захисту свободи інформації. Той факт, що практично в усіх країнах були прийняті нові конституції та запроваджена сучасна правова система, дав можливість поставити питання свободи інформації на центральне місце в законодавстві.

Незважаючи на те, що Законами України «Про інформацію»³⁸ та «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації»³⁹ визначено, що держава гарантує вільний доступ до відкритої інформації, на сьогодні немає нормативного акта на рівні закону, який би повною мірою регулював питання доступу громадян до інформації взагалі, а тим більше до інформації про діяльність органів державної влади та вищих посадових осіб. Однак є певні позитивні зрушення. Зокрема, народним депутатом України С.П. Головатим на розгляд Верховної Ради було внесено **Проект Закону № 2082 від 20.08.2002 «Про інформаційну відкритість органів державної влади та вищих посадових осіб України»**. Цей проект передбачає запровадження правил, які забезпечують більшу інформаційну відкритість органів державної влади та вищих посадових осіб України. Ним пропонується охопити питання щодо обов'язкового оприлюднення інформації про органи державної влади та про вищих посадових осіб України. Законопроект покликаний сприяти встановленню юридичної основи здійснення права людини на доступ до інформації про органи державної влади та вищих посадових осіб, що забезпечить громадянам право активно брати

участь у політичному житті держави, а також впливати на ті чи інші політичні процеси.

Однак, зважаючи на сучасні реалії і практику, навіть за умови прийняття такого закону найбільш надійною гарантією його реалізації є наявність ініціативи з боку органів виконавчої влади щодо підтримання відкритості своєї інформації. Але в Україні, по-перше, така гарантія відсутня, а, по-друге, їй притаманний суб'єктивний і непостійний характер.

2.1.2. Правові режими доступу до інформації. Класифікація інформації

Відповідно до Закону України «Про інформацію», здійснення права на отримання інформації безпосередньо пов'язане з поняттям **режиму доступу до інформації**. Режим доступу до інформації визначається як передбачений правовими нормами порядок отримання, використання, розповсюдження і зберігання інформації. Залежно від режиму доступу інформація поділяється на **відкриту інформацію та інформацію з обмеженням доступу** (стаття 28 Закону України «Про інформацію»). Доступ фактично є певною дозволеною процедурою, яка полягає в отриманні згоди компетентного органу (особи) на одержання документа чи інформації, отримання якої безпосередньо пов'язане з можливістю реалізації права на інформацію, та, відповідно, обмежує це право. Наведена класифікація викликає низку суперечностей у її застосуванні. По-перше, встановлення режиму доступу за цитованою нормою може застосовуватись і щодо відкритої інформації, що суперечить ст. 29 Закону України «Про інформацію», яка забороняє обмеження права на одержання відкритої інформації. По-друге, класифікація інформації за ознакою наявності процесуальної процедури її отримання — встановлено певний режим доступу, інформацією слід уважати інформацію з обмеженням доступу, якщо ні — то це відкрита інформація, без оцінювання змісту інформації як підстави для обмеження доступу до неї — не узгоджується з конституційною нормою про право на інформацію⁴⁰.

У свою чергу, **інформація з обмеженням доступу** поділяється на **конфіденційну і таємну**. До **таємної інформації** належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі. Порядок обігу таємної інформації та її захист визначається відповідними державними органами за умови додержання

³⁷ Гончарук Я., Гнидюк Н. Свобода інформації та виконавча гілка влади: Правові норми. Інституції. Процедура. — К., 2002. — С. 68.

³⁸ Закон України «Про інформацію» від 02.10.1992 № 2657-XII.

³⁹ Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» від 23.09.1997 № 539/97-ВР.

⁴⁰ Субота Н. Конфіденційна інформація, що є власністю держави: вид інформації з обмеженням доступу чи засіб обмеження доступу до відкритої інформації // Юридичний журнал. — 2003. — № 9 (15).

вимог, встановлених цим Законом (стаття 30 Закону «Про інформацію»).

Оскільки ст. 21 Закону «Про інформацію» передбачає, що джерела і порядок одержання, використання, поширення та зберігання офіційної інформації державних органів всіх рівнів визначаються актами законодавства про ці органи, то можна очікувати, що вони можуть бути відображені у відповідних законах, наприклад Законах «Про міліцію» (1990 р.) або «Про службу безпеки України» (1992 р.). Наприклад, ст. 3 Закону України «Про міліцію» забороняє розголошення відомостей, які становлять службу таємнистю, а ст. 7 Закону «Про Службу безпеки України» — військову, службу, комерційну таємницю, проте визначення цих термінів у законі немає. Тому, можливо, віднесення інформації до категорії таємної визначається та регулюється внутрішньовідомчими актами та інструкціями, і підставою до їх створення може бути лише ст. 37 Закону «Про інформацію», яка містить загальні положення про інформацію, що не підлягає розголошенню згідно з іншими законодавчими або нормативними актами. Відомо, що не всі внутрішньовідомчі акти публікуються в офіційних виданнях, і, таким чином, державні органи стають подібними до власників інформації, які на власний розсуд приймають рішення про надання або відмову у наданні інформації⁴¹.

Законодавством України чітко не визначено, яка саме інформація захищається державою. Із наведених норм видно, що тільки законом може бути встановлено, яку інформацію слід відносити до категорії таємної. У цій сфері у нас є лише один закон — **Закон України «Про державну таємницю»**⁴² від 21 січня 1994 року. Тому грифи, якими державні органи щедро наділяють різні правові акти (укази і розпорядження Президента, постанови, інструкції, накази органів виконавчої влади тощо) — «служба таємниці», «для службового користування», «не для друку» — є самочинними і незаконними. Законними можна визнати тільки такі грифи секретності як «особливо таємно», «цілком таємно», «таємно», які визначені Законом України «Про державну таємницю».

Утім, навіть якщо на документи ставляться грифи «служба таємниці», «не для друку» тощо, то повинні існувати відповідні процедури надання та зняття цих грифів, визначатися підстави для таких дій. Вочевидь потрібним є також і регламент організації доступу до документів. Проте офіційно зареєстрованих Міністерством юстиції нормативних актів щодо порядку роботи з документами, які мають грифи «служба таємниці», «не для друку», взагалі не існує.

Що ж до порядку роботи з документами, які мають **гриф «для службового користування»** (ДСК), то він був схвалений КМУ у Постанові № 1813 від 27 листопада 1998 року «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави». Згідно з п. 2 Постанови, центральні і місцеві органи виконавчої влади та органи місцевого самоврядування повинні у шестимісячний термін розробити і ввести в дію переліки конфіденційної інформації, що є власністю держави. Цій інформації надається гриф ДСК. Хто саме і виходячи з яких критеріїв повинен вирішувати, які саме відомості є конфіденційними, Інструкція не визначає. Також не зрозуміло, чи будуть доступні ці переліки для широкого загалу. Адже мало не кожне відомство відтепер може мати подібний перелік. Можливо, логічно прийняти «Звід відомостей, які віднесені до конфіденційної інформації, що є власністю держави»⁴³.

Також зазначений порядок передбачає:

— здійснення контролю за нерозголошення відомостей, що містяться в документах з грифом «Для службового користування» режимно-секретними підрозділами організації;

— надання громадянам доступу до інформації, що міститься в документах з грифом «Для службового користування», лише за наявності письмового запиту від організації, в якій працює громадянин, за згодою працівника установи або в масових бібліотеках за аналогічним письмовим клопотанням;

— надання представникам ЗМІ доступу після попереднього розгляду конкретних документів експертними комісіями за письмовим дозволом керівника установи, що надала документів гриф «Для службового користування».

При такій ситуації інформація, що потрапила до державного органу, може стати конфіденційною завдяки рішенняно керівника цього органу, про що її творець (першоджерело) може навіть не здогадуватися.

Процедура доступу за Інструкцією, що передбачає застосування грифу, його обмеження, встановлення порядку роботи з документами та їх зберігання, умов технічного захисту інформації, функціонування експертних комісій як органу для вирішення питання доступу до інформації для «сторонніх», нагадує порядок, установлений стосовно інформації, що є державною таємницею. Суттєва відмінність полягає

⁴¹ Гончак Я., Гнидок Н. Свобода інформації та виконавча гілка влади... — С. 95.

⁴² Закон України «Про державну таємницю» від 21.01.1994 № 3855-ХІІ.

⁴³ Захаров Євген, Рапа Ірина. Доступ до інформації: починаємо заново? // www.kituka.kiev.ua.

в тому, що суспільні відносини пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці, регулюються відповідним законом, яким, до речі, чітко встановлено перелік інформації, яка не може бути віднесена до державної таємниці, та збороняється віднесення до державної таємниці будь-яких відомостей, якщо цим будуть зважуватися зміст і обсяг конституційних прав і свобод людини та громадянина. Користуючись же положенням зазначеної вище Інструкції, державні органи не позбавлені можливості присвоїти гриф «для службового користування» практично кожному документові, обмеживши в такий спосіб доступ до інформації, що міститься в такому документі. У кінцевому рахунку маємо ще один вид інформації з обмеженим доступом, яка за відсутності будь-яких правил стосовно змісту та обсягу інформації, що підлягає «грифуванню», фактично утаємничується від заінтересованих осіб⁴⁴.

Досліджуючи питання **можливості існування в держави власної конфіденційної інформації** взагалі, слід акцентувати увагу на таких законодавчих положеннях. Власністю держави вважається інформація, що створена коштом державного бюджету (ст. 38 Закону України «Про інформацію»), відповідно держава є власником інформації, що створюється в процесі діяльності державних органів, а останні здійснюють володіння, користування і розпорядження такою інформацією. Конфіденційна інформація у ст. 30 Закону визначається як відомості, що перебувають у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюються за їхнім бажанням відповідно до передбачених ними умов. Органи державної влади та органи місцевого самоврядування в ч.ч. 2, 3 і 4 Закону «Про інформацію» не згадуються серед осіб, які мають право самостійно визначати належність певної інформації до категорії конфіденційної, встановлювати порядок доступу до такої інформації та систему її захисту. Крім того, державні органи відповідно до ст. 19 Конституції України мають діяти тільки на підставах, у межах повноважень і способом, передбаченими Конституцією України і законами України, що не допускає застосування таких категорій, як «поширення інформації за бажанням держави» та «самостійне визначення державним органом порядку доступу до інформації». Отже, існування конфіденційної інформації, що є власністю держави, не узгоджується з наведеними вище нормами⁴⁵.

Конфіденційну інформацію можуть мати у власності лише фізичні та юридичні особи, що не є органами державної влади та органами місцевого самоврядування, тобто юридичні особи приватного права. Перебування такої інформації у володінні чи користуванні державних органів у зв'язку зі здійсненням останніми своїх функцій не позбавляє її статусу конфіденційної інформації приватних осіб, так як і не надає такій інформації статусу конфіденційної, що належить державі чи державному органу. Застосування подібного підходу повністю відповідає чинному законодавству та забезпечує як дотримання прав зацікавлених осіб на одержання інформації держави, так і дотримання прав осіб у частині захисту конфіденційної інформації, оскільки підстав для розкриття конфіденційної інформації за наявності застереження щодо допустимості таких дій з боку її власника державні органи не мають⁴⁶.

Також на сьогодні суттєво розширеним став обсяг **інформації, яка засекречується**. До інформації у сферах оборони, економіки, зовнішніх відносин, державної безпеки та охорони правопорядку, яка може бути віднесена до державної таємниці, відтепер додана також інформація у сфері науки і техніки, а саме інформація «про наукові, науково-дослідні, дослідно-конструкторські та проектні роботи, на основі яких можуть бути створені прогресивні технології, нові види виробництва, продукції та технологічних процесів, що мають важливе оборонне чи економічне значення або суттєво впливають на зовнішньоекономічну діяльність та національну безпеку України» (ст. 8 Закону України «Про державну таємницю»). У сфері державної безпеки і правопорядку з'явилися нові позиції: до державної таємниці може бути віднесена інформація «про особовий склад органів, що здійснюють оперативно-розшукову діяльність», «про організацію режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, державні програми, плани та інші заходи у сфері охорони державної таємниці», «про організацію, зміст, стан і плани розвитку технічного захисту секретної інформації» та «про результати перевірок, здійснюваних згідно з законом прокурором у порядку відповідного наглядку за додержанням законів та про зміст матеріалів дізнання, досудового слідства та судочинства з питань, зазначених у цій статті сфер»⁴⁷.

Таким чином, одна з найактуальніших проблем, що пов'язана із забезпеченням права громадян на доступ до публічної інформації в Україні, — це наявність та широке неправомірне застосування грифів обмеження доступу до інформації.

⁴⁴ Субота Н. Конфіденційна інформація, що є власністю держави: вид інформації з обмеженим доступом чи засіб обмеження доступу до відкритої інформації // Юридичний журнал. — 2003. — № 9 (15).

⁴⁵ Там само.

⁴⁶ Там само.

⁴⁷ Захаров Євген, Рапп Ірина. Доступ до інформації: починаємо заново? ...

Для того щоб знайти для України оптимальний варіант вирішення описаних вище проблем, слід звернутися до практики зарубіжних країн.

Такі країни, як Австрія і Швеція, забезпечують конституційне право доступу до інформації, яка належить уряду. В Конституції *Австрії* визначено загальне право доступу до інформації, згідно з яким державні установи, наділені владними повноваженнями, зобов'язані розголошувати інформацію, яка перебуває в межах їхньої компетенції. Єдиним винятком є зобов'язання службовців зберігати таємницю для захисту певних інтересів. Конституція делегує виконання положень, які стосуються цих прав Бундсерату та Націоналісту (Верхня та Нижня палати парламенту відповідно), згідно з їхніми повноваженнями. Конституція *Швеції* проголошує свободу інформації та також визначає певні обмеження з цього права. Одночасно робиться посилання на Закон Про свободу преси від 1766 року (зі змінами, внесеними в 1994) і на положення, що стосуються права доступу до публічних документів. Цей доступ обмежений щодо офіційних документів, тобто документів, що зберігаються органами влади, якщо вони розглядаються як такі, що були отримані, опрацьовані або узатягнені органом влади. Зазвичай документ класифікується як офіційний, у разі якщо він відповідає певному рівню завершеності, або якщо він відправляється за межі органу влади. Внутрішні документи або попередні нарисы чи проекти рішень вважаються офіційними документами лише у разі, якщо вони приймаються для архівування та реєстрації. Закон також подає перелік документів, які не вважаються офіційними документами. Винятки з права доступу зазначені в ст. 12 Закону, згідно з положеннями якої, органи влади мають право відмовити в доступі до офіційних документів лише у разі необхідності захисту окремих інтересів (державна безпека, відносини з іноземними країнами та міжнародними організаціями; грошова політика; наглядова діяльність органів влади; попередження або викриття злочину; публічні економічні інтереси, захист особистого життя; збереження тварин та різновидів рослин)⁴⁸. Хоча шведське право забезпечує широкий доступ до більшості урядових документів, на практиці влада відмовляє в інформації, яка б могла поставити уряд в незручне становище. Найвідомішим прикладом є справа Бофора. Після того як журналісти повідомили, що Бофор — найбільший виробник зброї у Швеції — уклав контракт з урядом Індії, уряд провів розслідування і підготував відповідь, частину якої відмовився оприлюднити. Тільки після опублікування в індійській газеті найбільш дискредитуючих уривків, уряд оприлюднив звіт повністю.

Теоретико-правові та практичні засади доступу до інформації

Згідно з *голландським законодавством*, влада може відхилити запит на інформацію без урахування балансу інтересів, якщо її розголошення загрожуватиме єдності Корони, державній безпеці або захисту інтересів приватних осіб⁴⁹.

У *США* та *Німеччині* конституційне право доступу до інформації закріплене положеннями нормативних актів, що гарантують свободу вираження поглядів та свободу преси. У США таке право є в кожного громадянина (як стверджує Закон про свободу інформації). Навпаки, у Німеччині тільки представники засобів масової інформації мають право доступу до урядової інформації, що гарантовано п. 2 статті 5 Конституції. Право на інформацію, яка належить урядом земель, гарантовано законодавчими актами земель про свободу преси (наприклад, Закон Землі Бранденбург, Закон про свободу інформації Землі Берлін).

Конституція Іспанії визнає право громадянності на доступ до урядової інформації, крім тих випадків, коли її розголошення зачіпало б безпеку держави, розслідування злочинів або приватне життя громадян. Порядок надання секретної інформації визначається відповідним законодавством. Існує також Закон Іспанії «Про правила діяльності державної адміністрації та адміністративні процедури», положення якого передбачають право громадян на доступ до реєстрів та документів, якими володіє адміністрація. Згідно з цим Законом громадяни мають право на доступ до реєстрів та документів, які формують частину досьє та зберігаються в адміністративних архівах. Досьє можуть стосуватися питань, які були завершені в момент складання запиту. Право доступу не застосовується до специфічних питань, таких як неадміністративні питання; інформація про питання національної безпеки та державної оборони; документи, які стосуються кримінальних процесів та розслідувань, що здійснюються; комерційної та промислової таємниці; грошової політики. Існує спеціальний механізм захисту документів, які стосуються особистого життя, та певних документів, які мають відношення до судочинства, яке здійснюється при захисті громадянських прав. Органи влади можуть відмовити в доступі до інформації у таких трьох випадках: у випадку захисту публічних інтересів, спеціальних інтересів третіх осіб, або у разі, коли це заборонено законом⁵⁰.

У *Франції* 1979 року до загального закону, який надає доступ до адміністративних документів (1978), було внесено певні зміни Законом «Про обґрунтування адміністративних документів та про покращення відносин між адміністрацією та громадськістю». У 2000 році в

⁴⁸ Гоншяк Я., Гнилюк Н. Свобода інформації та виконавча гілка влади... — С. 42, 48.

⁴⁹ Закони та практика ЗМІ у одиницях демократії світу (порівняльний аналіз) / ARTICLE 19, Харківська правозахисна група. — Харків: Фоно, 2000. — 200 с.

⁵⁰ Гоншяк Я., Гнилюк Н. Свобода інформації та виконавча гілка влади... — С. 47.

згадані закони вносились зміни з метою представити їх у більш узгоджений та комплексний спосіб. Цей Закон розмежовує нормативні та ненормативні акти, останні потім доопрацьовуються в окреме законодавство. Закон визначає перелік виключень, відповідно до яких органи влади можуть відмовити у доступі до документів, якщо розкриття інформації може завдати шкоди захищеним інтересам. До захищених інтересів відносяться: секретні обговорення уряду або органів, наділених владними повноваженнями, національна безпека, зовнішні відносини, грошова політика, державна безпека та громадський порядок, процесуальні дії, особисті справи або документи, які стосуються особистого життя, документи, що стосуються порушення податкових або митних правил чи державних секретів. Право доступу не поширюється на проекти документів та на документи, якіносять підготовчий характер до тих пір, поки вони не були схвалені. Закон регулює дві групи документів з обмеженим доступом. Перша група містить винятки з метою захисту публічних інтересів та забороняє обіг документів, оприлюднення яких може бути згубним для специфічних публічних інтересів, про які вже говорилося вище. Друга група стосується доступу до нормативних документів, розкриття яких може завдати шкоди приватності особистого життя, медичним секретам, комерційним та промисловим таємницям. Згідно із положеннями закону лише захищені особи мають право доступу до цієї категорії документів⁵¹.

Великобританія — єдина країна, яка довгий час не мала законодавства про доступ до інформації, і в якій тривалий час презюмувалося необхідність збереження урядової таємниці. Однак у 2000 році з прийняттям Закону «Про свободу інформації» було запроваджено процедур розголошення інформації, якою володіють органи державної влади чи особи, які надають послуги громадянам. При розголошенні інформації з обмеженим доступом застосовується тест «заподієйної шкоди», якщо її розкриття може заподіяти шкоду певним інтересам (напр., у випадках питань охорони здоров'я та безпеки, доступ до неї обмежено, якщо її розголошення може зашкодити фізичному або психічному стану особи). Положення Закону чітко не визначають випадки, у яких органи влади повинні застосовувати простий або комплексний тест «заподієйної шкоди» (Біла книга запропонувала застосовувати комплексний тест майже у всіх сферах діяльності. Однак у випадку інформації, пов'язаної із «забезпеченням узгодженого процесу розробки політики та політичних консультацій в уряді» — простий тест «заподієйної шкоди»). Обмеження доступу до інформації визначаються залежно від виду документа та його змісту, як у випадку з інформацією, пов'язаною з питаннями національної безпеки або з

діяльністю органів, що відповідають за питання безпеки; інформацією, якою володіють органи влади з метою судового розгляду або розслідування; записи органів судової влади; інформацією, яка пов'язана з розробкою державної політики; інформацією, що була надана конфіденційно, кореспонденцією з Ї Величністю Королевою та ін. Але навіть у випадку, коли органи влади згідно з положеннями Закону не повинні задовольняти запити на інформацію, Закон вимагає застосування тесту «публічних інтересів» та розголошення інформації, якщо публічні інтереси переважують у даній справі. У такому випадку органи влади повинні застосовувати двоступінчасту перевірку: по-перше, визначити, чи належить інформації до категорії з обмеженим доступом (і якщо це так, то застосувати тест «заподієйної шкоди»), і по-друге — розглянути публічні інтереси при розкритті інформації⁵².

Таким чином, виходячи із зарубіжного досвіду і положень Рекомендації Ради Європи № R(2002)2 про доступ до офіційних документів, можна виокремити певні ідеї, правила, дотримання яких сприятиме здійсненню права громадян на доступ до інформації в Україні:

По-перше, це максимальна відкритість з боку органів виконавчої влади. Це означає, що будь-яка інформація, якою володіє орган влади, повинна бути відкрита і доступна, за винятком чітко визначеного переліку відомостей, доступ до яких обмежується на основі закону, а з боку органів виконавчої влади повинна виходити ініціатива щодо підтримання відкритості своєї інформації. Окрім цього, склади входить обов'язок опублікування основної інформації про діяльність органів виконавчої влади.

По-друге, це правомірне обмеження доступу до інформації. При цьому перелік відомостей, які входять до кола обмежень, має бути вичерпно визначений і оприлюднений. У даному випадку необхідно також дотримуватися двох принципів. Перший — принцип максимального оприлюднення: вся інформація, яку зберігають державні органи влади підлягає оприлюдненню, винятки можуть бути тільки для дуже обмеженого числа випадків. Другий принцип характеризує вимоги щодо обмежень: а) винятки повинні бути зрозумілими; б) описуватися вузько; в) підлягати контролю на предмет наявності «шкоди» і впливу на «суспільний інтерес». А саме: рішення державного органу обмежити доступ до інформації є виправданим, якщо, по-перше, інформація має відношення до легітимної мети, передбаченої законом; по-друге, її оприлюднення має дійсно загрожувати спричиненням шкоди легітимній меті; по-третє, шкода, яка може бути запо-

⁵¹ Там само. — С. 44, 63.

⁵² Там само. — С. 66—67.

діяна вказаній меті, повинна бути вагомішою, ніж суспільний інтерес в отриманні інформації⁵³.

Наприклад, в Австрії існує практика, відповідно до якої у разі виникнення попиту на секретну інформацію, представники влади мають право вирішувати, чи зберігати конфіденційність, чи задовольнити зацікавленість громадськості і розкрити її.

По-третє, має бути чітко визначена процедура отримання інформації, відповідальність за її надання. Ідеться про те, що всі формальності при отриманні промадянином доступу до інформації повинні бути обґрунтовані і визначені в законі, а відмова в наданні може бути фактично оскаржена. Окрім цього, на законодавчому рівні необхідно встановити санкції щодо винних посадових осіб, які перешкоджають законному отриманню громадянином інформації.

Цей підрозділ в основному розкрив зміст інформації, виходячи з критерію доступу до неї. Однак класифікувати інформацію можна й за іншими ознаками:

а) за видами інформації (відповідно до статті 18 Закону України «Про інформацію»): статистична інформація; адміністративна інформація (дані); масова інформація; інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування; правова інформація; інформація про особу (інформація персонального характеру, персональні дані); інформація довілково-енциклопедичного характеру; соціологічна інформація.

б) за ступенем систематизації — систематизована в інформаційних системах (каталоги, енциклопедії, рубрикатори і т.д.) і несистематизована інформація, тобто вільна;

в) за видом носія — на паперовому, відео — і звукова, комп'ютерна інформація;

г) за сферою застосування — масова інформація, що поширюється через ЗМІ, Інтернет, і газету, для певного кола осіб, пов'язана з професійними інтересами.

Така класифікація має, швидше, науково-теоретичний характер, але в багатьох випадках, залежно від умов і сфер використання інформації, може також мати і вагомe практичне значення.

2.1.3. Правове регулювання інформації персонального характеру

Як зазначалося в кінці попереднього підрозділу, одним із видів інформації є інформація про особу.

У міжнародному законодавстві інформація персонального характеру отримала свій захист з прийняттям 10 грудня 1948 року Генераль-

ною Асамблеєю ООН Загальної декларації прав людини, у статті 12 якої зазначається:

«...Ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його життя, тайну його кореспонденції або на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань».

Європейська Конвенція про захист прав та основних свобод сприяла захисту такої інформації через право кожної людини «на повагу» до її особистого та сімейного життя.

Спершу до проблеми захисту персональних даних на міжнародному рівні звернувся Організація з економічного співробітництва і розвитку (ОЕСР), що прийняла у 1980 р. Директиву про захист недоторканності приватного життя і міжнародних обмінів персональними даними, у якій були зафіксовані основні принципи роботи з персональними даними. Ці принципи були розвинені і конкретизовані в Міжнародній конвенції «Про охорону особи стосовно автоматизованої обробки персональних даних» (1981 р.), яка стала основою для відповідного національного законодавства. Надалі система захисту персональних даних розвивалася в Директиві Європейського Союзу і Парламенту 95/46/ЄС від 24 жовтня 1995 р. про захист прав приватних осіб щодо опрацювання персональних даних і вільного руху таких даних і Директиві 97/66/ЄС від 15 грудня 1997 р. щодо опрацювання персональних даних і захисту конфіденційності в телекомунікаційному секторі⁵⁴.

У розвинутих країнах (США, країнах ЄС) було розроблено законодавство з питань захисту персональних даних — прийнято понад 25 національних нормативних спеціалізованих актів, до того ж деякі з них доопрацьовані і змінені у зв'язку з розвитком телекомунікацій. При цьому можна зауважити, що сучасні закони інколи намагаються враховувати особливості отримання, зберігання, опрацювання і використання персональних даних в Інтернеті. Зокрема, останніми роками в США ведуться дебати з приводу питання щодо необхідності розробити закон про недоторканність приватного життя для приватного сектора. Попередній склад контресеу розглядав понад 100 законопроектів про невтручання в приватне життя, у тому числі про недоторканність генетичних і медичних даних; інформації, яка поширюється через мережу Інтернет; приватне життя дітей і т.д. Потодженням був лише один законопроект, що стосувався отримання персональної інформації через Інтернет від дітей. На сьогодні Білий дім і приватний

⁵³ Захаров Є. Свобода висловлювань і приватність. — 2001. — № 1.

⁵⁴ Захита персональних даних: опыт правового регулирования. — М.: Галерия, 2001. — 236 с.

сектор загалом покладаються на саморегулювання і вважають, що нові закони не потрібні — крім деяких поправок до правил ведення медичного обліку. Сьогодні конгресмени намагаються покращити закон про недоторканість фінансового життя громадян, заборонивши банкам продавати персональні дані клієнтів без їхнього дозволу, однак ця пропозиція зустрілась із серйозним опором з боку банків. У деяких штатах, в тому числі в Каліфорнії, Нью-Йорку і Массачусетсі, спостерігається підвищена суспільна активність у зв'язку з розглядом там законопроектів про всебічний захист приватного життя громадян⁵⁵.

Підходи різних країн до законодавчого регулювання роботи з персональними даними мають певну національну специфіку, однак слід виділити ряд загальних рис, що очевидно пов'язані з потребою гармонізації європейського законодавства з національним⁵⁶.

По-перше, створюється національне законодавство (включаючи підзаконні акти), що дозволяє регулювати відносини, пов'язані з отриманням, зберіганням, автоматичною обробкою і використанням персональних даних. До того ж частіше за все це законодавство створюється як самостійне поряд із загальним законодавством про захист права на недоторканність особистого життя і забезпечує:

- захист персональних даних осіб від несанкціонованого доступу до них з боку інших осіб, у тому числі і представників державних органів і служб, що не мають на те необхідних повноважень;
- забезпечення збереженості, цілісності і достовірності даних у процесі роботи з ними, у тому числі і при передачі міжнародними комунікаціями;

— забезпечення належного правового режиму цих даних при роботі з ними для різноманітних категорій суб'єктів персональних даних;

— забезпечення контролю за використанням персональних даних з боку самого суб'єкта⁵⁷.

По-друге, створюється спеціальна інституційна інфраструктура, що забезпечує ефективний нагляд за дотриманням прав суб'єктів персональних даних (наприклад, інститути Уповноважених з питань захисту персональних даних). Чверть століття функціонує цей інститут у країнах Європи, він довів свою ефективність і гарантує право доступу суб'єкта до інформації про себе і контроль за належним використанням баз, що містять персональні дані. У деяких країнах апарат Уповноважених несе достатньо велике навантаження, реєструючи і розглядаючи за рік понад 10 тисяч заяв громадян⁵⁸.

⁵⁵ Там само.

⁵⁶ Там само.

⁵⁷ Там само.

⁵⁸ Там само.

Інститут Уповноважених з питань захисту персональних даних ґрунтується на принципах функціонування інституту омбудсмена і є розвиненою самостійною незалежною структурою, що доповнює традиційні інститути державної влади. Створення незалежного інституту, вочевидь, пов'язане з необхідністю контролювати діяльність різних гілок державної влади і створення більш доступного для суб'єктів персональних даних і оперативно-діючого механізму захисту їхніх прав.

З метою запобігти таким порушенням основних прав людини, як незаконне поширення персональних даних, зберігання неправдивих персональних даних, а також несанкціоноване використання чи опублікування таких даних, і одночасно не завадити вільному обміну персональними даними між країнами, країни-члени **ОЕСР** вважали за необхідне розробити **Основні положення** про захист недоторканності приватного життя і міжнародних обмінів персональними даними.

Основні положення, прийняті в формі **рекомендацій Ради ОЕСР**, були розроблені групою експертів, яку очолював суддя М.Д. Кірбі. Рекомендації були прийняті і вступили в силу 23 вересня 1980 р.

Основні положення **визначають два види принципів** застосування:

- а) на національному рівні;
- б) на міжнародному рівні.

На національному рівні:

— принцип обмеження обсягу даних, що збираються (всі дані повинні отримуватися законним і чесним чином — якщо можливо, з відомо або згоди суб'єкта даних);

— принцип якості даних (дані повинні бути повними і регулярно оновлюватись);

— принцип конкретизації мети, з якою дані збираються і використовуються;

— принцип обмежень на використання даних полягає в можливості їх використання лише відповідно до принципу конкретизації мети або, якщо:

- а) суб'єкт даних дає на те свою згоду;
- б) це дозволено законом;

— принцип забезпечення безпеки (має мати місце належний механізм захисту від ризиків, втрат, несанкціонованого доступу, знищення чи використання);

— принцип відкритості (відкритість за наявності дотримання умов доступу);

принцип індивідуальної участі полягає в тому, що індивід має мати право:

- а) отримувати від розпорядника відомості про наявність у нього персональних даних щодо індивіда;

б) отримувати персональні дані щодо себе в розумні терміни, у межах розумної процедури, за помірну плату (якщо плата передбачена) і в зручній для розуміння формі;

в) у разі відмови отримати роз'яснення щодо мотиву відмови та можливість її опротестувати;

г) опротестовувати дані, і вимагати їх знищення, виправлення чи доповнення;

— принцип відповідальності розпорядника даних за дотримання перелічених вище принципів.

На міжнародному рівні:

— врахування можливих наслідків;

— вживання засобів для забезпечення безперешкодного міжнародного обміну персональними даними;

— сприяння обміну даними.

Пояснювальний меморандум, що додається до основних положень, вказує, що однією з характерних рис діяльності країн-членів ОЕСР протягом останніх десятиліть є розробка законів про захист недоторканості приватного життя.

Група експертів, які готували Основні положення, вважала за необхідне супроводити їх **пояснювальним Меморандумом**. У першій його частині міститься інформація з питань, що цікавлять країни-члени.

Друга частина складається з 2 підрозділів:

1) коментар із загальних питань Основних положень

2) коментар окремих пунктів.

Окрім принципів, **метою** Основних положень є:

— досягнення країнами-членами певних мінімальних стандартів захисту недоторканості приватного життя та індивідуальних свобод щодо персональних даних;

— зведення до мінімуму суперечностей між правилами і практикою у країнах-членах;

— забезпечення дотримання інтересів країн-членів у процесі захисту персональних даних і уникнення непотрібних перепон на шляху обміну персональними даними між країнами-членами;

— усунення причин, наскільки це можливо, які б могли спровокувати країни-члени відмовитися від міжнародного обміну інформацією.

У Страсбурзі 28 січня 1981 року було прийнято **Конвенцію № 108 про захист осіб стосовно автоматизованої обробки персональних даних**.

Метою цієї Конвенції є забезпечення на території кожної Сторони для кожної особи незалежно від її національності або проживання, поваги її прав і основних свобод, і зокрема її права на приватність, стосовно автоматизованої обробки персональних даних, що її стосуються («захист даних»).

Для цієї цілі Конвенції використовуються такі визначення:

а) **«персональні дані»** означають будь-яку інформацію, що стосується ідентифікованої особи або особи, яка може бути ідентифікована («суб'єкт даних»);

б) **«файл даних для автоматизованої обробки»** означає будь-який масив даних, що підлягає автоматизованій обробці;

с) **«автоматизована обробка»** включає такі операції, що здійснюються повністю або частково за допомогою автоматизованих засобів: зберігання даних, виконання логічних і/або арифметичних операцій з цими даними, зміна, знищення, пошук або поширення даних;

д) **«контролер файлу»** означає фізичну чи юридичну особу, державний орган, установу або будь-який інший орган, що має повноваження відповідно до національного законодавства вирішувати питання щодо цілей файлу даних для автоматизованої обробки, категорій персональних даних, що мають зберігатися, та операцій, які мають здійснюватися з ними.

Для забезпечення належної якості персональних даних, що підлягають автоматизованій обробці, вони:

а) отримуються та обробляються правомірно та законно;

б) зберігаються для визначених і законних цілей та не використовуються у спосіб, несумісний з цими цілями;

с) повинні бути адекватними, відповідними і не надмірними з точки зору цілей, заради яких вони зберігаються;

д) повинні бути точними та в разі необхідності оновлюватися;

е) зберігаються у формі, яка дозволяє ідентифікувати суб'єктів даних не довше, ніж це необхідно для цілі, заради якої такі дані зберігаються.

Мають місце також **особливі категорії даних**. До них відносять персональні дані, що свідчать про расову належність, політичні погляди або релігійні чи інші переконання, а також персональні дані, що стосуються здоров'я або статевого життя. Ці дані не можуть піддаватися автоматизованій обробці, якщо внутрішнє право не надає відповідних гарантій. Це правило застосовується також до персональних даних, які стосуються злочинів. Для захисту персональних даних, що зберігаються у файлах даних для автоматизованої обробки, вживаються відповідні заходи захисту, спрямовані на запобігання випадковому чи несанкціонованому знищенню або випадковій втраті, а також на запобігання несанкціонованому доступу, зміні або поширенню.

Будь-якій особі згідно з Конвенцією має бути надана можливість: а) встановлювати існування автоматизованих файлів персональних даних, його головні цілі, а також особистість та місце постійного розташування чи місце діяльності контролера файлу;

в) отримувати через розумні проміжки часу та без надмірної затримки або витрат підтвердження або спростування зберігання персональних даних, що її стосуються, в автоматизованому файлі даних, а також отримувати такі дані у зрозумілій формі;

с) вимагати у відповідних випадках виправлення або знищення таких даних, якщо вони оброблялися з порушенням положень внутрішнього права, що запроваджують основоположні принципи, визначені у статтях 5 і 6 цієї Конвенції;

д) використовувати засоби правового захисту в разі незадоволення, передбаченого у пунктах в і с цієї статті запиту про підтвердження або у відповідних випадках про надання, виправлення або знищення даних.

Конвенція містить положення щодо **транскордонних потоків** персональних даних та внутрішнє право. Відповідно до цих положень сторона не може лише з метою захисту приватності забороняти або зумовлювати спеціальними дозволами транскордонні потоки персональних даних, що передаються на територію іншої Сторони. Однак кожна Сторона має право відступати від цих положень:

а) якщо її законодавство містить спеціальні положення для деяких категорій персональних даних або автоматизованих файлів персональних даних, у зв'язку з характером цих даних або цих файлів, за винятком випадків, коли положення іншої Сторони забезпечують еквівалентний захист;

в) якщо передача даних здійснюється з її території на територію держави, що не є Договірною, через територію іншої Сторони, для запобігання порушенню такою передачею законодавства Сторони.

Сторони погоджуються надавати одна одній взаємну допомогу з метою імплементації цієї Конвенції. Для цього:

а) кожна Сторона призначає один або більше органів, назву та адресу яких вона повідомляє Генеральному секретареві Ради Європи;

в) кожна Сторона, яка призначила більше одного органу, зазначає у своєму повідомленні сферу повноважень кожного з них.

Орган, призначений Стороною, на запит органу, призначеного іншою Стороною:

а) надає інформацію про свої законодавство та адміністративну практику в галузі захисту даних;

в) відповідно до свого внутрішнього права та з метою виключно захисту приватності вживає всіх відповідних заходів для надання достовірної інформації, що стосується конкретної автоматизованої обробки, яка здійснюється на його території, за винятком, однак, персональних даних, що обробляються.

Кожна Сторона надає допомогу будь-якій особі, що мешкає за кордоном, у здійсненні прав, наданих її внутрішнім законодавством.

Якщо така особа мешкає на території іншої Сторони, їй надається можливість подати свій запит через орган, призначений цією Стороною. **Запит** про надання допомоги має містити всі необхідні відомості, що стосуються, зокрема:

а) прізвища, адреси та будь-яких інших відповідних відомостей, які ідентифікують особу, що звертається із запитом;

б) автоматизованого файлу персональних даних, якого стосується запит, або його контролера;

с) цілі запиту.

Орган, призначений Стороною, який отримав від органу, призначеного іншою Стороною, інформацію, що супроводжує запит про надання допомоги, або у відповідь на його власний запит про надання допомоги, використовує цю інформацію тільки для цілей, зазначених у запиті про надання допомоги. 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. Призначеному органі на свій власний розсуд і без явно вираженої згоди суб'єкта даних, що проживає за кордоном, у жодному випадку не дозволяється звертатися із запитом про надання допомоги від імені зацікавленої особи. Призначений орган, якому адресується запит про надання допомоги, може відмовитися задовольняти такий запит, якщо:

а) запит є несумісним із повноваженнями, якими наділені в галузі захисту даних органи, що відповідають за виконання прохання;

б) запит не відповідає положенням цієї Конвенції;

с) задоволення запиту може порушити суверенітет, безпеку або громадський порядок Сторони, якою він був призначений, або права та основні свободи осіб, що перебувають під юрисдикцією цієї Сторони.

Положення вказаної Конвенції Ради Європи були доповнені і розвинуті в **Директиві Європейського Союзу 95/46/СЕ** «Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних» (м. Люксембург, 24.10.95 р.), яка має обов'язковий характер для країн-членів ЄС.

Найбільш важливими рекомендаціями директиви 95/46/ЕС є такі³⁹: — обробка персональних даних повинна здійснюватися лише за згодою зацікавленої фізичної особи.

— фізична особа повинна бути повідомлена про факти обробки її персональних даних під час їх реєстрації, крім випадків, передбачених законодавством;

³⁹ Брижко В. До питання щодо міжнародних стандартів захисту даних // Правова інформатика — 2004. — № 2. — С. 48—49.

— фізична особа має право знати про передачу її персональних даних третім особам, а також — точну та повну інформацію про обставини такої передачі;

— право доступу до персональних даних не повинне завдавати шкоди комерційній таємниці та правам інтелектуальної власності;

— щодо доступу та окремих повноважень з обробки персональних даних держава-член має право встановити винятки з правил, які зазначені у Директиві 95/46/ЄС, виходячи з інтересів національної безпеки, оборони, охорони порядку, найважливіших економічних чи фінансових інтересів, проведення досліджень, встановлення нових юридичних процедур та переслідування порушень професійних норм поведінки;

— захист персональних даних передбачає використання технічних та організаційних заходів з моменту створення системи обробки;

— відповідальною за обробку персональних даних та їх передачу в електронній формі є особа, яка надає послуги зв'язку, несе відповідальність за додаткову та необхідну для функціонування засобів зв'язку обробку персональних даних;

— національне законодавство повинне передбачати відповідальність суб'єктів відносин, пов'язаних з обробкою персональних даних, за невиконання вимог щодо захисту персональних даних згідно з чинними нормами як приватного, так і публічного права;

— держави-члени зобов'язані вживати заходи для повного виконання рекомендацій Директиви 95/46/ЄС. Національне законодавство не повинне містити правові норми, які б сприяли зниженню рівня захисту, а навпаки, повинне мати за мету забезпечення підвищення рівня захисту персональних даних.

Забороняється здійснювати обробку персональних даних:

— якщо обробка персональних даних не відповідає цілям, для яких збиралися дані, насамперед цілям, пов'язаним з виборами, коли відсутні правові норми, що встановлюють гарантії їх захисту;

— коли персональні дані можуть заповдіяти шкоду правам людини та основним свободам, приватному життю інших осіб;

— коли персональні дані пов'язані виключно з особистими інтересами та справами домашнього господарства (особисте листування, ведення списків та ін.)

Варто також згадати, що згідно з умовами статті 15 Статуту Ради Європи, 9 вересня 1991 року на 461-му засіданні засупників міністрів була прийнята **Рекомендація № (91) 10** щодо передачі третім сторонам даних особистого характеру, якими володіють державні органи. Принципи, які містяться у рекомендації, охоплюють всі дані особистого характеру, які збираються державними органами та які можуть бути передані третім сторонам. Принципи також покликані забезпечити

повноту до приватного життя суб'єкта даних, коли його дані передаються третім сторонам.

Принцип 1.1 підкреслює, що Рекомендація насамперед стосується даних особистого характеру, які автоматично обробляються державними органами.

Принцип 1.2 дозволяє державам-членам поширювати принципи Рекомендації на дані особистого характеру, якими володіють державні органи та які зберігаються у формі неавтоматизованого архіву. Ця гнучкість є важливою, оскільки категорії даних, якими володіють державні органи та які зберігаються у формі неавтоматизованого архіву, різні.

Принцип 1.3 присвячений визначенню низки важливих термінів, які часто використовуються у Рекомендації, а саме такі, як «дані особистого характеру», «державні органи», «файли доступні для третіх осіб», «передача», «третя сторона».

Принцип 2 Рекомендації передбачає потребу в застережних заходах та гарантіях, якими має супроводжуватися передача даних особистого характеру або файлів даних особистого характеру третім особам.

Принцип 2.1 підкреслює необхідність здійснювати передачу даних, що ґрунтуються на існуванні правової бази, яка дозволяє її здійснення. Однак, передача даних особистого характеру або файлів даних третім особам повинна здійснюватися за умови, якщо:

- 1) це передбачено конкретним законом; або
- 2) громадськість має до них доступ відповідно до правових норм, які регулюють доступ до інформації державного сектору; або
- 3) передача проводиться відповідно до внутрішньодержавного права стосовно захисту даних; або

4) суб'єкт даних висловив добровільну згоду, що ґрунтується на отриманій інформації.

Принцип 2.2 підкреслює важливість подальшої поваги до принципу визначення або остаточного призначення цілі після передачі. З цією метою передбачається, що дані особистого характеру або файли даних особистого характеру не можуть бути передані третім особам для цілей, несумісних з тими, для яких збиралися дані, якщо тільки не існує відповідних застережних заходів та гарантій у відповідному національному законодавстві.

Принцип 2.3 містить положення про те, що обробка даних третьою стороною після їх передачі повинна підпадати під вимоги національного законодавства із захисту даних, включаючи процедурний контроль, що здійснюється органами влади із захисту даних.

Принцип 3 стосується даних особистого характеру, які загалом не є доступними для третіх сторін через їхню секретність або через можливість завдання шкоди особистому життю суб'єктів даних, якщо вони передаватимуться третім сторонам.

Принцип 4 стосується даних особистого характеру, які є загально-доступними згідно з правовими нормами.

Принцип 5 висуває ряд застережних заходів та гарантій стосовно даних особистого характеру, які автоматично оброблюються та які містяться у файлах, доступних для третіх сторін. Перш за все пропеси обробки, які здійснюються державними органами, підпадають під дію положень національного законодавства. Окрім цього, повинні існувати прийняті технічні заходи для того, щоб запобігти масовому пересиланню файлів даних особистого характеру у порушення постулатів, які регулюють збереження та передачу електронних файлів.

Принципи 6.1 та 6.2 надають суб'єктові даних компенсаційні гарантії для того, щоб регулювати подальшу обробку його даних третіми сторонами.

Принцип 6.3 підкреслює права суб'єкта даних щодо захисту його даних, які оброблюються третіми сторонами та які були отримані з файлів, доступних для третіх сторін. Ці права включають право доступу, внесення змін та вилучення даних у випадку, якщо обробка була проведена всупереч принципам захисту даних.

Принцип 7 стосується об'єднання і зіставлення файлів.

У **принципі 8** йдеться про транскордонний потік даних, а саме аналіз ряду ситуацій, у яких може здійснюватись транскордонна передача:

— передача може здійснюватися на територію держави, яка ратифікувала Конвенцію про захист даних;

— передача може здійснюватися на територію держави, яка хоч і не є Договірною стороною, але має правові норми, які відповідають Конвенції та цій Рекомендації;

— передача може здійснюватися на територію держави, яка не має правових норм, які відповідають Конвенції або Рекомендації.

Взагалі, дослідження правового регулювання персональних даних за кордоном та на міжнародному рівні приділяється значно більше уваги порівняно з дослідженням цього питання в Україні. Це стосується не лише відсутності в Україні спеціальної законодавчої бази, а й відсутності наукових розробок та досліджень громадського сектора у цій сфері. Одні з перших ґрунтовні дослідження проблематики захисту персональних даних знаходять своє відображення у працях к. ю. н., керівника інтернет-проекту «Права людини та Інтернет» А. Пазюка. Зокрема, він присвячує увагу проблемам захисту права громадян на приватність персональних даних, у тому числі у зв'язку з діяльністю правоохоронних органів тощо⁶⁰.

⁶⁰ Див., напр.: Пазюк А.В. Захист прав громадян у зв'язку з обробкою персональних даних у правоохоронній діяльності: європейські стандарти і Україна. — К.: МГО Прайвесі Юкрейн, 2001. — 258 с.

Пазюк А.В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти. — К.: МГО Прайвесі Юкрейн, 2000. — 88 с.

Варто наголосити на тому, що сучасний стан нормативно-правової бази України не забезпечує захист прав людини щодо виконання положень статей 3, 32, 34 **Конституції України** стосовно персональних даних. Наявність у законодавстві в частині інформаційних правовідносин нечітко визначених, колізійних положень і прогалин, негативно впливає на забезпечення конституційних прав і свобод людини і громадянина. Закон України «Про інформацію» закріплює лише загальні принципи доступу громадян до інформації, що стосується їх особистого. Механізм реалізації зазначеного права належним чином не визначений.

Зокрема стаття 23 Закону України «Про інформацію» зазначає, що «інформація про особу — це сукупність документованих або публічно оголошених відомостей про особу». Основними даними про особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження. Джерелами документованої інформації про особу, відповідно до Закону, є видані на її ім'я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень. Також зазначається, що забороняється збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених законом. Міститься норма і про те, що «кожна особа має право на ознайомлення з інформацією, збіраною про неї».

Стаття 31 Закону України «Про інформацію» присвячена доступу громадян до інформації про них. Але варто зазначити, що положень Конституції і кількох статей в Законі «Про інформацію» не достатньо для того, щоб в Україні належним чином регулювалося питання щодо інформації персонального характеру.

Україна зобов'язана привести своє законодавство у відповідність з міжнародними стандартами, які відображають зміст прав і свобод людини стосовно поводження з інформацією персонального характеру. Постановою Верховної Ради України «Про засади державної політики України в галузі прав людини» від 17 червня 1999 року, зокрема, передбачає серед основних напрямів державної політики у галузі прав людини:

«...Створення належних умов, вироблення механізмів і процедур для повної і безперешкодної реалізації кожною особою своїх прав та законних інтересів;

Приведення законодавства України у відповідність з універсальними стандартами прав людини Організації Об'єднаних Націй та Ради Європи...»

Звідси випливає обов'язок України щодо гармонізації національного законодавства з міжнародними стандартами.

На сьогодні у парламенті є три законопроекти, які стосуються персональних даних, — це проект Закону «Про інформацію персонального характеру», проект Закону «Про захист персональних даних» (було прийнято за основу Постановою ВРУ від 15.05.2003 № 748-ІV), проект Закону «Про Єдиний реєстр персональних даних». Законопроекти покликані вирішити вищезазначені проблеми, а також:

- дати чітке і правильне визначення персональних даних;
- встановити порядок обробки персональних даних фізичних і юридичних осіб;
- визначити права і обов'язки осіб, яких стосується інформація персонального характеру, а також визначити підстави й умови легітимного і пропорційного обмеження цих прав для забезпечення прав інших осіб, потреб суспільства і держави;
- визначити статус, компетенцію і повноваження органу державної влади, уповноваженого реалізовувати державну політику в галузі обробки персональних даних, забезпечувати ефективну реалізацію прав людини стосовно обробки інформації персонального характеру;
- встановити режими доступу до інформації (персональних даних);
- викласти умови щодо внесення змін та доповнень до персональних даних;
- визначити види відповідальності та умови відшкодування матеріальної та моральної шкоди, порядок оскарження протиправних дій;
- врегулювати місце міжнародних принципів в законодавстві України, а також відносини України з іншими державами та підтримки громадян України, які проживають за кордоном.

Прийняття спеціалізованого закону щодо персональних даних потягне за собою необхідність **внесення змін** до законодавства, зокрема в Закони України «Про інформацію», «Про ліцензування певних видів господарської діяльності». Певних змін зазнають: Цивільний процесуальний кодекс України, Кримінальний кодекс України, Кодекс України про адміністративні правопорушення.

Проект Закону «Про інформацію персонального характеру» було зареєстровано у Верховній Раді України 12 листопада 2001 року. Законом було представлений народним депутатом України Олександром Задорожним. У законопроекті досить чітко виписано механізми захисту людини від основних видів дискримінації, що були визнані Радою Європи: за расовими і статевими ознаками, релігійними і політичними переконаннями (статті 7, 8, 9). Окрім цього, прописана процедура захисту і відновлення прав (стаття 22), обмежених, наприклад, в інтересах національної безпеки тощо.

Принципи обробки даних про притягнення суб'єкта до кримінальної чи адміністративної відповідальності (стаття 10) в європейських

країнах прописуються в окремих законах, а не в базовому законі про персональні дані.

Законопроект також містить механізм контролю за тими, хто займається діяльністю, пов'язаною з персональними даними, — через створення спеціального органу, уповноваженого контролювати таку діяльність. Орган повинен діяти з дозволу суду, і рішення про реузультати перевірок також приймають суди, що забезпечуватиме громадянам захист від свавілля влади. Однак механізм відповідальності цього органу за незаконне поширення отриманої інформації не завадило б прописати більш чітко. Містить законопроект і явно негативні положення. Так, передбачається ліцензування діяльності з обробки персональних даних (стаття 27). Але, по-перше, в більшості розвинутих країн сьогодні немає державного ліцензування подібної діяльності. По-друге, вимоги статті 27 можна трактувати досить широко, і при бажанні під ліцензію можна «підвести» навіть користувачів, які збирають в адресній книзі Outlook (чи іншій електронній поштовій системі) відомості про своїх знайомих.

Проект Закону України «Про захист персональних даних» у першу чергу намагається врегулювати питання захисту прав особи. Він ґрунтується на наданні людині права власності на її персональні дані.

Однак юридичній практиці досі відомі лише два інститути власності — матеріальної та інтелектуальної. Проектом фактично пропонується введення нового інституту власності. З одного боку, це справді дуже ефективний механізм захисту приватного життя людини від будь-якого втручання. З іншої — і українське, і міжнародне право поки недостатньо готові до цього. Наприклад, одразу виникає питання про захист персональних даних неповнолітніх — адже до 18 років громадяни України не можуть набувати право власності, окрім як через своїх законних представників (батьків, опікунів і піклувальників чи державний орган з опіки і піклування). Таким чином, якщо до прийняття такого закону не змінити чи доповнити значну частину українського законодавства, в Україні залишаться незахищені діти і — автоматично — їхні батьки, оскільки за даними дитини можна «вирахувати» багато даних про батьків.

Окрім цього, інститут права власності, що використовується вже кілька тисячоліть, належить до речей, обмежених у просторі, — приватності об'єктів за результатами матеріального виробництва. Право власності закріплює абсолютне право на речі. Цей правовий режим неможливо поширити на нематеріальні об'єкти, оскільки матеріальний об'єкт обмежений у просторі і його використання пов'язане з фактичним володінням. «Володіння» на нематеріальний об'єкт існувати не може, тому він може бути використаний одночасно необмеженим колом осіб. Розпорядження нематеріальним об'єктом може

сумішати з і збереженням права використання за першоволодільцем (особа, яка має виключне право на нематеріальний об'єкт, наприклад, інформацію; термін «власник» є недоречним, оскільки відноситься до інституту речового права власності) та наділенням правом використання кількох осіб⁶¹.

Захист осіб згідно з проектом застосовується як до автоматизованого, так і до ручного оброблення персональних даних.

Принципи захисту даних відображені в різних зобов'язаннях, накладених на різних суб'єктів (передусім це стосується якості даних, технічної безпеки, обставин, за яких можна здійснювати їх обробку) та в правах наданих особам, чії дані є об'єктом обробки, бути повідомленими про таку обробку, мати доступ до даних, бути в змозі вимагати їх виправлення або заперечувати обробці за певних обставин.

Позитивними у законопроекті є положення ст. 4 законопроекту, у якій йдеться про те, що персональні дані фізичної особи, яка претендує чи обіймає виборну посаду (у представницьких органах) або посаду державного службовця першої категорії не відносяться до інформації з обмеженим доступом. Однак, вважаємо, що слід виписати цю норму ширше і поширити її на публічних осіб, не даючи перелік посад.

Одночасно проект також містить ряд недоліків, наприклад:

— не містить заборони на об'єднання баз персональних даних, що обробляються з різними цілями;

— не окреслює процес знищення (утилізації) персональних даних.

На думку авторів **Проекту Закону України «Про реєстрацію фізичних осіб в Україні»**, існує необхідність регламентувати законодавчим шляхом діяльність, пов'язану з нагромадженням персональних даних і забезпеченням їхнього використання за призначенням в інтересах прав людини і національної безпеки держави. Проект, зокрема, ставить на меті поширення інформації персонального характеру, у тому числі конфіденційної інформації про особу, в інтересах національної безпеки, економічного добробуту та прав людини. Завданням законопроекту є створення правової бази регулювання відносин особи і держави за умов запровадження єдиної державної системи реєстрації, ідентифікації та обліку фізичних осіб, що проживають чи перебувають на території України, Єдиного державного реєстру інформації персонального характеру, забезпечення фізичних осіб документами Єдиного реєстру, які відповідають міжнародним вимогам.

Однак основні положення, які містяться у законопроекті, недовідають об'єднувати кожний пункт даних, які вносять у Єди-

ний реєстр, а саме мету і межі включення таких даних до реєстру. Дослідивши законопроект, можна дійти висновку, що внаслідок прийняття може бути суттєво порушено право особи на захист інформації персонального характеру.

Як зазначалося раніше, Закон України «Про інформацію» закріплює лише загальні принципи доступу громадян до інформації, що стосується їх особистості. Механізм реалізації зазначеного права належним чином не визначений. Тому виникає потреба в прийнятті закону, який би сприяв усуненню недоліків і прогалин в національному законодавчому регулюванні питань поводження з персональними даними, приведення його у відповідність до міжнародних, зокрема європейських, стандартів у цій галузі.

2.2. Процедура реалізації права на доступ до інформації

2.2.1. Активний доступ до інформації

Слід проводити чітке розмежування між інформаційним обслуговуванням населення і власне можливістю громадян вимагати від держави інформацію. Передбачається, що суть права на доступ до інформації проявляється не в тому, що органи влади активно надають громадськості будь-яку інформацію на свій розсуд, а власне у зворотному зв'язку у відносинах людини і держави. Однак централізоване постачання громадськості нормативною та іншою інформацією — це необхідний і природний елемент державного управління. І зацікавленою стороною тут уже буде не тільки громадянин, а й держава, оскільки результат, тобто ефективне управління, має значення для всього суспільства і держави, а не тільки для окремих індивідів.

Право на доступ до інформації, без сумніву, відкриває можливість безпосереднього ознайомлення з інформацією органів виконавчої влади (**активне право**).

До процедури активного доступу до інформації органів виконавчої влади можна віднести такі форми доступу:

- 1) направлення громадянами запиту до органів виконавчої влади про надання інформації;
- 2) відвідування відкритих робочих засідань органів влади;
- 3) доступ до відкритих архівів офіційної інформації органів виконавчої влади.

Найбільш повно в законодавстві України описано такий спосіб отримання інформації від державних органів, як **звернення з інформаційними запитами** про надання офіційної документованої інформації державних органів та інформації про діяльність органів законодавчої, виконавчої і судової влади, а також інформації, що стосується діяльності цих органів і їх посадових осіб.

⁶¹ Котляр Д. Правова природа та підходи до регулювання комерційної таємниці // ПАРЛАМЕНТ. — 2004. — № 3. — С.35.

Ч. 1 статті 302 Цивільного кодексу України (як і ч. 2 статті 34 Конституції України) *під правом громадян на інформацію розуміє право фізичної особи вільно збирати, зберігати, використовувати і поширювати інформацію.*

Статтею 40 Конституції України *гарантується право громадян на- правляти індивідуальні чи колективні письмові звернення або особисто звертатись до органів державної влади, органів місцевого самоврядування та посадових і службових осіб цих органів, що зобов'язані розглянути звернення і дати обґрунтовану відповідь у встановлений законом строк. Також Цивільним кодексом надається можливість суб'єкту відносин у сфері інформації вимагати усунення порушень його права та відшкодування майнової та моральної шкоди, завданої таким правопорушенням* (ч. 2 ст. 200 ЦК України).

Під *інформаційним запитом* щодо доступу до офіційних документів частинна 1 статті 32 Закону України «Про інформацію» розуміє письмове звернення з вимогою про надання можливості ознайомлення з офіційними документами. *Офіційними документами*, згідно з частиною 2 статті 21 Закону України «Про інформацію», є законодавчі акти України, інші акти, що приймаються Верховною Радою та її органами, акти Президента України, підзаконні нормативні акти, не- нормативні акти державних органів, акти органів місцевого самоврядування.

Під *запитом* щодо надання письмової або усної інформації частинна 3 статті 32 Закону розуміє звернення з вимогою надати письмову або усну інформацію про діяльність органів законодавчої, виконавчої та судової влади України, їх посадових осіб з окремих питань.

Як свідчить зарубіжна практика, серед базових питань у регулюванні порядку звернення громадян із запитами про надання інформації найбільш значимими є такі моменти.

По-перше, проблемним є питання *строків підготовки відповіді на запит* і порядок вирахування цих термінів. Частина 1 статті 33 Закону «Про інформацію» зазначає, що термін вивчення запиту на предмет можливості його задоволення не повинен перевищувати десяти календарних днів. Зазалом, у законопроектах і чинному законодавстві термін підготовки відповіді диференціюється від одного тижня до одного місяця. У зарубіжній практиці терміни підготовки відповіді наближаються до нижчої межі. У виняткових випадках, це пов'язується з значним обсягом інформації, що вимагається, то можна скористатися встановленим механізмом відстрочки в наданні інформації. Що стосується часу, з якого починається вирахування строків підготовки відповіді, то доцільно його пов'язувати з датою отримання запиту у відповідному органі влади, що еквівалентно даті реєстрації вхідної кореспонденції. У випадку, коли орган влади не володіє інфор-

мацією, що запитується, передбачається не відмова в наданні інформації, а перенаправлення запиту в орган влади, який зобов'язаний такою інформацією володіти. При цьому строк підготовки відповіді у зв'язку з некоректно складеним запитом не продовжується, а починає вираховуватися спочатку при отриманні запиту в іншому органі.

По-друге, важливим є питання про *підстави відмови* в наданні інформації за запитом. Вичерпний перелік підстав для відмови в задоволенні інформаційних запитів встановлено статтею 37 Закону України «Про інформацію». Так, не підлягають обов'язковому наданню для ознайомлення за інформаційними запитами офіційні документи, які містяться у собі:

- інформацію, визнану у встановленому порядку державною таємницею;
- конфіденційну інформацію;
- інформацію про оперативну і слідчу роботу органів прокуратури, МВС, СБУ, роботу органів дідзання та суду в тих випадках, коли її розголошення може зашкодити оперативним заходам, розслідуванню чи дідзанням, порушити право людини на справедливий та об'єктивний судовий розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи;
- інформацію, що стосується особистого життя громадян;
- документи, що становлять внутрішньовідому службову кореспонденцію (доповідні записки, листування між підрозділами та інше), якщо вони пов'язані з розробкою напряду діяльності установи, процесом прийняття рішень і передують їх прийняттю;
- інформацію, що не підлягає розголошенню згідно з іншими законодавчими або нормативними актами. Установа, до якої звернуто запит, може не надавати для ознайомлення документ, якщо він містить інформацію, яка не підлягає розголошенню на підставі нормативного акта іншої державної установи, а та держава установа, яка розглядає запит, не має права вирішувати питання щодо її розсекречення;
- інформацію фінансових установ, підготовлену для контрольно-фінансових відомств.

По-третє, умови *відшкодування* промаданями інформаційних послуг, що надаються органами виконавчої влади. Частини 9, 10 статті 35 Закону «Про інформацію» зазначають, що запитувачі мають право робити виписки з наданих їм для ознайомлення офіційних документів, фотографувати їх, записувати текст на магнітну плівку тощо. Власник документу має право за відповідну плату виготовляти за бажанням запитувача копії запитуваних документів. Не підлягає оплаті робота щодо пошуку офіційних документів.

Іноколи можна почути думки щодо доцільності закріплення в законодавстві про доступ визначений мінімум видів публічної інформації, яка надається безкоштовно. Цей мінімум може пов'яз-

зуватися з незначним обсягом потрібної інформації або ж з тим, що інформація вже публікувалась у загальнодоступних джерелах, або, якщо громадянин подає запит, пов'язаний з перевіркою своїх персональних даних, або з тим, що пересилка інформації громадянину з його дозволу здійснюється в електронній формі. Загальноприйнятим є те, що в інших випадках громадянин зобов'язаний оплачувати лише витрати щодо копіювання відповідної інформації. Однак у разі, якщо для задоволення запиту вимагається проведення аналітичної роботи, реферування і здійснення інших додаткових трудовітських робіт, можуть встановлюватися певні розцінки на підготовку відповідей на запит про інформацію. При цьому важливо слідкувати за тим, щоб органи виконавчої влади не намагались виконувати свої прямі посадові обов'язки щодо підготовки аналітичних звітів чи проведення іншої роботи, безпосередньо не пов'язаної із задоволенням запитів, за рахунок засобів громадян, що звертаються із запитом.

Однак у будь-якому разі кошти, які отримують публічні органи за надання доступу до інформації, не повинні бути такими, щоб стримувати потенційних заявників. Це обумовлено тим, що за законами про свободу інформації їхньою основною метою є сприяння відкритому доступу до інформації. Встановлено, що довготермінове надання режиму відкритості завжди виправдовує необхідні в таких випадках витрати.

Можна визначити певні гарантії для того, щоб платні послуги не перешкоджали вільному здійсненню інформаційних запитів. Можна використовувати подвійний механізм оплати, який складається з основної плати за кожний запит і диференційованої плати (залежної від вартості поновлення і зберігання інформації). Другий вид плати може бути або відмінений, або значно знижений у випадку запитів щодо одержання персональної інформації, а також запитів в інтересах громадськості (наприклад, якщо мета запиту є пов'язаною з публікацією). Інколи висока плата за комерційні запити фактично субсидує запити, що стосуються інтересів громадськості.

Але незважаючи на можливі переваги оплатності послуг щодо надання інформації, така постановка питання створює ситуацію, коли доступ до інформації стає обмежений для тих осіб, які не можуть собі це дозволити. Ця примітка також застосовується, коли інформація доступна лише завдяки новим технологіям, а більшість сімей все ще не має обладнання, необхідного для отримання інформації on-line⁶².

Цікавим є питання *форм, у якій запити поділяються*. За законодавством України це може бути письмова або усна форма. Однак у

законодавстві варто деталізувати цей перелік, а саме можна вказати, що запити на інформацію можуть бути адресовані органам виконавчої влади в такій формі:

- особистого усного звернення;
- звернення по довідковому телефону відповідного органу влади;
- письмового запиту, що надходить поштою чи шляхом особистої передачі;

— текстових повідомлень, що передаються каналами зв'язку (електронна пошта, факс).

Окрім цього, слід зазначити, що частіше за все відповідь на запит надсилається у формі, у якій був адресований запит, якщо сам запит не визначає форми відповіді.

Останнім часом набуло актуальності питання про забезпечення можливості звернення громадян до органів державної влади через інформаційні технології. Така можливість в іноземних країнах забезпечується поданням інформаційного запиту громадянами до органів державної влади, органів місцевого самоврядування через Інтернет. Щоб ця система ефективно діяла, необхідно створити таке програмне забезпечення, яке б дозволяло прослідкувати рух звернення з моменту його надходження до моменту його виконання; визначення типу (переліку) звернень, які падають чи не падають під такі, що потребують чи не потребують розгляду і виконання (є чи не є юридично значимі). До того ж необхідно внести зміни до Закону України «Про звернення громадян» у частині регламентації процедури звернення громадян через Інтернет (порядок подачі такого звернення, строки розгляду та ін.)

Наступна форма доступу до інформації органів виконавчої влади пов'язана з **можливістю відвідувати відкриті засідання цих органів**. Однак, за загальним правилом, відкритість засідання гарантується можливістю присутності на них саме зацікавлених осіб. Окрім цього, зважаючи на особливості природи утворення і діяльності органів виконавчої влади, присутність на відкритих засіданнях громадян повинна мати пасивний характер, оскільки не можна ототожнювати попити доступу до інформації з можливістю впливу громадськості на прийняття рішень органів виконавчої влади.

Щодо доступу до **відкритих архівів органів виконавчої влади** як ще однієї альтернативної форми забезпечення доступу громадян до публічної інформації, слід зазначити таке. Прийнято вважати, що цей напрямок реалізації доступу в цілому врегульовано в законодавстві про архіви і архівні фонди. Насправді, воно забезпечує можливість громадян ознайомлюватися з інформацією, що міститься в централізованих бібліотечних і архівних фондах. Однак законодавство про архіви і архівні фонди орієнтовано на збереженість і централізацію інформації, у той час як законодавство про доступ до інформації, як

⁶² Гончарж Я., Гнидюк Н. Свобода інформації та виконавча гілка влади... — С. 27.

правило, акцентує увагу на порядку і гарантіях доступності до інформації. Тому в законодавстві про право доступу до інформації вимагається хоча б пов'язати норми про доступ до інформації органів влади із законодавством про архіви й архівний фонд, однак у перспективі слід врегулювати й порядок доступу до фондів офіційної інформації, спеціально створюваних у бібліотеках і архівах⁶³.

З іншого боку, доступ до бібліотек і баз даних не є гарантією безпосереднього отримання інформації від органів влади. В інформаційному спілкуванні громадян з органами влади знову з'являється посередники. Це може сприяти тому, що дана форма надання інформації втратить свій потенціал бути гарантією гласності діяльності органів виконавчої влади. Для вирішення цього завдання слід передбачити можливість громадян отримати доступ до інформації, що міститься у відкритих архівах, які формують самі органи виконавчої влади⁶⁴.

2.2.2. Пасивне право на доступ до інформації

Інша загальна система гарантій доступу до інформації пов'язана з механізмом **пасивного доступу**. За способом забезпечення громадян інформацією можна виділити такі форми: поширення інформації в засобах масової інформації, випуск спеціалізованих брошур і збірників, розміщення інформації в Інтернеті, розміщення інформації на стендах офіційної інформації в приміщеннях, де розташовані органи виконавчої влади. Однак більш показовим є аналіз тих форм надання інформації, які виділяють за змістом інформації. Тому можна виділити такі форми опублікування офіційної інформації органів виконавчої влади:

- опублікування нормативно-правової інформації;
- опублікування регуляторних звітів про виконану роботу;
- поширення офіційної інформації, пов'язаної з поточними подіями (звернення, відповіді, виступи, коментарі та ін.).

Порядок всебічного й об'єктивного висвітлення діяльності органів державної влади та органів місцевого самоврядування засобами масової інформації і захисту їх від монопольного впливу органів тієї чи іншої гілки державної влади або органів місцевого самоврядування визначається Законом України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» від 23 вересня 1997 року. Під «висвітленням діяльності органів державної влади та органів місцевого

го самоврядування в Україні» даний Закон розуміє 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.

Порядок висвітлення діяльності Кабінету Міністрів України, центральних та місцевих органів виконавчої влади визначається статтею 11 зазначеного Закону. Відповідно до викладених у ній положень, у засобах масової інформації висвітлюються засідання Кабінету Міністрів України, на яких розглядаються питання, що належать до його конституційних повноважень; видані постанови і розпорядження, заяви Кабінету Міністрів України та Прем'єр-міністра України; наради з широкого кола соціально-економічних та регіональних питань; візити офіційних урядових делегацій України за кордон, їхня участь у міжнародних форумах, а також перебування в Україні офіційних іноземних урядових делегацій; проведення загальнодержавних і міжнародних заходів, організація яких покладається на Кабінет Міністрів України. Інформація про діяльність Кабінету Міністрів України, центральних і місцевих органів виконавчої влади здійснюється у формі офіційних повідомлень, репортажів, коментарів та інтерв'ю членів Кабінету Міністрів України і керівників центральних та місцевих органів виконавчої влади, прес-конференцій, брифінгів, «круглих столів», щотижневих інформаційних аналітичних передач.

Рішення про повну теле- і радіотрансляцію або розширений теле- і радіозвіт про засідання Кабінету Міністрів України чи проведення інших важливих державних заходів, організація яких покладається на Кабінет Міністрів України, приймає Прем'єр-міністр України не пізніше як за добу до часу теле- і радіотрансляції, за винятком окремих непередбачених надзвичайних ситуацій, коли теле- і радіотрансляція здійснюється негайно.

Діяльність місцевих органів виконавчої влади висвітлюється регіональними телерадіоорганізаціями. Місцеві органи виконавчої влади укладають відповідні угоди на висвітлення їхньої діяльності з регіональними телерадіоорганізаціями за рахунок місцевих бюджетів.

Серед характерних особливостей Закону про порядок висвітлення можна виокремити такі. По-перше, обов'язок висвітлювати діяльність органів влади державними ЗМІ не може тлумачитись як обмеження для висвітлення таких подій недержавними ЗМІ. По-друге, регулюється порядок поширення лише інформаційних програм про основні офіційні події. По-третє, у Законі встановлено порядок висвітлення діяльності лише вищих органів влади в державних ЗМІ, у той час як висвітлення діяльності міністерств і відомств відводиться на розсуд редакцій.

⁶³ Актуальні проблеми забезпечення доступу к інформації. — М.: Інститут проблем інформаційного права, 2004. — С. 235.

⁶⁴ Там само.

Опублікування офіційної інформації в аудіовізуальних і друкованих державних і недержавних ЗМІ не вичерпує можливостей пасивного доступу до інформації про діяльність органів виконавчої влади. З врахуванням значного розвитку інформаційних технологій важливий засіб інформаційної взаємодії громадян і органів влади — це передача і поширення інформації в інформаційних мережах загального користування. За допомогою публікації інформації в Інтернеті можлива реалізація всіх наведених вище напрямків забезпечення права на інформацію. Сучасні інтернет-технології дозволяють зробити спілкування влади і громадян значно різноманітнішим і ефективнішим (форуми, телеконференції, повідомлення електронною поштою, електронні архіви, запровадження пошуківих систем і т. д.). За кордоном значну політичну підтримку отримують ініціативи організації мережевої інформаційної взаємодії громадян і організації з органами влади (наприклад, у Болгарії існує програма «Доступ до інформації», у реалізації якої значну роль відіграють саме громадські організації). В Україні на сьогодні врахування світових тенденцій у сфері побудови «електронного урядування» виражається в найрізноманітніших формах: шляхом організації акцій інтерактивного спілкування посадових осіб і громадян, шляхом підписання міжнародних документів про розвиток інформаційного суспільства, через створення інформаційних сайтів органів влади в Інтернеті (наприклад, урядовий портал), за допомогою офіційного визнання електронного документообігу між органами влади і громадянами (організаціями), шляхом прийняття довготривалих програм розвитку галузі.

Отже, структура суб'єктивного права громадян на доступ до інформації поділяється на можливість пасивного і активного доступу. За способом активного доступу виділяють можливість отримання інформації на основі запиту, шляхом відвідування засідань органів влади і через ознайомлення з відкритими архівами органів виконавчої влади. За способом пасивного доступу виділяють можливість отримання громадянським інформації про органи влади шляхом публікування відомостей у державних і недержавних ЗМІ, у спеціалізованих брошурах і збірниках офіційної інформації, через забезпечення доступу громадян до офіційних сторінок органів влади в мережі Інтернет, електронним базам даних на компактних носіях інформації, загальним бібліотечним і архівним фондам, стендам офіційної інформації в місцях розташування органів влади і т. д. За змістом пасивного доступу до інформації виділяють надання нормативно-правових актів, офіційних звітів про діяльність органів влади, а також інформації про основні поточні події в діяльності органів виконавчої влади.

2.3. Оскарження і відповідальність за порушення права на доступ до інформації

Існування чіткої та дієвої адміністративної процедури оскарження рішень та дій публічної адміністрації є однією з найважливіших гарантій для громадян: у разі невідповідної поведінки державних органів.

Згідно зі статтею 47 Закону України «Про інформацію», порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність. Відповідальність за порушення законодавства про інформацію несуть особи, винні у вчиненні таких дій, як:

- 1) необґрунтована відмова від надання відповідної інформації;
- 2) надання інформації, що не відповідає дійсності;
- 3) несвоєчасне надання інформації;
- 4) навмисне приховування інформації;
- 5) примушення до поширення або перешкоджання поширенню певної інформації, а також цензура;
- 6) поширення відомостей, що не відповідають дійсності, ганьблять честь і гідність особи;

7) безпідставна відмова від поширення певної інформації;

8) використання і поширення інформації стосовно особистого життя громадянина без його згоди особою, яка є власником відповідної інформації внаслідок виконання своїх службових обов'язків;

9) розголошення державної або іншої таємниці, що охороняється законом, особою, яка повинна охороняти цю таємницю;

10) порушення порядку зберігання інформації;

11) навмисне знищення інформації;

12) необґрунтоване віднесення окремих видів інформації до категорії відомостей з обмеженим доступом.

Цікавим є питання правового регулювання відповідальності за розголошення державної таємниці в інших країнах. Австрія, Швеція та США забезпечують найвагомішу підтримку преси при публікації відомостей, що містять державну таємницю. В Австрії та Швеції журналісти й редактори підлягають судовому переслідуванню за розголошення державної таємниці, якщо воно могло завдати значної шкоди національній безпеці або міжнародній відносинам. Однак у Швеції журналісти не можуть бути примушені до розкриття джерела виходу журнальної інформації, якщо тільки розкриття не пов'язане з національною безпекою; у США представників преси не можна переслідувати судом за публікацію практично будь-якої секретної інформації; єдина категорія публікацій, що карається судом, — це розкриття імен агентів розвідувальних служб, якщо публікація такої інформації завдає шкоди діяльності таких

служб. (Однак інші категорії інформації можуть підлягати іншим обмеженням⁶⁵.)

У деяких країнах (Австралія, Німеччина і Норвегія) той факт, що розкриття слугує суспільному інтересу, забезпечує захист опублікування інформації, отриманої незаконним шляхом, а також забезпечує захист будь-якому державному службовцеві, через якого було отримано інформацію. У Німеччині не надається захист при опублікуванні матеріалу, який можна віднести до цілком таємного.

Навіть у тих країнах, де пресу не карають за розголошення секретної інформації, державний службовець, відповідальний за надання інформації, може бути звинувачений у порушенні конфіденційності, притягнений до кримінальної або цивільної відповідальності або звільнений з роботи (Австрія, Австралія, США). У деяких країнах відсутнє законодавство, що встановлює відповідальність за незбереження конфіденційної інформації та Канаді злочином вважається опублікування секретної інформації, що стосується оборони країни, а спеціальне виправдання на основі суспільного інтересу для преси або службовців, що надали таку інформацію, відсутнє.

У свою чергу, стаття 48 Закону «Про інформацію» присвячена порядку оскарження протиправних дій. Зокрема, зазначається, що в разі вчинення державними органами протиправних дій, передбачених Законом, ці дії підлягають **оскарженню до органів вищого рівня або до суду**. Скарги на протиправні дії посадових осіб подаються в орган вищого рівня, яким підпорядковані ці посадові особи. У разі незадоволення скарги, поданої до органу вищого рівня, зацікавлена особа має право оскаржити протиправні дії посадових осіб до суду.

У більшості країн відмова в отриманні інформації також є предметом адміністративного контролю вищого органу самої адміністрації (Німеччина, Нідерланди) або ж органу, спеціально створеного з метою задоволення таких скарг (Австралія, Канада, Франція, Швеція). Рішення цих органів можна оскаржити в суді. Наявність адміністративного контролю, що здійснюється спеціально створеним для цього органом, корисна тим, що може полегшити процес розгляду скарг, хоча адміністративна затримка лишається проблемою всіх країн⁶⁶.

У Франції спеціальна комісія (Комісія щодо доступу до адміністративних документів) розглядає скарги та суперечки з приводу доступу до інформації. Більшість проблем розв'язується на цьому рівні. Подавець заяви, не задоволений рішенням Комісії, може вимагати перегляду справи адміністративним судом. У Швеції омбудсмен, при-

значений парламентом, контролює розкриття матеріалів і розв'язує суперечки. В Австралії допускаються безпосередні звернення до омбудсмена або до адміністративного апеляційного трибуналу; Канада допускає звернення лише до спеціального уповноваженого. Однак лише австралійський трибунал може прийняти рішення про розголошення матеріалів; омбудсмен та спеціальний уповноважений можуть лише давати відповідні рекомендації. У США апеляція може бути подана голові закладу, який відмовився надати інформацію.

Законодавство низки країн вимагає, щоб причини будь-якої відмови подавалися в письмовій формі і щоб подавач заяви був поінформований про право на апеляцію (Австралія, Норвегія, Швеція). У Швеції часто є обов'язковим подавати відмову та її причини в письмовому вигляді.

Звертаючись до забезпечення права на інформацію в європейських країнах, варто зазначити, що там використовують **кілька зразків (моделей)** при реалізації відповідних положень:

(1) Закон про свободу інформації трактується як нормативний акт, що має силу конституції. Це означає, що не існує окремого органу, який виконує положення цього Закону та не існує окремих структур у системі виконавчої влади, які відповідають виключно за питання доступу до публічної інформації. Зазвичай нагляд за реалізацією закону здійснюють парламенти, а в разі захисту інтересів громадян — омбудсмени та суди. Такий підхід, наприклад, характерний для Швеції, Данії, Бельгії, Фінляндії, Австрії, Німеччини та Нідерландів.

(2) У деяких країнах реалізація положень закону про свободу інформації супроводжувалася створенням окремих органів, які відповідали за підготовку підзаконних актів та за координацію процесу впровадження відповідних програм у системі державного управління. Подібні органи функціонували від двох до п'яти років та були ліквідовані після виконання покладених на них функцій і завдань. Такий процес відбувався в Бельгії, Фінляндії та Чеській Республіці. Підготовчий етап запровадження відповідних механізмів у сфері доступу до інформації було віднесено до сфери повноважень міністра юстиції (Данія та Угорщина), або до компетенції міністра фінансів.

(3) Кілька країн застосовували іншу стратегію для здійснення упорядкованих питань доступу до інформації — вони прийняли рішення про створення окремих органів виконавчої влади, які будуть відповідати за весь спектр питань, пов'язаних з інформацією. Наприклад, у Великій Британії та Ірландії існує Офіс уповноваженого з питань інформації, а у Франції і Португалії було створено спеціальну Комісію з питань доступу до адміністративних документів⁶⁷.

⁶⁵ Закони та практика ЗМІ у одиницях демократії світу (порівняльний аналіз) / ARTICLE 19, Харківська правозахисна група. — Харків: Фоліо, 2000. — 200 с.

⁶⁶ Там само.

⁶⁷ Гоншяк Я., Гнидок Н. Свобода інформації та виконавча гілка влади... — С. 95.

Загальноприйнятою практикою для більшості європейських країн є розмежування інформаційних служб в організаційній структурі кожного державного органу. Основне завдання цих служб — сприяти потоку інформації між відповідним державним органом, засобами масової інформації та пересічними громадянами.

Інформаційні служби в сучасних урядах європейських країн відіграють за надання громадянам комплексної та достовірної інформації щодо всіх аспектів діяльності уряду на всіх можливих типах інформаційних носіїв. Комплексний характер цієї діяльності призводить до того, що зазвичай інформаційні послуги діляться на дві частини: послуги, які надаються через урядовий інформаційний центр та інформаційні служби в міністерствах. В основному структурні підрозділи виконують п'ять груп завдань:

- консультативні послуги для службовців, які обіймають посади спеціалістів департаментів;
- організації комунікації зі ЗМІ;
- надання інформації громадянам;
- дослідження та аналітична робота;
- координація інформаційної політики та покращення інформаційних потоків усередині урядових органів.

Отже, правові основи доступу до публічної інформації є лише частиною більш комплексної проблеми. На практиці способів функціонування державних органів та стилів роботи їх структурних підрозділів є чинниками, які в дійсності визначають, яка інформація, у якому форматі та за яких умов доступна для громадян. Тому надзвичайно важливе значення для практичного впровадження свободи інформації має організація та спосіб функціонування інституцій, відповідальних за дотримання права на доступ громадянської до інформації.

ЗАМІСТЬ ВИСНОВКІВ. ПЕРСПЕКТИВИ РОЗВИТКУ ЗАКОНОДАВСТВА УКРАЇНИ ПРО ДОСТУП ДО ІНФОРМАЦІЇ

Підбиваючи підсумки, слід зазначити, що право на доступ до інформації є одним із невід'ємних прав людини і громадянина, яке повинне забезпечуватися, насамперед, наявністю ефективних правових механізмів його здійснення. Потрібно також пам'ятати, що функціонування інформаційного суспільства можливе лише за умов існування демократичної, правової держави, де панує принцип верховенства права і максимально забезпечується реалізація прав людини.

Дослідивши проблематику доступу до публічної інформації, захисту персональних даних, а саме проблему правового регулювання цих питань, хотілося б виділити такі основні аспекти.

1. Право на доступ до інформації є конституційним правом людини, передбачене і гарантоване статтею 34 Конституцією України, яка, у свою чергу, ґрунтується на положеннях Європейської конвенції про захист прав та основних свобод людини (стаття 10), Міжнародного пакту про громадянські і політичні права (статті 18, 19) тощо. Для забезпечення доступу до інформації у Рекомендаціях Парламентської Асамблеї Ради Європи Раді Міністрів (81)19, схвалених у 1987 році, були визначені основні принципи щодо доступу до інформації, яка перебуває в розпорядженні органів державної влади⁶⁸. До цих принципів відносяться такі:

- Усі громадяни мають право складати запит на інформацію, яка перебуває в розпорядженні органів публічної влади.
- Заборонено відмовляти в запиті на інформацію лише тому, що інформація, на яку складається запит, не стосується особистих інтересів зацікавленої сторони.
- Кожен запит на інформацію повинен бути розглянутий у визначений термін, а в разі відмови у наданні документів, повинні бути чітко пояснені (обґрунтовані) причини відмови.
- Доступ до інформації може бути обмежений у випадках, визначених законом, і тих, які стосуються інтересів національної безпеки, громадського порядку, розслідування кримінальних злочинів або які можуть порушити право на приватність.

2. Основна суть права на доступ до інформації полягає у можливості кожного вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб і на свій вибір.

⁶⁸ Recueil des résolutions et recommandations du Comité des Ministres du Conseil de l'Europe relatives au droit administratif avec leurs rapports explicatifs. Document préparé par la Direction des Affaires Juridiques CJ-DA (94) Info 1, Strasbourg, 1994.

Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

3. Дане право повинне гарантуватися державою, що включає в себе, зокрема, визначення на законодавчому рівні інформації, доступ до якої обмежується, і мету обмеження. При цьому перелік відомостей, доступ до яких обмежено, має бути вичерпно визначений і оприлюднений. Відкритою має бути інформація про повноваження, структуру, організацію діяльності органів державної влади та адміністративні послуги, які вони надають, їхнє майно, матеріально-технічне забезпечення, фінансування, кількість працівників, розмір оплати їхньої праці, особливості їхнього соціально-побутового та медичного забезпечення. У даному випадку необхідно також дотримуватися двох принципів. Перший — принцип максимального оприлюднення: вся інформація, якою володіють державні органи влади, підлягає оприлюдненню; кількість винятків повинна бути обмежена. Другий принцип характеризує вимоги щодо обмежень: а) винятки повинні бути зрозумілими; б) описуватися вузько; в) підлягати контролю на предмет наявності «шкоди» і впливу на «суспільні інтереси».

4. Правові та інші механізми доступу до інформації не повинні порушувати право на захист персональних даних. Як зазначалося раніше, Закон України «Про інформацію» закріплює лише загальні принципи доступу громадян до інформації, що стосується їх особи. Механізм реалізації зазначеного права належним чином не визначений. Тому виникає потреба в прийнятті закону, який би сприяв усуненню недоліків і прогалин в національному законодавчому регулюванні питань пов'язаних з персональними даними, приведення його у відповідність до міжнародних, зокрема європейських, стандартів у цій галузі.

5. Право на доступ до інформації та захист персональних даних повинні забезпечуватися насамперед наявністю відповідних правових та інших механізмів його забезпечення.

Отже, до основних проблем, які пов'язані з доступом громадян до інформації і, відповідно, стоять на перешкоді забезпечення прозорості діяльності публічної адміністрації, належать:

- наявність та широке неправомірне застосування грифів обмеження доступу до інформації;

- хаотичний розвиток інформаційного законодавства, який полягає в ігноруванні великої кількості нормативно-правових актів про інформацію різних рівнів, що суперечать одне одному;

- невпорядкованість термінології інформаційного законодавства, що нерідко призводить до різного застосування правових норм на практиці;

- неналежне виконання вимоги органами влади оприлюднювати інформацію про свою діяльність;

- відсутність реальних механізмів забезпечення відповідальності за порушення інформаційного законодавства.

Ці проблеми значно ускладнюють участь громадян у політичному житті держави.

Таким чином, існує цілком достатньо підстав для суттєвого оновлення законодавства України про інформацію. Виникає потреба в розробці концепції розвитку інформаційного законодавства, як окремої галузі, що об'єднує у собі окремі правові інститути. Так, розвиток інформаційного законодавства має відбуватися шляхом вирішення двох послідовних завдань:

- прийняття базового закону «Про інформацію» у новій редакції та спеціальних законів у галузі інформаційного права;

- систематизація інформаційного законодавства шляхом кодифікації, тобто прийняття Інформаційного кодексу, який об'єднав би окремі правові інститути галузі.

В умовах євроінтеграції, враховуючи зарубіжний досвід і положення Рекомендації Ради Європи № R(2002)2 про доступ до офіційних документів, можна виокремити певні ідеї, які слід запровадити в Україні з метою забезпечення права громадян на доступ до інформації.

По-перше, це максимальна відкритість і політична воля з боку органів виконавчої влади. Це означає, що будь-яка інформація, якою володіє орган влади, має бути відкрита і доступна, за винятком чітко визначеного переліку відомостей, доступ до яких обмежується на основі закону, а з боку органів виконавчої влади повинна виходити ініціатива щодо підтримання відкритості своєї інформації. Окрім цього, сюди входить обов'язок опублікування основної інформації про діяльність органів виконавчої влади.

По-друге, це правомірне обмеження доступу до інформації. При цьому перелік відомостей, які входять до кола обмежень, має бути вичерпно визначений і оприлюднений. А саме: рішення державного органу обмежити доступ до інформації є виправданим, якщо, по-перше, інформація має відношення до легітимної мети, передбаченої законом; по-друге, її оприлюднення має дійсно загрожувати спричиненням шкоди легітимній меті; по-третє, школа, яка може бути заподіяна вказаній меті, повинна бути вагомішою, ніж суспільний інтерес в отриманні інформації.

По-третє, має бути чітко визначена процедура отримання інформації, відповідальність за її надання. Ідеться про те, що всі формальності при отриманні громадянином доступу до інформації повинні бути обґрунтовані і вказані в законі, а відмова в наданні може бути фактично оскаржена. Окрім цього, на законодавчому рівні необхідно встановити санкції щодо винних посадових осіб, які перешкоджають законному отриманню громадянином інформації.

5. Структура суб'єктивного права громадян на доступ до інформації поділяється на можливість пасивного і активного доступу. За способом активного доступу виокремлюють можливість отримання інформації на основі запиту, шляхом відвідування засідань органів влади і через ознайомлення з відкритими архівами органів виконавчої влади. За способом пасивного доступу виділяють можливість отримання громадянином інформації про органи влади шляхом публікування відомостей в державних і недержавних ЗМІ, у спеціалізованих брошурах і збірниках офіційної інформації, через забезпечення доступу громадян до офіційних сторінок органів влади в мережі Інтернет, електронних баз даних на компактних носіях інформації, загальних бібліотечних і архівних фондів, стендів офіційної інформації в місцях розташування органів влади і т. д. За змістом пасивного доступу до інформації виділяють надання нормативно-правових актів, офіційних звітів про діяльність органів влади, а також інформації про основні поточні події в діяльності органів виконавчої влади.

6. Існування чіткої та дієвої адміністративної процедури проти адміністративних рішень та дій публічної адміністрації є однією з найважливіших гарантій для громадян: у разі невідповідної або сумнівної поведінки державних органів, їхні права та інтереси не будуть зневажати або порушувати, якщо немає реальних підстав у вищого рівня, які це обґрунтовують.

Правові основи доступу до публічної інформації є лише частиною більш комплексної проблеми. На практиці спосіб функціонування державних органів та стиль роботи їх структурних підрозділів є чинниками, які в дійсності визначають, яка інформація, у якому форматі та за яких умов доступна для громадян. Тому надзвичайно важливе значення для практичного впровадження свободи інформації має організація та спосіб функціонування інституцій відповідальних за отримання права на доступ громадської до інформації.

Вирішивши проблему нефективного законодавства, передбачивши механізми його реалізації, можна буде забезпечити реальне здійснення передбаченого Конституцією України права людини на доступ до інформації, що є необхідною умовою забезпечення прозорості діяльності публічної адміністрації, оскільки для України настав час, коли цим питанням буде надано комплексного та дієвого характеру.

КОНЦЕПЦІЯ ЗАКОНУ УКРАЇНИ «ПРО ДОСТУП ДО ІНФОРМАЦІЇ»⁷⁰

Проект⁶⁹

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. На сьогодні багато труднощів у сфері доступу громадян до інформації, якою володіють органи державної влади та органи місцевого самоврядування. Свідченням цього є скарги громадян на відмову в задоволенні запитів на інформацію до органів вищого рівня чи суду.

1.1.1. Органи державної влади та органи місцевого самоврядування фактично безпідставно відмовляють у наданні інформації, відносячи її до інформації з обмеженим доступом, неправомірно застосовуючи при цьому грифи обмеження доступу до інформації, такі як: «опублікуванню не підлягає», «не для друку», «для службового користування»;

1.1.2. Органи державної влади та органи місцевого самоврядування не повністю виконують вимогу оприлюднювати інформацію про свою діяльність;

1.1.3. Існують великі труднощі в отриманні громадянами локальних нормативно-правових актів (а в деяких випадках це взагалі неможливо) місцевих органів виконавчої влади та органів місцевого самоврядування, не кажучи вже про проекти таких актів.

1.1.4. Не врегульована також проблема доступу громадян до інформації про себе (інформації персонального характеру).

1.1.5. Не всі внутрішньовідомчі акти публікуються в офіційних виданнях (стаття 37 Закону України «Про інформацію» містить загальні положення про інформацію, яка не підлягає розголошенню згідно з іншими законодавчими актами), і, таким чином, державні органи стають подібними до власників інформації, які на власний розсуд приймають рішення про надання або відмову в наданні інформації.

1.1.6. Відсутність чітких процедур та інституцій, спеціально призначених для захисту права на доступ до інформації. Відсутність інструкцій чи форм для складання запитів на інформацію.

1.1.7. Невизначення механізму надання документів, які зберігаються органами влади;

1.1.8. Наявність у правовому регулюванні надто великої кількості оціночних понять, дискреційних меж щодо визначення режиму відкритості/закритості інформації тощо.

⁶⁹ Проект Центру політико-правових реформ.

⁷⁰ Можливо, більш вдалою була б назва: «Концепція Закону України «Про свободу інформації»».

Ці та інші проблеми пов'язані, в першу чергу, з відсутністю якісних правових механізмів здійснення права людини на свободу інформації, оскільки чинне законодавство України про свободу інформації не відповідає сучасному рівню розвитку інформаційних відносин та не в змозі адекватно вирішувати проблеми, що виникають. Більшість чинних законів та підзаконних нормативно-правових актів, спрямованих на регулювання інформаційних відносин, були прийняті до набрання чинності Конституцією, і навіть зі значними змінами і доповненнями непридатні для задоволення потреб сьогодення. Найбільш істотними є недоліки базових, власне інформаційних законів («Про інформацію», «Про державну таємницю» та ін.), які практично не мають власного змісту (норм, придатних до практичного застосування), тобто або відсилають до інших нормативно-правових актів (які також містять посилання, що не можуть бути застосовані до інформаційних відносин), або містять норми-декларації. Існує також багато проблем, пов'язаних з використанням термінології інформаційного законодавства.

Це все пояснює необхідність вдосконалення законодавства України про свободу інформації, а саме — прийняття нового Закону про свободу інформації (доступ до інформації).

Свобода інформації — передбачене Конституцією України право, що включає в себе право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб — на свій вибір. Здійснення цього права може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або промислового порядку.

Будь-яка особа, яка складає запит на інформацію до органу державної влади, органу місцевого самоврядування має право:

- бути повідомленою, чи зберігає орган державної влади або орган місцевого самоврядування відомості, які містять відповідну інформацію, або відомості, з яких така інформація може бути отримана;
 - у разі наявності в органі державної влади, органі місцевого самоврядування такої інформації, отримати її.
- Кожній особі забезпечується вільний доступ до інформації, яка стосується її особисто, крім випадків, передбачених законами України.

1.2. У Законі про свободу інформації (доступ до інформації) слід використовувати такі терміни:

Інформація — відомості про об'єкти, події, явища та процеси незалежно від форм їх вираження.

Розпорядники інформації — суб'єкти відносин у сфері доступу до інформації, що визначені у п.п.2 п. 4.1.

Режим доступу до інформації — передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації.

Відкрита інформація — будь-яка інформація, що не віднесена законом до категорії інформації з обмеженим доступом.

Інформація з обмеженим доступом — це інформація, яка призначена для обмеженої групи людей і стосується виконання ними роботи або посадових обов'язків, та розкриття або втрата якої, згідно з характером та змістом такої інформації, перешкоджає або може перешкодити діяльності органу, або спричиняє чи може спричинити шкоду законним інтересам фізичних або юридичних осіб.

Конфіденційна інформація — інформація, яка перебуває у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб приватного права і поширюється за їхнім бажанням відповідно до передбачених ними умов.

Таємна інформація — інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Комерційна таємниця — склад і обсяг відомостей, що визначені керівником підприємства відповідно до ч.1 ст. 30 Закону України «Про підприємства в Україні» та постанови Кабінету Міністрів України від 09.08.93 № 611 «Про перелік відомостей, що не становлять комерційної таємниці».

Комерційна таємниця підприємства — відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) яких може завдати шкоди його інтересам.

Службова таємниця — склад і обсяг відомостей, що є в розпорядженні конкретного органу державної контролюльно-ревізійної служби або її посадової особи стосовно об'єктів контролю, контрольних, правоохоронних та інших державних органів, їх працівників, способів досягнення визначених законодавством завдань, що необхідні для якісного проведення контролюльно-ревізійних дій, забезпечення відповідної їх раптовості та ефективності і які з цієї причини на певний період не підлягають зовнішньому чи внутрішньому розголошенню.

Професійна таємниця — матеріали, документи, інші відомості, якими користуються в процесі та у зв'язку з виконанням своїх посадових обов'язків посадові особи державних органів, що здійснюють регулювання ринків фінансових послуг, та особи, які залучаються до здійснення цих функцій, і які забороняється розголошувати у будь-якій формі до моменту прийняття рішення відповідним уповноваженим державним органом.

Інформація персонального характеру — зафіксована на матеріальному носії будь-яка інформація про фізичну особу, що ідентифікована чи може бути ідентифікована. Такою, що може бути ідентифікована, вважається будь-яка фізична особа, чия особистість може бути встановлена безпосередньо чи опосередковано, зокрема через ідентифікаційний номер або один чи декілька специфічних елементів фізичної, фізіологічної, психічної, економічної, культурної або соціальної totoжності.

Державна таємниця — вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому Законом, державною таємницею і підлягають охороні державою.

Запит на інформацію — звернення з вимогою надати письмову або усну інформацію про діяльність органів влади, органів місцевого самоврядування з окремих питань.

Право власності на інформацію — це врегульовані законом суспільні відносини щодо володіння, користування і розпорядження інформацією.

1.3. Сфера дії Закону про свободу (доступ до інформації) охоплює відносини, пов'язані із забезпеченням права на доступ до інформації, якою володіють органи державної влади, органи місцевого самоврядування згідно із принципом, що така інформація повинна бути доступна громадянськості, щоб винятки з права на доступ до інформації були обмежені та чітко визначені.

Для цього Закону також поширюється на відносини, пов'язані із забезпеченням права на доступ до інформації, якою володіють приватні структури стосовно одержання інформації про себе особисто і в разі необхідності здійснення або захисту свого права; доступ до цієї інформації може бути обмежений у виняткових ситуаціях.

1.4. Право на свободу (доступ до) інформації здійснюється на підставі таких принципів:

- гарантованість права на доступ до інформації;
- відкритість, доступність інформації та свобода її обміну;
- об'єктивність, вірогідність інформації;
- повнота і точність інформації;
- законність одержання, використання, поширення та зберігання інформації;
- простота і своєчасність одержання інформації;
- непорушність прав інших громадян;

• забезпечення оскарження відмови або обмеження у наданні доступу до інформації.

1.5. Право на свободу (доступ до) інформації гарантується:

- обов'язком органів державної влади та органів місцевого самоврядування інформувати про себе та свою діяльність;
- створенням у державних органах та органах місцевого самоврядування спеціальних інформаційних служб або систем, що забезпечували б у встановленому порядку доступ до інформації;
- вільним доступом до статистичних даних, архівних, бібліотечних та музейних фондів; обмеження цього доступу зумовлюються лише специфікою цінностей та особливими умовами їх збереження, що визначається законодавством;
- створенням механізмів реалізації права на доступ до інформації;
- здійсненням контролю за додержанням законодавства про свободу інформації;
- встановленням відповідальності за порушення законодавства про свободу інформації.

II. РЕЖИМ ДОСТУПУ ДО ІНФОРМАЦІЇ. КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ

Необхідно чітко розмежовувати інформацію за режимом доступу до неї, а також визначити контроль (суб'єктів контролю) за режимом доступу до інформації.

2.1. За режимом доступу до інформації інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Існує державний та парламентський контроль за режимом доступу до інформації.

Завдання контролю за режимом доступу до інформації полягає в забезпеченні додержання вимог законодавства про інформацію всіма органами державної влади, органами місцевого самоврядування, фізичними та юридичними особами, недопущенні необґрунтованого віднесення відомостей до категорії інформації з обмеженим доступом.

Державний контроль за додержанням встановленого режиму здійснюється Уповноваженим органом виконавчої влади, правовий статус якого визначається Кабінетом Міністрів України.

Парламентський контроль за додержанням режиму доступу до інформації здійснюється Уповноваженим Верховної Ради України з прав людини.

2.2. Доступ до відкритої інформації забезпечується шляхом:

- систематичної публікації її в офіційних друкованих виданнях (бюлетенях, збірниках);
- поширення її засобами масової комунікації;
- безпосереднього її надання зацікавленим державним органам,

органам місцевого самоврядування, фізичним та юридичним особам.

Порядок і умови надання державним органам, органам місцевого самоврядування, фізичним та юридичним особам і представникам громадськості відомостей за запитами встановлюються цим Законом або договорами (угодами), якщо надання інформації здійснюється на договірній основі.

Обмеження права на одержання відкритої інформації забороняється законом.

2.3. До інформації з обмеженим доступом відносяться:

1) конфіденційна інформація;

2) таємна інформація.

Конфіденційною визнається інформація:

- якій було надано такого статусу згідно із законом;
- яка містить комерційну, службову, професійну та іншу таємницю;
- яка стосується приватного життя фізичних осіб (інформація персонального характеру).

Фізичні та юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбачені законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої загрожує життю і здоров'ю людей.

2.4. Інформація класифікується як комерційна таємниця, якщо у разі її розкриття, орган державної влади, орган місцевого самоврядування може вплинути на конкурентоспроможність особи, яка надала цю інформацію.

Захист комерційної таємниці фізичних або юридичних осіб не може обмежувати прав інших фізичних або юридичних осіб на доступ до інформації, яка є доступною відповідно до закону.

Не є комерційною таємницею установчі документи, документи, що дозволяють займатися господарською діяльністю, інформація за всіма встановленими формами державної звітності, дані, потрібні для обчислення й сплати податків (інших обов'язкових платежів), та документи про їх сплату й платоспроможність підприємства, установи, організації тощо.

2.5. Службовими таємницями є:

1) положення плану контролю-ревізійної роботи на термін до часу повідомлення об'єкта контролю про початок проведення ревізії (перевірки);

2) факти виявлених під час проведення ревізій і перевірок порушень, зловживань до їх повного документального підтвердження й закріплення в актах, а також заплановані з цією метою зустрічні перевірки, раптові інвентаризації готівки й майна, контрольні обміри та інші ревізійні дії;

3) надані правоохоронними органами оперативні та інші відомості щодо діяльності підприємств, установ і організацій (вчинених порушень, зловживань посадових осіб, дані посадовими особами письмові пояснення, протоколи допиту з конкретних питань тощо);

4) інформація про оперативну й слідчу роботу органів прокуратури, МВС, СБУ, їх органів дізнання в тих випадках, коли її розголошення може зашкодити слідству, порушити право людини на справедливий та об'єктивний розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи;

5) конкретні пояснення посадових осіб щодо виявлених фактів зловживань, крадіжок тощо;

6) відомості, які містяться у зверненнях громадян щодо їхнього (чи інших громадян) особистого життя, та інша інформація, що зачіпає (порушує) їхні права та законні інтереси;

7) документи, що становлять внутрішньовідомчу службу кореспонденцію (доповідні записки, листування між підрозділами, матеріали колегій тощо), якщо вони пов'язані з розробкою напрямку діяльності ДКРС, процесом прийняття рішень і передують їх прийняттю;

8) інформація банківських і фінансових установ, підготовлена на запити органів державної контролю-ревізійної служби;

9) чернетки матеріалів ревізій і перевірок.

Матеріали, які надаються для аналізу або перевірки, а також відомості та документи про фінансовий, майновий стан юридичних і фізичних осіб, що надходять до Уповноваженого органу виконавчої влади у сфері регулювання ринків фінансових послуг, становлять професійну таємницю і можуть бути використані лише для здійснення Уповнова-

женим органом його функцій, включаючи випадки щодо законодавчо встановленого порядку обміну інформацією.

Несанкціоноване розголошення будь-яких відомостей, матеріалів, документів, що відносяться до професійної таємниці, тягне відповідальність відповідно до законів, крім випадків, коли таке розголошення необхідне для запобігання легалізації грошей, набутих злочинним шляхом.

Інформацією, що містить іншу таємницю, визнається:

- 1) інформація, зібрана під час розгляду судових справ, до того як справу передадуть до суду, але не довше дії строку обмеження;
 - 2) інформація, зібрана в процесі здійснення державного нагляду, до набуття чинності рішення, прийнятого з цього питання;
 - 3) інформація, оприлюднення якої може зашкодити міжнародним відносинам держави;
 - 4) інформація, розкриття якої зашкодить об'єктам, що охороняються як національна спадщина;
 - 5) інформація, розкриття якої зашкодить збереженню території та біологічних видів, а також біорізноманітності та ареалам, що перебувають під охороною;
 - 6) інформація, що включає описи систем безпеки, організації системи безпеки та заходів безпеки;
 - 7) інформація про технологічні рішення, якщо її оприлюднення зашкодить інтересам розпорядника інформації або якщо угодою її віднесено до інформації для внутрішнього користування.
- Статус інформації з обмеженим доступом може бути надано інформації для внутрішнього користування органів державної влади, органів місцевого самоврядування щодо підготовки питань тільки протягом часу, коли такий орган приймає рішення стосовно певного питання.

2.6. Інформація, що стосується приватного життя фізичних осіб (інформація персонального характеру)

Кожна особа має право:

- знати у період збирання інформації, які відомості про неї і з якою метою збираються, як, ким і з якою метою вони використовуються;
- доступу до інформації про неї, заперечувати її правильність, повноту, доречність тощо.

Органи державної влади, органи місцевого самоврядування, інформаційні системи яких вміщують інформацію про громадян, зобов'язані надавати її безперешкодно і безкоштовно на вимогу осіб, яких вона стосується, крім випадків, передбачених законом, а також вживати заходів щодо запобігання несанкціонованому доступу до неї. У

разі порушень цих вимог Закон гарантує захист громадян від завданої їм шкоди використанням такої інформації.

Забороняється доступ сторонніх осіб до відомостей про іншу особу, зібраних відповідно до чинного законодавства органами державної влади, органами місцевого самоврядування.

Зберігання інформації про громадян не повинно тривати довше, ніж це необхідно для законно встановленої мети.

Всі установи, які збирають інформацію про громадян, повинні на початку роботи з нею здійснити у встановленому Кабінетом Міністрів України порядку державну реєстрацію відповідних баз даних.

Необхідна кількість даних про громадян, яку можна одержати законним шляхом, має бути максимально обмеженою і може використовуватися лише для законно встановленої мети.

Відмова в доступі до такої інформації, або приховування її, або незаконні збирання, використання, зберігання чи поширення можуть бути оскаржені до суду.

2.7. Інформація, що містить відомості, які становлять державну таємницю.

Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї здійснюється відповідно до закону про цю інформацію.

Порядок обігу такої інформації та її захисту визначається відповідними органами державної влади за умови додержання вимог, встановлених цим Законом.

Порядок і терміни оприлюднення таємної інформації визначаються відповідним законом.

III. РЕАЛІЗАЦІЯ ПРАВА НА ДОСТУП ДО ІНФОРМАЦІЇ

3.1. Кожна особа має право звернутися до державних органів, органів місцевого самоврядування, приватних осіб і вимагати надання будь-якого офіційного документа, незалежно від того, стосується цей документ її особисто чи ні, крім випадків обмеження доступу, передбачених цим Законом.

Особа, яка робить запит на інформацію, повинна оформити цей запит:

1) усно, звернувшись безпосередньо чи зателефонувавши до розпорядника інформації, або

2) письмово, шляхом особистого вручення запиту на інформацію, або надіславши його поштою, факсом чи електронною поштою.

Запит на інформацію може бути індивідуальним або колективним. Він подається у письмовій формі.

Особа, яка нездатна через неграмотність або недієздатність скласти запит на інформацію має право скласти усний запит, а службовець, що отримав усний запит, повинен оформити його у письмовій формі, вказавши в ній своє ім'я, посаду, що він обіймає в даній організації, та представити копію запиту особі, що його склала.

3.2. Запит на інформацію повинен містити таку інформацію, що надається в усній чи письмовій формі:

- 1) прізвище, ім'я та по батькові запитувача;
- 2) назву юридичної особи, у разі якщо запит на інформацію подається від її імені;
- 3) деталі, пов'язані з особою, яка робить запит на інформацію (поштова чи електронна адреса, факс або номер телефону), шляхом використання яких розпорядник інформації зможе надіслати інформацію чи зв'язатися з особою, яка зробила запит;
- 4) зміст інформації чи вид, назву та зміст документа, на який зроблено запит, або інформацію про реквізити документа, які відомі особі, що робить запит на інформацію;
- 5) спосіб задоволення запиту на інформацію.

Органи державної влади, органи місцевого самоврядування зобов'язані надавати інформацію, що стосується їхньої діяльності, письмово, усно або через інші засоби комунікації.

Запит на інформацію повинен визначити право, яке особа хоче захистити або здійснити шляхом складання запиту на інформацію, і зазначити причини, чому дана інформація необхідна для дотримання або захисту цього права.

Орган державної влади, орган місцевого самоврядування може визначити форму запитів на інформацію за умови, якщо такі форми значно не затримують розгляд запитів або не створюють надмірних перешкод для тих, хто їх складає.

Орган державної влади, орган місцевого самоврядування, який отримав запит на інформацію, повинен надати повідомлення, що підтверджує отримання запиту.

3.3. Орган державної влади, орган місцевого самоврядування повинен дати відповідь на запит на інформацію у строк, що не перевищує двадцяти робочих днів з моменту отримання запиту.

Якщо запит на інформацію стосується інформації, яка необхідна для захисту життя чи свободи особи, то відповідь повинна бути надана протягом 48 годин.

Орган державної влади, орган місцевого самоврядування може письмовим повідомленням продовжити строк розгляду запиту до одного місяця у випадку, якщо запит стосується великого обсягу інформації або вимагає пошуку інформації серед значної кількості даних, та якщо

виконання запиту протягом двадцяти робочих днів буде перешкоджати щоденній діяльності органу.

Невиконання вимоги надати відповідь на запит на інформацію вважається відмовою у його задоволенні.

3.4. Відповідь на запит на інформацію повинна бути надана у письмовій формі та містити:

- плату, у разі її стягнення щодо будь-якої частини запиту, що надається, та форму, у якій дана інформація буде представлена;
- причини відмови у задоволенні будь-якої частини запиту на інформацію;
- у випадку будь-якої відмови зазначати, чи зберігає орган державної влади або орган місцевого самоврядування відомості, що містять відповідну інформацію, факт такої відмови та обґрунтовані причини відмови у наданні інформації; та
- право особи, яка склала запит, на подання скарги.

Будь-яка частина запиту, яка визнана такою, що може бути розкрита, повинна бути передана негайно; єдина затримка у її наданні може бути спричинена положеннями, передбаченими п. 3.7 Концепції.

3.5. Відкрита інформація, яка не потребує будь-якої додаткової обробки, надається безкоштовно.

Плата за надання інформації не повинна перевищувати витрат на її пошук, додаткову обробку, копіювання документів або інформації. Орган державної влади, орган місцевого самоврядування може не вимагати компенсації за будь-які інші витрати, які виникли в процесі вирішення правових чи політичних питань, які стосуються відповіді на запит на інформацію.

Кожний запитувач інформації може клопотати про звільнення від оплати послуг, а орган державної влади чи орган місцевого самоврядування може прийняти рішення надати інформацію за меншу плату або безкоштовно.

Очікувана плата за надання інформації повинна бути повідомлена запитувачеві до реєстрації моменту його запиту.

3.6. Керівник установи, яка є розпорядником інформації, чи фізична особа — розпорядник інформації, несуть відповідальність за організацію доступу до інформації відповідно до Закону.

Розпорядник інформації може, використовуючи інструкцію чи інші документи, визначити структурну одиницю та посадових осіб чи службовців, відповідальних за задоволення запитів на інформацію (службовців з питань інформації) та публікацію інформації, а також за

процедуру внутрішнього опрацювання запиту на інформацію або підготовку інформації, що підлягає розкриттю.

Якщо розпорядник інформації не встановить компетенцію посадових осіб чи службовців щодо задоволення запитів на інформацію, то кожна посадова особа (чи службовець), якій доручено задовольнити запит на інформацію або до якої надійде запит, є відповідальною за задоволення запиту на інформацію таким способом, який відповідає згаданим вимогам.

Керівник установи, що є розпорядником інформації, несе відповідальність за належне розкриття інформації у спосіб, що відповідає встановленим вимогам, за винятком випадків, коли процес розкриття інформації покладається законодавством на іншу особу.

3.7. Відмова та відстрочка задоволення запиту на інформацію.

Розпорядник інформації повинен відмовити в задоволенні запиту, якщо:

- 1) інформація, яка вимагається, вінесена до інформації з обмеженим доступом, а особа, яка складає запит, не має права доступу до цієї інформації;
- 2) розпорядник інформації не володіє необхідною інформацією, не знає, хто володіє нею, і не може встановити розпорядника цієї інформації;
- 3) задоволення запиту на інформацію є неможливим, оскільки зі змісту запиту не зрозуміло, яка саме інформація необхідна особі, яка робить запит;
- 4) особа, яка складає запит на інформацію, не оплатила витрати, пов'язані із задоволенням запиту на інформацію, якщо плата передбачена законом, а розпорядник інформації не відкликав вимоги щодо компенсації понесених витрат.

Розпорядник інформації має право відмовитися задовольнити запит, якщо:

- 1) необхідна інформація вже була надана іншій особі, яка склала запит, і особа не дає пояснень про необхідність одержання інформації повторно;
- 2) задоволення запиту вимагатиме зміни в організації роботи розпорядника інформації, порушить виконання покладених на нього завдань або вимагатиме непотрібних і непропорційних витрат через великі обсяги інформації, що вимагається;
- 3) запит на інформацію не може бути задоволений лише наданням інформації.

Відмова в задоволенні запиту доводиться до відома запитувача у письмовій формі з роз'ясненням порядку оскарження прийнятого рішення.

У відмові має бути зазначено:

- 1) посадову особу (розпорядника інформації);
- 2) дату відмови;
- 3) мотивовану підставу відмови;

Відстрочка задоволення запиту допускається у разі, якщо запитуваний документ не може бути наданий для ознайомлення у місячний термін. Повідомлення про відстрочку доводиться до відома запитувача у письмовій формі з роз'ясненням порядку оскарження прийнятого рішення.

У повідомленні про відстрочку має бути зазначено:

- 1) посадову особу розпорядника інформації;
- 2) дату надсилання або видачі повідомлення про відстрочку;
- 3) причини, з яких запитуваний документ не може бути видано у встановлений цим Законом строк;
- 4) строк, у який буде задоволено запит.

Відмова та відстрочка задоволення запиту щодо надання письмової інформації здійснюються в аналогічному порядку.

3.8. Відмову або відстрочку задоволення запиту на інформацію може бути оскаржено.

У разі відмови у наданні інформації (документа, який містить необхідну інформацію) для ознайомлення або відстрочки задоволення запиту на інформацію запитувач має право оскаржити відмову або відстрочку до органу вишого рівня.

Якщо на скаргу, подану до органу вишого рівня, дається негативна відповідь, запитувач має право оскаржити цю відмову до Уповноваженого органу виконавчої влади, а в разі незадоволення його рішенням — до Уповноваженого Верховної Ради України з прав людини (надалі — Уповноважений).

Відмову або відстрочку задоволення запиту на інформацію може бути оскаржено безпосередньо до суду.

3.9. Не підлягають обов'язковому наданню для ознайомлення за запитами на інформацію офіційні документи, які містять у собі:

- інформацію, визнану у встановленому порядку державною таємницею;
- конфіденційну інформацію;
- інформацію про оперативну і слідчу роботу органів прокуратури, МВС, СБУ, роботу органів дізнання та суду в тих випадках, коли її розголошення може зашкодити оперативним заходам, розслідуванню чи дізнанню, порушити право людини на справедливий та об'єктивний судовий розгляд її справи, створити загрозу життю та здоров'ю будь-якої особи;

- інформацію, що стосується особистого життя громадян;
- документи, що становлять внутрішньовідомчу службу кореспонденцію (доповідні записки, листування між підрозділами та інше), якщо вони пов'язані з розробкою напряму діяльності установи, процесом прийняття рішень і передують їх прийняттю;
- інформацію, що не підлягає розголошенню згідно з іншими законодавчими або нормативними актами. Установа, до якої звернуто запит на інформацію, може не надавати для ознайомлення документ, якщо він містить інформацію, яка не підлягає розголошенню на підставі нормативного акта іншої державної установи, а та державна установа, яка розглядає запит на інформацію, не має права вирішувати питання щодо її розсекречення;
- інформацію фінансових установ, підготовлену для контрольно-фінансових відомств.

3.10. Інформація є об'єктом права власності фізичних, юридичних осіб та держави. Інформація може бути об'єктом права власності як у повному обсязі, так і об'єктом лише володіння, користування чи розпорядження.

Власник інформації щодо об'єктів своєї власності має право здійснювати будь-які законні дії.

- Підставами виникнення права власності на інформацію є:
- створення інформації своїми силами і за свій рахунок;
 - договір на створення інформації;
 - договір, що містить умови переходу права власності на інформацію до іншої особи.

Інформація, створена на кошти державного бюджету, є державною власністю.

Власник інформації має право призначити особу, яка здійснює володіння, користування і розпорядження інформацією, і визначати правила обробки інформації та доступ до неї, а також встановлювати інші умови щодо інформації.

IV. СУБ'ЄКТИ ВІДНОСИН У СФЕРІ ДОСТУПУ ДО ІНФОРМАЦІЇ, ЇХНІ ПРАВА ТА ОБОВ'ЯЗКИ

Необхідно визначити перелік уповноважених суб'єктів, їхню компетенцію щодо забезпечення здійснення громадянами права на доступ до інформації. У деяких зарубіжних країнах існують органи парламентського контролю за забезпеченням доступу до інформації, омбудсмени (уповноважені з питань інформації), або окремі органи ви-

конавчої влади, які відповідають за весь спектр питань, пов'язаних з інформацією. В Україні немає таких органів, тому немає можливості оскаржувати відмови у доступі до інформації, окрім як у судовому порядку, що є, як правило, неефективним. Тому повноваження парламентського контролю щодо здійснення права на доступ до інформації покладеться на Уповноваженого Верховної Ради України з прав людини, а державного контролю — на Уповноважений орган виконавчої влади.

4.1. Суб'єктами відносин у сфері доступу до інформації є:

- 1) фізичні, юридичні особи — запитувачі інформації;
- 2) органи державної влади, органи місцевого самоврядування, юридичні особи державного сектора, недержавні юридичні особи та фізичні особи на умовах, визначених частинами першою і другою статті 28, а також, у разі створення, службовці з питань інформації — розпорядники інформації;
- 3) Уповноважений орган виконавчої влади, відповідальний за здійснення державної політики у сфері забезпечення доступу до інформації (надалі — Уповноважений орган виконавчої влади);
- 4) Уповноважений Верховної Ради України з прав людини.

4.2. Суб'єкти відносин у сфері доступу до інформації мають право одержувати (виробляти, добувати), використовувати, поширювати та зберігати інформацію у будь-якій формі з використанням будь-яких засобів, крім випадків, передбачених законом.

Кожний суб'єкт відносин у сфері доступу до інформації для забезпечення своїх прав, свобод та законних інтересів має право про одержання інформації про:

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

4.3. Суб'єкти відносин у сфері доступу до інформації зобов'язані:

- поважати права та свободи інших осіб;
- використовувати інформацію відповідно до закону або договору (угоди);
- забезпечувати додержання принципів свободи інформації;
- забезпечувати доступ до інформації на умовах, передбачених законом або договором (угодою);
- зберігати інформацію в належному стані протягом встановленого строку і надавати іншим особам у встановленому законом порядку;
- відшкодовувати шкоду, заподіяну при порушенні законодавства про свободу інформації.

4.4. Обов'язок оприлюднювати інформацію.

Кожний орган державної влади, орган місцевого самоврядування зобов'язаний публікувати та поширювати в доступній формі не рідше ніж один раз на рік інформацію, яка містить:

- 1) опис своєї організаційної структури, функцій, повноважень та фінансових ресурсів;
- 2) детальні дані про послуги, які орган безпосередньо надає громадянам;
- 3) механізми складання запиту на інформацію чи механізми оскарження, доступні для громадян, які стосуються діяльності або бездіяльності даного органу, разом зі стислим змістом запитів, скарг та ін.;
- 4) інструкцію, яка містить адекватні інформації про систему обліку, види інформації, яку зберігає орган, категорії інформації, що публікується, а також процедури, якої необхідно дотримуватися при складанні запиту на інформацію;
- 5) опис функціональних обов'язків керівництва органу та процедури прийняття рішень;
- 6) будь-які акти, правила, інструкції щодо виконання органом своїх функцій;
- 7) зміст усіх прийнятих рішень, які зачіпають інтереси громадян разом з причинами, які обґрунтовують необхідність їх прийняття, офіційним тлумаченням положень та іншими важливими матеріалами, які їх стосуються;
- 8) будь-які механізми чи процедури, за допомогою яких громадськість може представляти свої інтереси або в інший спосіб впливати на процес формування політики чи на реалізацію повноважень органу.

4.5. Обов'язки розпорядників інформації поширюються на недержавних юридичних осіб та фізичних осіб, якщо вони виконують державні обов'язки відповідно до законодавства чи за контрактом, включаючи надання освітніх, соціальних або інших державних послуг, — стосовно інформації, пов'язаної з виконанням їхніх обов'язків.

До розпорядників інформації прирівнюються:

- 1) підприємства, що займають домінуюче становище на ринку, або наділені спеціальними чи виключними правами, або є природними монополіями, — стосовно інформації щодо умов та цін постачання товарів, послуг та цін на них;
- 2) неприбуткові асоціації, фонди та компанії, у яких державний орган, орган місцевого самоврядування чи недержавна юридична особа є членом, засновником або учасником, — стосовно інформації щодо використання фондів, виділених з державного чи місцевого бюджетів.

Розпорядники інформації зобов'язані надати доступ до інформації, якщо вони володіють, згідно з процедурами, передбаченими Законом.

Надаючи доступ до інформації, розпорядник інформації зобов'язаний:

- 1) забезпечити доступ до документів, до яких особа, яка робить запит на інформацію, просить дати їй доступ, якщо ця особа має право на доступ до інформації;
- 2) вести реєстр документів, зберігання яких йому довірено;
- 3) розголошувати інформацію, яку належить розкривати відповідно до Закону;
- 4) регулярно оприлюднювати інформацію щодо виконання обов'язків державою;
- 5) допомагати особам, які складають запит на інформацію;
- 6) інформувати осіб, які роблять запит на інформацію, про існуючі обмеження доступу до документів;
- 7) забезпечити додержання обмежень на доступ до інформації;
- 8) не надавати свідомо дезорієнтуючу, неточну та недостовірну інформацію, а також, у випадку сумніву, перевіряти правильність і точність наданої інформації.

Орган державної влади, орган місцевого самоврядування (службовці з питань інформації — у разі створення такої посади) повинен щорічно подавати Уповноваженому Верховної ради України з прав людини звіт про свою діяльність стосовно запитів на інформацію, який повинен містити таку інформацію:

- кількість отриманих запитів на інформацію, задоволених або відхилених;
- кількість разів і на основі яких норм закону були відхилені запити на інформацію;
- кількість скарг на відмову у наданні інформації;
- плата, стягнена за задоволення запитів на інформацію;
- інформацію про виконання обов'язку оприлюднювати інформацію;
- іншу необхідну інформацію.

4.6. Уповноважений орган виконавчої влади здійснює державний нагляд за розпорядниками інформації у процесі задоволення запитів на інформацію та її розкриття.

Уповноважений орган виконавчої влади може здійснювати контрольні перевірки на основі скарг чи з власної ініціативи.

У процесі здійснення контролю Уповноважений орган виконавчої влади повинен пересвідчитися, що:

- 1) кожен запит на інформацію було зареєстровано відповідно до процедури, визначеної Законом;

- 2) кожен запит на інформацію було задоволено згідно з процедурою, у межах строку та у спосіб, передбачений Законом;
- 3) відмова задовольнити певний запит на інформацію або відстроювання задоволення вимогам Закону;
- 4) обмеження доступу до певної інформації встановлено відповідно до процедури, передбаченої Законом;
- 5) кожен розпорядник інформації виконує свої обов'язки щодо оприлюднення інформації.

4.7. Уповноважений Верховної Ради України з прав людини (надалі — Уповноважений) є орган парламентського контролю за додержанням конституційних прав і свобод людини.

Правовий статус Уповноваженого визначається Конституцією України і Законом.

Уповноважений забезпечує реалізацію прав громадян на вільний доступ до інформації в порядку, визначеному цим Законом.

У. ПРОЦЕДУРА ОСКАРЖЕННЯ ВІДМОВИ І ВІДСТРОЧКИ ЗАДОВОЛЕННЯ ЗАПИТУ НА ІНФОРМАЦІЮ

5.1. Нагляд за виконанням цього Закону в межах своєї компетенції здійснюють:

- 1) Уповноважений орган виконавчої влади відповідно до процедури, передбаченої цим Законом;
- 2) Уповноважений Верховної Ради України з прав людини.

5.2. Подання скарги до Уповноваженого органу виконавчої влади.

Особа, яка отримала відмову в задоволенні запиту на інформацію чи в разі відстроювання задоволення запиту, а також негативну відповідь органу вищого рівня в разі оскарження до нього цієї відмови чи відстроювання, має право звернутися до Уповноваженого органу виконавчої влади з проханням розпочати контрольні перевірки.

Особа, що звертається з проханням розпочати контрольні перевірки Уповноваженим органом виконавчої влади, повинна подати письмову скаргу, яка повинна містити:

- 1) ім'я та прізвище особи, яка подає скаргу, на ім'я якої подається скарга, якщо скарга подається на ім'я іншої особи;
- 2) поштова адреса та контактний телефон особи;
- 3) інформація про розпорядника інформації, який відмовляється задовольнити запит на інформацію або не відповів на такий запит, або якщо представлена інформація є недостовірною;
- 4) зміст запиту на інформацію, поданого розпорядником;

- 5) підстави особи, яка робить запит на інформацію, вважати, що діяльність розпорядника інформації є незаконною.

Якщо, на думку особи, яка подає скаргу, розпорядник інформації відмовився задовольнити запит незаконно чи представив недостовірну інформацію, особа, яка подає скаргу, повинна додати копію письмової відмови розпорядника інформації задовольнити запит або недостовірну інформацію, представлену розпорядником інформації.

5.3. Розгляд скарг Уповноваженим органом виконавчої влади.

Уповноважений орган виконавчої влади повинен проаналізувати скаргу та перевірити правильність дій розпорядника інформації протягом десяти днів після одержання скарги.

Уповноважений орган виконавчої влади може продовжити строк розгляду до тридцяти днів, якщо необхідно уточнити скаргу або надати додаткові пояснення та документи для розгляду скарги. Уповноважений орган виконавчої влади повинен повідомити особу, яка подає скаргу, про будь-яке продовження строку розгляду протягом десяти днів після одержання скарги.

5.4. Уповноважений орган виконавчої влади може відмовити у розгляді скарги, якщо:

- 1) скарга є анонімною;
- 2) подана скарга не стосується діяльності конкретного розпорядника інформації;
- 3) набуло чинності рішення суду в тій самій справі;
- 4) скарга є безпідставною, оскільки дії розпорядника інформації стосовно відмови у задоволенні запиту на інформацію були законними.

Уповноважений орган виконавчої влади повинен повідомити особу, яка подає скаргу, про свою відмову розглянути скаргу в письмовій формі, виклавши причини відмови.

Якщо особа, яка подає скаргу, не погоджується з рішенням Уповноваженого органу виконавчої влади, то вона має право оскаржити його до Уповноваженого Верховної Ради України з прав людини.

5.5. Компетентні посадові особи Уповноваженого органу виконавчої влади, які здійснюють контроль, мають право:

- 1) вимагати пояснень та документів від розпорядників інформації;
- 2) перевірити документи стосовно доступу до інформації, що належить розпорядникам інформації, а також внутрішні документи, доступ до яких обмежено;
- 3) дати вказівку розпорядникам інформації дотримуватися законодавства;

- 4) розпочати розслідування у справах, що стосуються адміністративних правопорушень відповідно до процедури, передбаченої КпАП;
- 5) зробити пропозицію розпорядникам інформації щодо вдосконалення організації доступу до інформації.

Уповноважений орган виконавчої влади повинен повідомити особу, яка подає скаргу, розпорядника інформації та вищий орган чи установу розпорядника про результати перевірки.

5.6. Уповноважений орган виконавчої влади може видати вказівки щодо приведення розпорядником інформації своєї діяльності у відповідність до Закону, якщо Уповноважений орган виконавчої влади переконається, що розпорядник інформації:

- 1) незаконно відмовив у задоволенні запиту;
- 2) не відповів на запит у межах встановленого строку;
- 3) не задовольнив запит належним чином;
- 4) не опрацював запит на інформацію належним чином;
- 5) не оприлюднив інформацію, як це вимагається;
- 6) незаконно встановив обмеження на доступ до інформації;
- 7) не встановив обмеження на доступ до інформації, яка містить персональні дані;
- 8) надав доступ до інформації, обмеження на доступ до якої встановлюються відповідно до цього Закону.

5.7. Розпорядник інформації повинен протягом п'яти робочих днів після одержання вказівки вжити заходів щодо виконання вказівок, а також повинен повідомити про це Уповноважений орган виконавчої влади.

Розпорядник має право оскаржити вказівку в суді.

5.8. Якщо розпорядник інформації не виконує вказівки Уповноваженого органу виконавчої влади і не оскаржив її в суді, Уповноважений орган виконавчої влади повинен почати адміністративне розслідування.

5.9. Подання скарги Уповноваженому.

Особа, яка склала запит на інформацію і після звернення до Уповноваженого органу виконавчої влади, має право звернутися до Уповноваженого для прийняття рішення у справі невиконання розпорядником інформації зобов'язань стосовно задоволення запиту на інформацію.

5.10. Рішення Уповноваженого щодо скарги.

Уповноважений приймє рішення щодо скарги у строк, що не перевищує 30 днів після одержання скарги.

Уповноважений має право відхилити скарги, які є безпідставними, або якщо скажник не використав будь-яких внутрішніх механізмів оскарження, передбачених законом.

У своєму рішенні Уповноважений має право:

- 1) відхилити скаргу;
- 2) вимагати від розпорядників інформацією здійснити кроки, необхідні для приведення їхніх дій у відповідність із нормами цього Закону;
- 3) вимагати відшкодування скажникові шкоди, якої він зазнав; та/або

4) у випадку очевидних порушень (помилки) розпорядниками інформації щодо виконання положень цього Закону, накласти на них штраф.

5.11. До моменту прийняття рішень Уповноважений має право проводити розслідування, включаючи видання наказів, необхідних для підтвердження доказів або змуснення свідків до зізнання.

Уповноважений може протягом розслідування проводити оцінку будь-яких відомостей (інформації) відповідно до цього Закону, жодна така інформація за жодних умов не може бути прихована від Уповноваженого.

5.12. Рішення Уповноваженого органу виконавчої влади, рішення Уповноваженого може бути оскаржено до суду.

5.13. Оскарження рішення розпорядника інформації до суду.

Запитувач має право оскаржити відмову розпорядника інформації у задоволенні або відстроку задоволення запиту на інформацію безпосередньо до суду.

У разі, коли запитувач звернувся до суду, обов'язок доводити законність відмови чи відстроки задоволення запиту покладається на відповідача — розпорядника інформації.

Суд має право для забезпечення повноти та об'єктивності розгляду справи запитати офіційні документи, у можливості ознайомлення з якими було відмовлено, і, вивчивши їх, прийняти рішення про обґрунтованість (або необґрунтованість) дій розпорядників інформації. Якщо відмову або відстроку визнано необґрунтованою, суд зобов'язує розпорядника інформації надати запитувачеві змогу ознайомитися з офіційним документом і виносить окрему ухвалу щодо посадових осіб розпорядників інформації, які відмовили запитувачеві.

Необґрунтована відмова у наданні змоги ознайомитися з офіційними документами або порушення визначеного строку її надання без поважних причин тягнуть за собою дисциплінарну або іншу відповіді-

дальність посадових осіб державних установ у порядку, встановленому законами України.

VI. ОХОРОНА ІНФОРМАЦІЇ. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО СВОБОДУ ІНФОРМАЦІЇ

6.1. Право на свободу інформації охороняється законом. Держава гарантує всім суб'єктам відносин у сфері доступу до інформації рівні права і можливості доступу до інформації.

Ніхто не може обмежувати права особи у виборі форми і джерел одержання інформації, за винятком випадків, передбачених законом.

Суб'єкт права на свободу інформації може вимагати усунення будь-яких порушень його права.

6.2. Інформація не може бути використана для закликів до поваження конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання расової, національної, релігійної ворожнечі, посягання на права і свободи людини.

Не підлягають розголошенню відомості, що становлять державну та іншу передбачену законодавством таємницю.

Не підлягають розголошенню відомості, що стосуються лікарської таємниці, прошових вкладів, прибутків від підприємницької діяльності, усиновлення (удочеріння), листування, телефонних розмов і телеграфних повідомлень, крім випадків, передбачених законом.

6.3. Відповідальність за порушення законодавства про свободу інформації.

Порушення законодавства України про свободу інформації тягне за собою дисциплінарну, цивільну, адміністративну або кримінальну відповідальність відповідно до законодавства України.

Відповідальність за порушення законодавства про свободу інформації несуть особи, винні у вчиненні таких порушень, як:

- необґрунтована відмова від надання відповідної інформації;
- надання інформації, що не відповідає дійсності;
- несвоєчасне надання інформації;
- навмисне приховування інформації;
- примушення до поширення або перешкоджання поширенню чи безпідставна відмова від поширення певної інформації;
- поширення відомостей, що не відповідають дійсності, ганьблять честь і гідність особи;

• використання і поширення інформації стосовно особистого життя громадянина без його згоди особою, яка є власником відповідної інформації внаслідок виконання своїх службових обов'язків;

• розголошення державної або іншої таємниці, що охороняється законом, особою, яка повинна охороняти цю таємницю;

• порушення порядку зберігання інформації;

• навмисне знищення інформації;

• необґрунтоване віднесення окремих видів інформації до категорії відомостей з обмеженим доступом.

6.4. Відшкодування матеріальної чи моральної шкоди

У випадках, коли правопорушення завдають фізичним, юридичним особам, органами державної влади, органам місцевого самоврядування матеріальної або моральної шкоди, особи, винні в цьому, відшкодовують її на підставі рішення суду. Розмір відшкодування визначається судом.

VII. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

ЧАСТИНА II

ЕЛЕКТРОННЕ УРЯДУВАННЯ:
СВІТОВИЙ ДОСВІД
І УКРАЇНСЬКІ РЕАЛІЇ

1. ПОНЯТТЯ І СУТЬ ЕЛЕКТРОННОГО УРЯДУВАННЯ

Поняття «електронне урядування» на сьогодні вже не є цілком невідомим і новим, як це було кілька років тому. Пов'язуючи його з доступом до публічної інформації, можна сказати, що воно є ефективним засобом забезпечення такого доступу, а отже, сприяє прозорості та ефективності діяльності публічної адміністрації. З метою визначення змісту і ролі електронного урядування у даному контексті перш за все необхідно з'ясувати, що слід розуміти під самим поняттям «електронне урядування».

Існує багато дилем з приводу визначення цього поняття. Так, наприклад, на Заході поняття «електронне урядування» (англ. — «e-government» — дослідний переклад — «електронний уряд») не завжди розуміли однозначно. У певний час так називали футуристичний уряд «електронних проматан», що регулює життя і безпеку мережі в цілому й електронний бізнес зокрема. У сучасному розумінні термін «e-government» тлумачиться набагато ширше, ніж «електронний уряд» чи навіть більш правильне визначення — «електронне управління державою», тобто використання в органах державного управління сучасних технологій, у тому числі й інтернет-технологій. E-government зараз — це дуже лаконічний опис сучасного підходу до визначення ролі урядових органів у житті держави і суспільства, що все більше поширюється на Заході.

Отож, однозначного визначення «електронного уряду» сьогодні не існує. Дослідний переклад «e-government» не зовсім точний за змістом. Зрозуміло, що мається на увазі не тільки мережева інфраструктура виконавчої влади, а в цілому і вся інфраструктура органів влади. Можливо, мова повинна йти про «електронну державу», «електронний державний апарат», електронну інфраструктуру держави, державу інформаційного суспільства, або ж «електронне урядування». Замість «електронного уряду» більш доречно говорити про державну мережеву інформаційну інфраструктуру як інформаційно-комунікаційну систему, що забезпечує оптимальне, з погляду суспільства, функціонування всіх гілок і рівнів державної влади.

Визначення електронного урядування формується фахівцями, виходячи з різних принципів. Одні автори віддають перевагу визначенням описового характеру — які саме зміни відбуваються в суспільстві й окремих його структурах завдяки впровадженню електронного урядування. Інші вибирають прикладний аспект електронного урядування і просто перелічують різні застосування окремих його інструментів. Є також короткі технічні визначення, що акцентують увагу винятково на застосованих технологічних рішеннях і специфічних програмних продуктах, і економічні, що орієнтовані на максимальну ефективність управління державою. Кожний принцип правильний, оскільки у свій спосіб відображає конкретний аспект функціонування електронного урядування⁷¹.

⁷¹ Голобуцький О., Шевчук О. Електронний уряд. — К.: ЗАТ «Атлант UMS», 2002. — С. 9.

Концепція електронного урядування складається з двох взаємозалежних (і водночас самостійних) проєктів (підконцепцій). Це внутрішня урядова інформаційна інфраструктура, аналог корпоративної мережі, та зовнішня інформаційна інфраструктура, що взаємодіє з громадянами й організаціями. У рамках концепції «електронної держави» інтегруються інформаційні ресурси органів державної влади, забезпечують доступ до них, а також створюється система он-лайнних послуг (у тому числі, тих, що мають вартісне вираження). Урядова мережева інфраструктура повинна бути націлена на вирішення актуальних політичних, економічних і соціальних завдань держави і забезпечувати:

- реалізацію права громадян на доступ до відкритої державної інформації;
- доведення до громадськості об'єктивної і достовірної інформації про діяльність органів державної влади, що зміцнює довіру до держави та її політики;
- взаємодію і постійний діалог держави з громадянами й громадськими інституціями, а також необхідний рівень суспільного контролю за діяльністю державних органів і організацій;
- об'єднання інформаційних ресурсів і послуг органів державної влади, і місцевого самоврядування з метою зміцнення загальнонаціонального інформаційного простору;

• удосконалення системи державного управління, оптимізацію структури державного апарату, зниження фінансових і матеріальних витрат на його зміст, поетапне переведення частини державних послуг, що мають вартісне вираження, у систему державних мережевих послуг, що відповідає реальним потребам громадян і організацій;

• ефективну підтримку економічної діяльності державних суб'єктів, що займаються господарською діяльністю, дозволяючи їм ефективно інтегруватися в загальнонаціональний і світовий економічний простір;

• взаємодію і співробітництво з державними органами зарубіжних країн і міжнародних неурядових організацій.

Узагальнивши всі визначення поняття «електронний уряд», на нашу думку, доцільніше використовувати термін «*електронне урядування*», під яким слід розуміти *спосіб організації державної влади за допомогою систем логічних інформаційних мереж та сегментів глобальної інформаційної мережі, яка забезпечує функціонування певних служб в режимі реального часу та робить максимально простим і доступним щоденне спілкування громадянина з офіційними установами*.

На думку генерального бізнес-керівника корпорації Intel Стейсі Джерела Сміта, досягнення успіху в проєктах створення «електронного урядування» у будь-якій країні світу забезпечується наявністю трьох основних компонентів:

— забезпечення доступу до нових технологій якомога більшої кількості населення шляхом зменшення вартості доступу до мережі Інтернет, проєкту організації вивчення нових технологій, створення інтернет-кіосків;

— створення розгалуженої телекомунікаційної інфраструктури, що сприятиме активному розвитку різноманітних сфер соціально-економічного життя суспільства;

— затвердження відповідного законодавства, де чітко були б визначені права та обов'язки людини в «електронному суспільстві», а також базова термінологія⁷².

Загалом можна виділити наступні базові принципи функціонування системи електронного урядування:

- надання послуг у будь-який момент (електронне урядування працює 24 години на добу, 7 днів на тиждень, 365 днів на рік);
- максимальна простота і прозорість (має обслуговувати звичайних громадян, а не лише фахівців);
- єдині технічні стандарти і взаємна сумісність (електронні додатки повинні відповідати принципам загальної архітектури систем ідентифікації, безпеки, дизайну);
- забезпечення конфіденційності і дотримання правил інформаційної безпеки;
- беззастережна орієнтація на думку громадян при реалізації нововведень.

Шлях до електронного урядування складається з чотирьох окремих етапів. На першому етапі органи державної влади використовують мережу для розміщення інформації про себе для зручності громадян і ділових партнерів. Уже створені і працюють тисячі таких сайтів, що передачають односторонній зв'язок. На другому етапі ці сайти стають інструментами для двостороннього спілкування, що дозволяє громадянам повідомляти нову інформацію про себе і, наприклад, про зміну адреси (замість того, щоб дзвонити або писати з цього приводу). Таких сайтів теж чимало, хоча багато з них спрямовані на використання електронної пошти. На третьому етапі всі сайти надають можливість здійснювати офіційний і вартісний обмін інформацією, що підлягає кількісному виміру. Це може включати продовження терміну дії ліцензії, сплату штрафу або запис на курс навчання. Останній етап передбачає наявність порталу, що інтегрує весь комплекс послуг уряду і забезпечує доступ до них, виходячи з потреб і функціональних аспектів, а не з існуючої структури департаментів і відомств. Просте ім'я для входу в систему і пароль дозволять користувачеві спілкуватися з будь-яким підрозділом уряду. У багатьох іноземних урядах уже є плани створення таких порталів, однак у даний час лише два подібних сайти мають рівень вище місцевого: МАХІ, створений в австралійському штаті Вікторія, і eCitizen Centre, створений у Сінгапурі⁷³.

У кожній державі діяльність уряду сконцентрована навколо трьох основних сфер:

⁷² Брамс А. Intel готов сотрудничать электронному развитию Украины. // Агентство Интернет-Новостей 18.12.2001.

⁷³ Правительство и Интернет // Эксперт, 2000. // www.expert.ru/economy/govet.shtml.

економічний розвиток (виробництво і торгівля, підвищення конкурентоспроможності вітчизняних виробників на міжнародному ринку) — сегмент «уряд — бізнесу» (G2B);

підвищення ефективності роботи управлінського апарату (збір податків, закони і регулювання, реєстрація інформації, пошта) — сегмент «уряд — уряд» (G2G);

якості життя громадян (соціальні послуги, охорона здоров'я, безпека, освіта, захист навколишнього середовища) — сегмент «уряд — громадянинові» (G2C).

Забезпечення максимальної ефективності процесу управління державою, національного економікою та соціальними процесами, зробивши цю систему комфортнішою для споживача, — ось основне завдання електронного урядування.

Органи влади повинні використовувати найкращі і найсучасніші технології у галузі електронної пошти, електронного документообігу і комунікацій, що не поступаються технологіям корпоративного і приватного сектора. Створення єдиних точок контакту підвищує ефективність роботи. Міжвідомчий підхід дозволяє припинити розповсюджений вид шахрайства, коли особа кілька разів одержує ту саму пільгу, звертаючись за нею в різні інстанції⁷⁴.

Процес глобалізації набув неповоротного характеру. Прискорення темпів економічного розвитку змушує держави реагувати на зміни не менш швидко, аніж приватні структури. Для того щоб діалог (а в деяких випадках і співробітництво громадян з державою) був ефективним, ощадливим і мобільними, необхідно створити інтегровану електронну систему відносин платників податків з державою. Звичайно, така система має містити в собі доступ до інформації і послуг на веб-сайтах, по телефону, електронною поштою й у звичайному «офф-лайнному» режимі. Головним фактором стає зручність платника податків (громадянина або компанії), а не державних структур.

Кінцевою метою спільної роботи органів влади і платників податків повинно стати прийняття такого рішення, що створює нові переваги і нові можливості для населення, бізнесу, урядових структур.

Не варто очікувати миттєвої трансформації державних структур. Це досить тривалий процес. Він вимагає зміни культури відносин органів влади з платниками податків і форм взаємодії державних установ, розвитку нових навичок у всіх учасників процесу, наймання нового персоналу в урядові установи⁷⁵.

Перехід до застосування методів електронного урядування має вестися в усіх напрямках державного управління і суспільного сектора; відставання яких-небудь сфер порушить динаміку інформаційного розвитку країни. Перехід на інтернет-технології в масштабі країни фактично означає

трансформацію всіх основних форм діяльності урядових закладів і є складним організаційним, технологічним, соціальним процесом, що вимагає значних фінансових витрат і адміністративних зусиль. Успіх залежить від правильної стратегії і тактики на кожному з етапів реалізації програми, раціональної організації, координації і взаємодії всіх учасників процесу — виконавчої, законодавчої, судової влади всіх рівнів, бізнесу (бізнес-структур), університетів, громадських організацій і громадян. Треба буде розв'язати комплекс взаємозалежних політичних, правових, управлінських і технологічних питань, визначити джерела фінансування, навчити персонал. Процес комерціалізації уряду торкнувся всіх рівнів влади. Оптимальним вирішенням визнано створення загальнонаціональної багатофункціональної і багаторівневої інтегрованої інформаційної системи на базі Інтернету, у рамках якої забезпечуватиметься як управління країною і взаємодія урядових органів усіх рівнів (закритий для населення рівень), так і доступ населення до відкритої урядової інформації. Створення кожною державною інституцією окремих відкритих сайтів є нераціональним кроком. Прозорість уряду є важливим соціальним елементом і включає поступовий перехід інформаційного обслуговування громадян на електронні технології, що зводиться до країни знанні кошти. Крім того, діалог населення з урядовими службовцями через Інтернет дозволить раціональніше організувати взаємодію влади і громадян і оптимізувати процедуру спілкування. Органи влади стануть більш відкритими для населення, діяльність і конкретні рішення міністерств і відомств, місцевих органів влади стануть більш зрозумілими для громадян і підконтрольними їм. Прозорість публічної адміністрації буде сприяти підвищенню рівня довіри населення до влади, більшій ефективності влади і, як результат, — зменшенню стабільності в країні. Разом з тим, враховуючи, що в даний час до 90 % звернень до влади всіх рівнів здійснюється при особистому контакті громадян і співробітників державного апарату, і в майбутньому також збереться частина населення, що віддасть перевагу традиційному спілкуванню, потрібно розробити оптимальне співвідношення обох процедур і раціональний розподіл ресурсів на їх розвиток.

Перехід до «електронного урядування» починається з того, що різноманітні організації починають використовувати Інтернет. Пізніше організації починають надавати повну динамічну інформацію, з можливістю для пошуку за базами даних і службою відповідей на посилення електронною поштою. Установи все більше прагнуть запроваджувати різноманітні інтерактивні послуги, які дозволяють громадянам знаходити на державних веб-сайт і заповнювати різноманітні форми, призначати зустрічі, шукати роботу і так далі. Наступний крок — можливість надання фінансових і адміністративних послуг, щоб громадяни і приватні фірми могли купувати ліцензії і дозволи, подавати податкові декларації, платити штрафи за неналежне паркування і звертатися з проханнями про соціальні пільги. Це вимагає підвищення безпеки інформаційної структури «електронного урядування», що можна, як правило, досягти більш широким використанням таких технологій, як електронні підписи

⁷⁴ Задачи и возможности электронного правительства // <http://www.biz.pl/egov/articale.rhtml?id=6>.

⁷⁵ Голобуцький О., Шевчук О. Електронний уряд... — С. 28.

і сертифікати, а також смарт-карти. Потім організації можуть захотіти співпрацювати над втіленням порталів, які б дозволяли громадянам переходити від однієї служби до іншої без необхідності знову посідчувати свою особу. Інформація і послуги можуть бути тематично згруповані за життєвими ситуаціями або за конкретними галузями і в такому вигляді надані людям. У цей момент кількість процедур обміну інформацією через Інтернет досягне рівня «критичної маси», і вже не веб-сайти будуть представляти ті чи інші бюрократичні структури, а навпаки, організаційні структури будуть відображати існування в Інтернеті державної служби, орієнтованої на потреби громадян.

Така інформатизація призведе до корінного переосмислення ролі і структури державних органів. Громадяни опиняться «за кермом», а послуги й інформація для населення будуть надаватися тоді, там і таким чином, як цього захочуть люди. Громадяни зможуть персоналізувати доступ до порталів державних служб, а також користуватися не тільки послугами держави, а й послугами своїх улюблених комерційних веб-сайтів і промислових порталів. Завдяки легкості взаємодії з державними службами і доступу до публічної інформації, офіційних документів і рішень адміністративних органів люди будуть краще поінформовані і з більшим бажанням братимуть участь у процесі вирішення державних справ. Це зумовить виникнення інформаційних суспільств і становлення таких моделей урядування (правління), де громадяни ширше залучатимуться до процесу прийняття рішень⁷⁶.

О.А. Баранов виділяє такі наслідки впровадження електронного урядування:

- відкритість та прозорість діяльності урядів;
 - значне підвищення якості надання адміністративних послуг;
 - забезпечення доступу громадян до інформації державних органів за допомогою сучасних інформаційних технологій;
 - економія часових та матеріальних ресурсів урядів, громадян, бізнесу;
 - звільнення державних службовців від рутинної роботи;
 - деперсоніфікація взаємовідносин громадян, представників бізнесу у взаєминах з державними чиновниками;
 - створення єдиного «пункту контакту» громадян з державними структурами;
 - можливість цілодобового отримання адміністративних послуг;
 - підвищення рівня демократизації суспільства⁷⁷.
- Отож, автоматизація органів влади має очевидні перспективи для громадян, бізнесу та державних органів.

⁷⁶ Внедрение концепции «электронного правительства». Стратегия по автоматизации государственных служб, предлагаемая корпорацией Microsoft http://www.microsoft.com/pus/government/whitepapers/eGov_Strategy.asp#7.

⁷⁷ Баранов О. Електронний уряд в Україні: переломові та наслідки // Доповідь у рамках конференції «Електронний уряд та електронна демократія». 12. 04. 2002.

Перспективи для громадян

Громадяни все більшою мірою очікують від державних органів, що вони будуть діяти подібно до комерційних організацій. Громадянина не цікавить, які службовці або яка посадова особа відповідає за ту чи іншу державну програму чи вид адміністративних послуг для населення. Для того щоб надавати населенню персоналізоване обслуговування, державні служби повинні забезпечити можливість доступу до всієї інформації і всіх послуг через одне інтегроване джерело. За допомогою веб-порталів та електронних магазинів, через які люди отримують доступ до Інтернету, можна створити єдиний інтерфейс для всіх державних організацій, приховавши їх складну внутрішню структуру.

Крім того, єдина точка доступу дозволяє громадянам краще виразити своє ставлення до того, що вони очікують від державних органів, і що їм потрібно. Завдяки цьому люди зможуть більш активно брати участь у місцевому житті і політичних процесах, оскільки вони зможуть взаємодіяти з органами влади і отримувати доступ до публічної інформації, офіційних документів тощо.

Перспективи для бізнесу

Взаємодія з державними органами через Інтернет ще більше підвищує конкурентоспроможність приватних компаній і дає їм можливість просунути різні офіційні процедури, зменшити кількість канцелярської тяганини. Компаніям стає «легше» дотримуватися законів, і вони можуть швидше розпочати свою діяльність. Усе це досягається завдяки подані документів в електронному вигляді.

Перспективи для державних органів

Державні органи здатні змінити на краще думку населення про якість адміністративних послуг і підвищити довіру громадян, зробивши їх центром уваги будь-яких ініціатив при здійсненні своєї діяльності. Організації, орієнтовані на потреби громадян, усвідомлюють, що весь процес надання послуг населенню рідко здійснюється однією людиною. Тому вони об'єднують систему управління відносинами з клієнтами (Customer Relationship Management, CRM), документообіг в інтернет-технології, перетворюючи державних службовців на працівників, «які керують знаннями». Співпрацівники повинні вміти використовувати програмні засоби управління справами (case management tools), володіти будь-якою ситуацією, що виникла, і знати відповідні закони і норми; крім того, вони повинні бути затягнутими вирішувати проблемні ситуації і приймати рішення. Для цього необхідна можливість сумісного доступу службовців до файлів на їхніх електронних «робочих столах», одночасність у роботі з людьми, скорочення часу відповіді на звернення і зниження тягара адміністративної роботи⁷⁸.

⁷⁸ Внедрение концепции «электронного правительства» // http://www.microsoft.com/pus/government/whitepapers/eGov_Strategy.asp#2.

2. СВІТОВА ПРАКТИКА ЗАПРОВАДЖЕННЯ ТА ФУНКЦІОНУВАННЯ СИСТЕМИ ЕЛЕКТРОННОГО УРЯДУВАННЯ

Реалізація ідеї електронного урядування викликає величезний інтерес у всьому світі. США, Великобританія, Швеція, Данія, Норвегія, а також Коста-Ріка, Катар, Об'єднані Арабські Емірати, Латвія, Естонія, Чехія та багато інших країн уже застосовують або починають застосовувати методи електронного урядування. Зокрема, уряд США надає громадянам різноманітні послуги через Інтернет: видачу ліцензій, сплату штрафів тощо. В Англії реєстрація фірм потребує заповнення через мережу тільки однієї форми.

На Заході використання Інтернету органами влади розглядається зараз як одна з можливостей підвищити їхню ефективність, ось чому до популярних в Інтернеті позначень «В» і «С», що означає, відповідно, «бізнес» і «споживач» і давно використовуються у всіхких сполученнях (В2В: business to business — бізнес до бізнесу, В2С: business to consumer, сітізен — бізнес до споживача, громадянина), тепер додалося нове — «С» — «уряд». Як і раніше, у випадку з В2В і В2С, зараз багато хто очікує, що впровадження у державне управління інформаційних технологій дозволить швидко все оптимізувати: знизити витрати на утримання держави, прискорити взаємодію органів державної влади між собою і з громадянами. Один із найтоварніших аргументів на користь електронного урядування, що наводять його прихильники, — підвищення прозорості влади за рахунок переходу на новий рівень зв'язку (зворотного) як із громадянами, так і з бізнесом. По суті ж, йдеться про зміну парадигми державної влади. Світовий досвід свідчить про те, що модель електронного урядування природна і приваблива для тих країн і культур, у яких держава сприймається як обслуговуюча, сервісна структура.

Запровадження електронного урядування в провідних країнах відбувається під гаслом відкритості і підзвітності урядів громадянам. Підзвітність, у свою чергу, зводиться не лише до надання громадянам інформації електронним шляхом, а забезпечується можливістю відкритої оцінки роботи конкретних державних установ і розробкою доступних насценню засобів моніторингу показників їхньої роботи.

Позитивні приклади запровадження та функціонування електронних урядів в інших країнах, що подаються нижче, допоможуть зорієнтуватися у реальних перевагах цієї системи.

За даними експертів, найкраще налагоджена он-лайн робота по-даткових і поштової служб. З усіх досліджених країн лише Фінляндія та Сінгапур пропонують своїм громадянам послуги через мобільний зв'язок. Наприклад, Верховний суд Сінгапуру посилав громадянам SMS, щоб нагадати дату засідання. Крім того, ті громадяни Сінгапуру, котрі авторизовані на сайті, можуть електронним способом подавати до суду позови у незначних справах. Незабаром ця послуга буде доступна всім жителям країни.

Нижче подається аналіз практики запровадження та функціонування системи електронного урядування у деяких зарубіжних країнах⁷⁹.

США

Аналіз загальної стратегії уряду США у сфері інформаційно-комунікаційних технологій (ІКТ) дозволяє стверджувати, що уряд:

- зацікавлений у забезпеченні зручностей для громадян у відносинах з державними органами;
- бере на себе роль лідера в електронізації економіки, у тому числі в стимулюванні розвитку електронної комерції;
- реорганізовує свою роботу в межах національної ініціативи щодо зміннення контролю за своєю діяльністю з боку громадян.

У даний час федеральний уряд США приділяє особливу увагу:

- електронній торгівлі між державними організаціями та міністерствами, конкурентним електронним торгам на поставання товарів і надання послуг для задоволення державних потреб;
- доступу населення до урядової інформації;
- використанню смарт-карт, у тому числі у федеральному уряді;
- вирішенню різноманітних завдань, зокрема публікації офіційних документів на урядових веб-сайтах, електронізації сплати податків, надання статистичної інформації про роботу державних органів населенню;
- застосуванню ІКТ в медицині і сфері охорони здоров'я.

Доступність посадовців федерального уряду президента США для населення і країни забезпечується за допомогою системи Comlink, що розроблена в Массачусетському інституті технологій (MIT). Ця система сприяє наданню послуг, дозволяє публікувати урядові документи і відкрити для доступу всім користувачам Інтернету. Матеріали брифінгів, тексти висупів, звіти, проекти законів, що надаються канцелярією Білого дому розміщуються на сервері розповсюдження електронної інформації системи Comlink. За оцінками оглядачів, більш як мільйон користувачів щоденно отримують документи, що їх цікавлять.

Друга система — Open Meeting — була створена в рамках обговорення національної ініціативи підвищення підконтрольності уряду громадянам (ППУ). Вона дозволяє подавати пропозиції та одержувати відгуки на них в інтерактивному режимі електронною поштою. Однією з головних цілей створення цієї системи — спрощення процедури опитування та одержання пропозицій з різноманітних джерел. За наявними даними, системою Open Meeting скористалося понад 3 тисячі осіб, які подали близько 1200 пропозицій. Інформація для обговорення була структурована тематично, і, таким чином, кожен учасник обговорення ініціативи ППУ міг вибрати

⁷⁹ Бюрократія он-лайн // <http://www.esommerce.ru/digests/russian/issue91/press2063.html>.

ту чи іншу тему. Система передбачала виключно вільний обмін думками, без дебатів і прийняття кінцевих рішень.

Ці системи сприяли підвищенню доступності державних органів для населення країни і забезпечили громадян більш ефективними засобами доступу до державних документів. Водночас федеральні службовці отримали інформацію про настрій виборців⁸⁰.

Державні послуги у США для населення надаються сьогодні багатьма шляхами: через торгові точки, банки і відділення зв'язку. Державні установи укладають з компаніями угоди з надання послуг. Так, наприклад, громадяни і приватні компанії отримали можливість оплачувати рахунки і сплачувати податки через свій місцевий банк. Мережу державних послуг, що діє у реальному світі, слід розвивати і у віртуальному вимірі. Особа, котра здійснює банківські операції через мережу Інтернет, повинна мати можливість оплачувати рахунки і сплачувати податки через свій банк.

Електронна Європа

«Електронна Європа» — ініціатива Європейської комісії, виконавчого органу Євросоюзу, спрямована на прискорення трансформації європейського промислового суспільства в інформаційне. Європейці зацікавлені в покращенні та полегшенні доступу громадян до інформації держорганів, що забезпечує більшу прозорість діяльності органів державної влади, а також гарантуватиме більшу ефективність прийнятих Євросоюзом рішень. Необхідно здійснити великий обсяг роботи, для того щоб забезпечити громадянам доступ до веб-сайтів урядів окремих держав і європейських інституцій, забезпечивши їм зручні засоби для пошуку необхідної інформації.

Обмеження доступу до основних статистичних і економічних даних гальмує розвиток бізнесу загалом, а також приватного сектора вторинних послуг, що спрямовані на інформування суспільства зокрема. Тому необхідно полегшити одержання державної інформації, що, у свою чергу, стимулюватиме розвиток нових секторів послуг, які базуються на відкритих джерелах інформації.

Потенційний ефект після вирішення цього завдання важко переоцінити:

- уряди стануть ближчими до простих громадян;
- з'явиться можливість скоротити видатки на утримання урядових службовців;
- будуть створені додаткові робочі місця для тих, хто надає вторинні послуги;
- буде створено загальноєвропейський інформаційний ринок державної інформації⁸¹.

⁸⁰ Дрожжников В., Штрик А. Электронное правительство информационного общества // *РCWeek/Russian Edition www.rcweek.ru/year2000/n15/cr1251/strategy/index.htm*.
⁸¹ Дрожжников В., Штрик А. Нынешнее поколение европейцев будет жить в информационном обществе // *РCWeek/Russian Edition: http://www.rcweek.ru/Year2000/n13/cr1251/Strategy/chart2.htm*.

Великобританія

Впровадження електронного урядування у Великобританії ґрунтується на положеннях Білої книги «Модернізації уряду» (Modernising Government White Paper) й оформлене у «Стратегічну концепцію обслуговування суспільства в інформаційну добу» («E-citizen, e-business, e-government. A strategic framework for ruble service in the Information Age»). Основна мета концепції полягає в конкретизації процесу переходу до уряду інформаційної доби.

У програму включені такі питання:

- структура і перелік послуг, які необхідно запровадити для звичайних користувачів та урядових організацій;
- розширення спектра послуг, які надаються органами влади;
- забезпечення максимального охоплення населення урядовими послугами;
- покращення ефективності користування інформацією;
- визначення конкретних заходів щодо реалізації всіх змін, необхідних для впровадження концепції.

Досвід показує, що громадяни при взаємодії з урядом переслідують певні власні інтереси і при цьому бажають, щоб наданий їм сервіс був високоякісним, а способи його надання — доступними і зручними. Населення, як правило, не цікавить організаційна структура уряду, які функції має та чи інша державна установа, як ці функції розподілені між ними та між центральними і місцевими органами влади. Тому необхідно сформувати стратегічний план партнерства державних структур різних рівнів щодо надання адміністративних послуг найбільш розумними і раціональними способами для споживачів, ґрунтуючись на реаліях навколишнього середовища та нових способах здійснення комерції.

Урядова стратегія передбачає розвиток і використання всіх електронних видів надання послуг. Це означає, що послуги можуть надаватися через Інтернет, мобільний зв'язок, цифрове телебачення, спеціальні центри. Водночас електронний сервіс не виключає можливості особистого контакту. Певну стурбованість викликає проблема задоволення специфічних та індивідуальних потреб людей, а тому і передбачається створення бізнес-порталів для малих та середніх підприємств та особистих домашніх веб-сторінок для окремих громадян.

Цікаво розглянути чотири рівні «електронної» взаємодії, що виділяються у країнах західної демократії на прикладі Великобританії: державних установ з громадянами, громадян з бізнесом, державних установ з посадовцями та державних установ між собою. Ці рівні наведені у таблиці і позначені вже згаданими вище аббревіатурами: G2C, C2B, G2B, G2G.

Нові способи комерції змінюють відносини між громадянами та урядом. Оскільки доступ до інформації гарантується Законом про свободу інформації, всі урядові організації повинні відповідально ставитися до за-

Вид взаємодії	Опис заходів
Взаємодія державних установ з громадянами (G2C): Оподаткування, інформування, охорона здоров'я, освіта	Збільшення шляхів взаємодії, зручності, зниження вартості послуг, підвищення персональної спрямованості послуг, підвищення рівня інформованості населення про спектр послуг та політику державних органів, підвищення рівня демократії та відкритості суспільства
Взаємодія громадян з бізнесом (C2B): Підтримка програм розвитку, регулювання, оподаткування	Прискорення взаємодії, зменшення вартості послуг, спрощення управління.
Взаємодія державних установ з поставальниками (G2B): Електронні послуги	Зниження вартості послуг, покращення управління ресурсами
Взаємодія державних установ між собою (G2G): Зв'язки між міністерствами та агентствами, центральною та місцевою владою, а також між окремими політиками.	Підвищення достовірності даних та ефективності їх використання, зменшення вартості послуг, покращення використання баз даних, удосконалення системи державного управління

питів споживачів. Водночас важливо гарантувати захист персональних даних та комерційної інформації. Особливе місце займає тут питання взаємодії уряду з громадянами, оскільки зменшення вартості зв'язку створює підрунтя для зміни життєвих умов більшості населення. Для того щоб послуги, надані на базі сучасних технологій, відповідали висунутим вимогам, необхідно:

- забезпечити доступ до послуг саме там, де виникає найбільша потреба в них;
- використовувати широкий спектр засобів взаємозв'язку, включаючи дзвінки від громадян та мережу Інтернет;
- сегментувати ринок з урахуванням специфічних потреб різноманітних груп населення;

- забезпечити зворотний зв'язок щодо змісту і якості наданих послуг;
- організувати різносторонній аналіз інформації за різними моделями використання послуг;

залучити користувачів до процесу удосконалення та модернізації послуг.

Водночас трансформація традиційних форм взаємодії уряду і громадян у цифровій формі не повинна породжувати соціальну нерівність. У зв'язку з цим уряд зобов'язаний сприяти зменшенню цифрового розшарування суспільства. Для цього ведеться цілеспрямована політика у сфері підвищення комп'ютерної грамотності, створення навчальних центрів і покращення умов для підвищення кваліфікації персоналу у сфері інформаційних технологій, у тому числі через забезпечення доступу до національної освітньої мережі та мережевої бібліотеки Великобританії. Подолання цифрового бар'єру передбачає не лише підвищення комп'ютерної кваліфікації та забезпечення доступу до інформаційних ресурсів. Окремі громадяни не бажають або ж не мають можливості стати безпосередніми користувачами нових технологій. Але дана стратегія враховує і цю категорію громадян.

Прем'єр-міністр Великобританії вважає, що модернізований, ефективний уряд зобов'язаний підтримувати новітні досягнення та розробки в електронному бізнесі. Розглянуті вище стратегічні принципи спрямовані на реалізацію цих намірів шляхом реструктуризації комерційної діяльності уряду та впровадження нових технологій.

Основні положення стратегії уряду Великобританії спрямовані на сприяння інноваціям у сфері надання послуг громадянам. Однак єдина модель розвитку електронної комерції в органах влади поки що не створена. Окремі моделі розроблені лише для певних міністерств і агентств відповідно до їхніх функцій та кола споживачів. Аналізуючи ці моделі, можна виділити у них такі основні елементи:

- забезпечення інновацій за рахунок надання нових видів послуг; одночасний розвиток номенклатури послуг і поліпшення обміну інформацією між громадянами;

- обмін між громадянами та організаціями досвідом ведення комерційної діяльності з державними органами;
- забезпечення однотипного взаємозв'язку з користувачами послуг; наявність ефективної структури і механізмів успішного впровадження проєктів⁸².

Можливість прямого доступу громадян до урядових документів передбачена в офіційному документі «Модернізація уряду», у якому йдеться про «забезпечення надання послуг населенню 24 години на добу, 7 днів на тиждень». У країні вже розроблено програма «Прямий доступ» (Direct Access)⁸³, що дозволить усім державним установам надавати громадянам у зручний для них

⁸² Прожжиков В., Штрик А. Электронное правительство информационного общества // PCWeek/Russian Edition www.pcweek.ru/year2000/n15/cr1251/strategy/index.htm/.

⁸³ Direct Access Government www.dag-business.gov.uk.

час електронний доступ до всіх форм документів. Кількість таких форм перевищує 100 тисяч.

На першому етапі проекту громадяни роздруковуватимуть форми, заповнюватимуть і надсилатимуть у державні органи звичайною поштою. На другому етапі, коли буде належним чином відпрацьована технологія електронних підписів, форми будуть заповнюватися на комп'ютерах і надсилатися електронними каналами зв'язку.

Проект Direct Access допомагає скоротити потоки паперових документів і знизити витрати. Переваги Direct Access активно використовуються центральними і місцевими органами влади на всій території Великобританії⁸⁴.

Ірландія

Система електронного уряду спрямована на те, щоб покращити взаємодію між урядом і комерційними компаніями і забезпечити об'єднаний портал доступу бізнесу до уряду. Система розроблена під контролем Міністерства підприємств, торівлі та зайнятості і сприяє координації роботи різних урядових структур. Он-лайнova податкова служба дозволяє підприємствам одержувати інформацію про оподатковування, сплачувати податки, заповнивши відповідні електронні форми, а також одержувати податкові кредити.

Сайт Земельної служби надає компаніям інформацію про нерухомість і дає можливість здійснювати будь-які операції, пов'язані із землею і нерухомістю. Сайт Федерального агентства зайнятості містить інформацію про ринок робочої сили для роботодавців і працівників. Сайт Реєстраційної палати дає можливість:

- зареєструвати компанію будь-якої організаційно-правової форми;
- зареєструвати найменування компанії;
- внести зміни в статутні документи;
- оформити фінансові документи;
- легалізувати іноземні документи.

Уряд вважає, що необхідно прискорити розвиток системи електронно-го уряду й особливо деяких проектів, включаючи:

- створення загальнодоступних баз даних про найбільш значимі події громадянського життя та діяльність ірландських підприємств;
- розробку інформаційних проектів урядових закладів.

Електронний спосіб взаємодії з урядом дозволить знизити витрати і ефективно перерозподіляти ресурси⁸⁵.

Німеччина

Німеччина є однією з провідних країн у галузі розвитку Інтернету. Висока швидкість розвитку інформаційних технологій змушує державні органи вчитися використовувати їх для підвищення ефективності роботи і бути готови-

ми до швидких змін. З цією метою Німеччина приступила до реалізації програми BuidOnline 2005 («Німеччина в Мережі»), що спрямована на забезпечення надання всього спектра державних послуг через Інтернет до 2005 року. Внаслідок цього громадяни одержать доступ до 1,2 тис. он-лайнних послуг державних установ. Зокрема, у жителів країни з'явиться можливість заповнити податкову декларацію, продовжити дію водійського посвідчення або паспорту тощо через мережу Інтернет. У рамках програми також передбачається обладнати 181 відділення Національної служби зайнятості пунктами безкоштовного доступу в Інтернет для безробітних, які зможуть скористатися ними для надсилання своїх резюме і пошуку вакансій.

Деякі послуги вже надаються, у тому числі заповнення електронних заявок у Федеральному адміністративному відомстві, менеджмент службових поїздок федеральних працівників, а також управління інформацією у Федеральному міністерстві внутрішніх справ. Крім того, через мережу Інтернет приймаються прохання від студентів про надання їм фінансової допомоги. В усіх випадках відомості надходять у систему й автоматично направляються на сервер обробки даних документообігу. Після закінчення процесу обробки електронна форма з інформацією направляється назад користувачеві. Ці рішення були реалізовані шляхом впровадження новітніх інтернет-технологій в програми управління документообігом. Створені програми безкоштовно передаються в усі державні установи Німеччини. Серед переваг програми «BuidOnline 2005» варто виділити підвищення зручності роботи для громадян і більш раціональне використання управлінських ресурсів.

Донедавна менеджмент службових поїздок здійснювався в уряді Німеччини децентралізованим способом, що призвело до непотрібного дублювання і витрат ресурсів. Тому недавно було прийняте рішення, що приносить велику економію. Основним компонентом цього рішення стало призначення менеджера з питань організації поїздок. Використовуючи транспортну базу даних, менеджер домовляється з провайдерами послуг з метою вибору найкращого варіанту в конкретному випадку. Із впровадженням цієї системи купівельна спроможність федерального уряду зростає, схеми поїздок були переглянуті, а самі користувачі тепер набагато краще орієнтуються в наданих їм послугах. Впровадження служби планування поїздок зумовило 15-відсоткову економію всіх транспортних витрат і 50-відсоткову економію адміністративних витрат. Окрім цього, на регіональному і місцевому рівнях відбувається додаткова економія витрат.

Ще одним проектом, реалізованим у рамках впровадження електронного уряду, стало перетворення землі Шлезвіг-Гольштейн у «електронний регіон» (e-region) шляхом організації надійної інфраструктури, що дозволяє здійснювати швидкий і ефективний обмін інформацією. Цей проект спрямований на створення «державної універсальної установи», що забезпечить доступ до будь-яких послуг з будь-якого місця на території регіону⁸⁶.

⁸⁴ Direct Access Government www.dag-business.gov.uk.

⁸⁵ BASIS (доступ предпринятий к правительственной информации) <http://www.bizz.pl/egov/articale.php?id=45>.

Швеція

Уряд Швеції оцінив можливі наслідки переходу на електронну систему закупівель, і з'ясувалось, що це може дати 50-відсоткову економію коштів на проведенні операцій між контрагентами. Крім того, оцінка вказувала на підвищення якості пропонованих продуктів і послуг. Упевненість уряду у високій ефективності електронної торгівлі була настільки висока, що вже до кінця 1999 року шведські державні установи проводили електронним способом до 95 відсотків своїх закупівель.

Інформаційні програми обслуговують 125 тисяч користувачів, у тому числі поставальників продуктів і послуг працівників центральних і місцевих органів влади. Користувач цієї системи одержує доступ до баз даних, у яких зберігається інформація про контракти, ціни тощо. Ознайомившись з цією інформацією, можна скласти замовлення відповідно до фінансових вимог окремої установи. Система має також автоматичну процедуру узагодження рішень про закупівлі з керівництвом. Після схвалення начальника, замовлення електронними каналами зв'язу відправляється відповідному поставальникові⁸⁷.

Естонія

Уряд Естонії в рамках реалізації концепції «електронного урядування» створив та ввів у дію в червні 2001 року інтернет-портал «Сьогодні вирішувати» (Täna otsustan mina), за допомогою якого будь-який житель республіки може взяти участь в управлінні державою — висловити свою думку про поточні проєкти у країні, запропонувати поправки до законопроєктів тощо. Протягом останніх декількох років у країні успішно функціонує єдина комп'ютерна база даних та інтернет-портал, що забезпечують більш ефективну взаємодію між державними установами та громадянами Естонії.

Коментуючи новий пілотний проєкт, газета «Eesti Raevaleht» пише, що портал «Сьогодні вирішувати» дозволяє користувачеві висловлювати свою думку про поточні події у країні, вносити поправки до законопроєктів, а також голосувати. Якщо ідея поправки чи іншої пропозиції містить раціональне зерно і підтримується іншими інтернет-користувачами, естонський прем'єр-міністр відсилає цю пропозицію зі своєю резолюцією у відповідне міністерство.

Для користування порталом «Сьогодні вирішувати» необхідно пройти процедуру реєстрації, для того, щоб одна людина не мала можливості голосувати кілька разів. Однак ці дії уряду зазнають серйозної критики з боку опозиційних сил Естонії. Основний аргумент опозиціонерів полягає

в тому, що правлячі праволіберальні партії прагнуть заручитися додатковою підтримкою молодих громадян і серйозно утискати права традиційно активних літніх виборців, що не мають вдома комп'ютерів і не володіють навичками роботи з Інтернетом⁸⁸.

Швейцарія

Частиною програми швейцарського уряду у сфері розвитку інтернет-послуг (до 2005 року) є повний переклад перепису населення з паперової форми на електронну основу. Для успіху цього починання необхідне не тільки бездоганне володіння інформаційними технологіями, але й вирішення проблеми інформаційної нерівності в країні.

У Швейцарії проживає 7,2 млн осіб, які розмовляють чотирма національними мовами. З них 2 млн жителів регулярно користуються Інтернетом. У країні діють відмінні лінії зв'язку і телекомунікаційна інфраструктура, а органи влади активно просувають програми «електронного урядування». Очевидно, що глибокі зміни в інформаційних технологіях докорінно вплинули на роботу державних службовців, відкривши нові шляхи для збору й обробки даних.

Перепис населення проводиться у Швейцарії з 1850 р., і це не єдина країна, що почала переходити від паперових методів до електронних форм. Світовими першопрохідниками в цій галузі є, крім Швейцарії, США і Сінгапур. Мета таких проєктів — знизити витрати, зменшити час збору даних, прискорити обробку і підвищити цінність зібраних відомостей. Тому в ході проведення електронного перепису в Швейцарії людині не потрібно надавати інформацію, що вже зберігається в одній з державних служб. Загальна ідея проєкту полягає в новому підході до збору даних в інформаційному суспільстві.

У 2000 р. уряд запропонував громадянам Швейцарії вибір між традиційним паперовим і електронним методами перепису населення. Відомості, передані користувачами через мережу, кодувалися і зберігалися в центральній базі даних. Система була захищена, а громадяни могли скористатися телефонною підтримкою для надання інформації. Робота на веб-вузлі була досить проста: людина знаходила своє ім'я і вносила необхідні дані.

Важливим фактором, що сприяє успішній реалізації проєкту, стало співробітництво Статистичного управління з ІТ-компаніями, особливо з Microsoft, який став спонсором проєкту із самого початку проведення робіт. Систему не вдалося б реалізувати без підтримки партнерів. Інші фактори успіху — зручний інтерфейс веб-вузла, можливість вибору мови для користування, гнучкість і розширюваність системи, а також швидкість, з якою вона була розроблена.

⁸⁶ Перспективи розвитку «електронного правительства» в Германії // http://www.microsoft.com/press/government/pressletters/issue10/issue10_8.asp.

⁸⁷ Информационные решения для e-закупок в Швеции <http://www.biz.pl/egov/article.php?id=12>.

⁸⁸ Эстонское правительство станет ближе к виртуальному народу // Информационное агентство «Росбалт», 19 июня 2001 г. // <http://www.gosbalt.ru/index.php?cn=12178>.

Проект був дуже добре сприйнятий жителями Швейцарії: 300 тис. громадян заповнили форми перепису через Інтернет, а в роботі веб-вузла не було відзначено ніяких проблем з безпекою. Зібрані дані відрізнялися високою якістю. Типовим користувачем он-лайнної служби був громадянин з вищою освітою, що живе в невеликому містечку, яке налічує від 5 до 20 тис. жителів. Кошти, вкладені в систему, повернулися після першого ж її використання.

Хоча проект продемонстрував великі перспективи електронного перепису населення, необхідно вирішити серйозні питання, перш ніж у ньому зможе взяти участь усе населення країни. Найважливіша проблема в цьому напрямку — інформаційна нерівність серед населення. Рівень участі чітко свідчить про те, що Статистичному управлінню ще далеко до задушення всього населення. Людям усе ще бракує стимулів для використання Інтернету в подібній справі — вони звикли заповнювати форму перепису на папері. Частково причиною цього є недостатня довіра до збереження конфіденційності інформації. І поки ці питання не будуть вирішені, Статистичному управлінню доведеться використовувати обидва методи збору даних.

Надалі управління планує організувати поширення даних перепису через мережу Інтернет, створити інші електронні державні служби, наприклад для голосування і заповнення податкових декларацій, а також он-лайн нову систему збору даних для приватних компаній і державних органів. Очікується, що в ході перепису населення в 2010 р. при зборі даних будуть використовуватися електронні реєстри, он-лайнні форми і телефонні інтерв'ю.

Обробка даних електронного перепису населення у Швейцарії скоротилася на рік. Перепис населення у Швейцарії в 2000 році став європейською прем'єрою: уперше громадяни країни одержали можливість відповісти на запитання як на папері, так і через Інтернет.

Швейцарці реєструвалися на сайті електронного перепису www.e-sensus.ch, вводячи своє ім'я і пароль, після чого одержували форму з уже частково заповненими персональними даними. У їхньому розпорядженні була пояснювальна інформація, он-лайнна довідка і приклади відповідей на запитання.

Система електронного перепису адаптувала запитання, що ставляться, на підставі відповідей, даних на попередні запитання, а також перевіряла вірогідність і повноту інформації, що вводиться. Вона пропонує каля за питання, що не ставляться до даного жителя. Користувач же міг у будь-який момент перервати роботу із системою і повернутися до неї пізніше, причому вся раніше введена інформація автоматично зберігалася⁸⁹.

Сінгапур

З 1980 року Сінгапур приділяє інформаційним технологіям особливу увагу. Мета урядового плану — перетворити Сінгапур на «інтелектуальний острів», де державне управління, бізнес, освіта, наукові дослідження, дозвілля й інші сфери життєдіяльності взаємодіють на основі інформаційних технологій. На це виділяється щорічно більш як 400 млн дол. Комп'ютерна техніка широко використовується у сфері освіти: від дитячих садків до університетів. Сінгапур займає перше місце у світі за ступенем обладнання шкіл сучасними комп'ютерами і програмами: на сімох учнів початкових шкіл припадає один ПК, у середніх школах ця пропорція становить 5:1.

Ключова частина сінгапурської інформаційної стратегії — перша у світі державна інтерактивна мультимедійна мережа «Сінгапур-один». Вона дозволяє ефективно працювати в «інтелектуальному середовищі»: робити покупки, здійснювати банківські операції, знайомитися з новинами, розважатися. На 2002 рік «Сінгапур-один» мала 60 тис. користувачів. До кінця 2001 року ними стало 50 % сімей країни. Послугами Інтернету вже користується кожен шостий її житель.

Розроблена Національною радою комп'ютеризації система обслуговування громадян e-citizen, назва якої може розшифровуватися не тільки як «електронний громадянин», але і як «кожен громадянин» (every citizen), об'єднує всі електронні операції. Для організації портал надає доступ до електронних форм податкових та інших платежів, а також до системи електронних державних закупівель. Тут можна зареєструвати товарний знак або патент, одержати інформацію про різні урядові програми підтримки і розвитку бізнесу, про пільгові схеми кредитування, консалтинг і навчання, особливо ті, що стосуються малих і середніх підприємств.

Підхід Сінгапuru унікальний тим, що уряд країни ніколи не випустить з уваги питання, пов'язані з реалізацією концепції «електронного урядування». Так, наприклад, коли три роки тому Служба інформаційних технологій Міністерства оборони ввела в дію першу у світі інтернет-систему урядових закупівель, незабаром після цього Міністерство фінансів і Національна рада з питань обчислювальної техніки почали задумуватися над поширенням цієї системи на інші державні служби.

Електронні мережі Сінгапuru включають торговельну TradeNet (проходження по ній документів займає всього 3 хвилини), морську MarineNet, портову PortNet і електронну систему обліку судових документів Electronic Filing System⁹⁰.

⁸⁹ Перепис населення в Швейцарії // <http://www.iberiz.tu/egov/artiscale.rhtml?id=66>.

⁹⁰ «Сінгапур: єдиний портал електронного обслуговування громадян», eGovernment — технології и решения для электронного правительства // www.e-government.tu/article.rhtml?id=46.

Канада

Завдяки бурхливому росту інформаційних технологій і їхньому широкому розповсюдженню можна з впевненістю сказати, що сьогодні світ переживає нову революцію. Щодня понад 150 тис. нових користувачів уперше підключаються до мережі Інтернет. Суспільство пройшло довгий шлях: від загальних телефонних ліній для декількох абонентів до нинішнього рівня розвитку техніки, коли по одному кабелю може передаватися 15 млн розмов одночасно.

Єдиною альтернативою розвитку є перехід до нових технологій і створення на їхній основі процвітаючого співтовариства. Державні органи є однією з рушійних сил цього процесу.

Наприклад, уряд провінції Нью-Брансвік запровадив знижки на придбання комп'ютерів, і протягом двох років — термін дії цих знижок — комп'ютерні магазини повністю розпродали свій товар. У цій провінції було створено 230 комп'ютерних центрів, де можна освоїти навички роботи на комп'ютері, що служить важливим фактором подолання інформаційної нерівності. Кожен випускник середньої школи в цьому регіоні для одержання атестата повинен пред'явити свідоцтво про закінчення комп'ютерних курсів. Знижки на придбання комп'ютерів були впроваджені і в Квебеку, що спричинило те, що за рік кількість осіб, підключених до Інтернету, зросла на 13 %⁹¹.

Австралія

Органи влади штату Вікторія запровадили систему МАХІ, що стала лауреатом різних премій. МАХІ — єдиний вузол обслуговування населення, доступний не тільки з персональних комп'ютерів з Інтернет-доступом, але і через 50 веб-кіосків, а також по телефону 24 години на добу, 7 днів на тиждень, 365 днів у році. Система забезпечує проведення операцій між місцевим урядом і фізичними та юридичними особами.

Австралійське податкове управління (АПУ) ввело електронну форму податкових декларацій у 1999 році. Зараз 75 % усіх декларацій про прибутки надходять в електронному вигляді через портал податкового управління. Він об'єднаний калькуляторами, «розумними» банками, засобами зворотного зв'язку, звітами про роботу АПУ тощо.

Найближчим часом Податкове управління надасть компаніям на компакт-дисках програму «електронного обліку», що враховує потреби малих підприємств. Це допоможе їм в управлінні своїми фінансами й у бізнес-плануванні, полегшивши перехід на нову податкову систему.

Як тільки служба зайнятості прийняла рішення надавати якомога більше послуг через Мережу, вона мало не за одну ніч виявилася на 20-му

⁹¹ Канада: електронное взаимодействие правительства с бизнесом и гражданами // <http://www.ibiz.pl/egov/article.php?id=17>.

⁹² Интегрированные операции между гражданами и местными властями // <http://www.ibiz.pl/egov/article.php?id=15>.

місці щодо відвідуваності серед усіх веб-вузлів Австралії. В он-лайнівій службі зайнятості (www.jobsearch.gov.au) є могутня пошукова машина щодо вакансій, інформація про професії, аналізи і прогнози щодо ринку праці, відомості про навчання і дані про умови працевлаштування. Цей веб-вузол миттєво вплинув на всю промисловість країни: підприємства охоче реструктуризувалися на ньому, а сама служба перетворилася для них на головний засіб пошуку співробітників. Кілька місяців тому одна з найбільших австралійських газет запропонувала розмістити всі свої оголошення про працевлаштування на цьому веб-вузлі. Щорічна економія від роботи служби в мережі Інтернет становить майже 900 млн дол.⁹²

Південно-Африканська Республіка

Завдання, що стоять перед урядами країн, що розвиваються, у сфері подолання інформаційної нерівності, мають унікальний характер, причому їх успішне вирішення може позитивно позначитися на створенні інтегрованого суспільства і реалізації електронного уряду в рамках усієї країни.

Одна з існуючих проблем стосується інформаційного наповнення Інтернету і грамотності населення країн, що розвиваються. Одним з основних шляхів впровадження інформаційних технологій у країнах, що розвиваються, є якомога більш швидке об'єднання людей за допомогою «єдиного уряду». Ті держави, у яких цей процес ще не знайшов широкого застосування, мають навіть деяку перевагу, оскільки вони можуть просунутися у цьому плані вперед швидше, ніж країни з уже сформованою інфраструктурою. Інвестиції у створення нової інфраструктури найчастіше будуть меншими, аніж витрати на модернізацію вже наявного устаткування — у країнах, що розвиваються, найчастіше не існує ніякої бази для впровадження інформаційних технологій. Ступивши на шлях запровадження електронного урядування пізніше, ніж інші країни, ПАР одержала можливість уникнути помилок, зроблених першопрохідниками, і скористатися їхніми досягненнями.

У ПАР діє дві програми, спрямовані на подолання інформаційної нерівності: SIGTA і Millennium Africa Renaissance. Діяльність Південноафриканського агентства з інформаційних технологій SIGTA (State Information Technology Agency of South Africa) спрямована на активне впровадження інформаційних технологій в управлінні державою. Призначенням проекту Millennium Africa Renaissance («Африканське відродження на рубежі тисячоріч») є підтримання миру, безпеки і стабільності, а також впровадження демократичних форм правління. У цьому проекті сформульовані стратегії у сфері розвитку африканської промисловості і людських ресурсів, пропонується план інвестицій у сфері інформаційної технології, зв'язок,

⁹³ Электронная сеть — гарантия «прозрачных» и честных выборов в Южной Африке // <http://www.ibiz.pl/egov/article.php?id=27>.

транспортну й енергетичну інфраструктуру, а також описуються механізми фінансування.

З огляду на ті проблеми, які необхідно подолати країнам, що розвиваються, і ті можливості, що можуть бути для цього використані, Південно-Африканська Республіка розробила поетапний план створення електронного уряду. Перша стадія, «єдиний уряд», націлена на те, щоб у першу чергу поліпшити взаємодію державних відомств між собою. Реалізація другої стадії, «універсального доступу», дозволить будь-якій людині підключатися до державних служб через мережу Інтернет, не зустрічаючи ніяких мовних перешкод.

Сьогодні проект SIDA уже повністю реалізований. Крім того, введена в дію національна система ідентифікації особи користувача (iset ID) на основі смарт-карт і окремі елементи електронної судової системи. Основні складові успішного впровадження проєктів — прискорення обслуговування клієнтів, прийняття вартість, актуальність інформації, доступність і легкість у використанні.

Електронна мережа — гарантія «прозорих» і чесних виборів у Південній Африці. Загальнонаціональні вибори 2 червня 1999 року перенесли виборчий процес у ПАР в інформаційне століття. Для країни, де відсутня розвинена технологічна інфраструктура, а в сільській місцевості у деяких місцях немає навіть телефонного зв'язку, це грандіозне досягнення.

Для складання першого в країні виборчого списку застосовувалися спеціальні пристрої зчитування штрих-коду (на зразок контрольних сканерів, використовуваних у супермаркетах). У цілому було зареєстровано понад 18 млн виборців. Для збору й оприлюднення результатів голосування був створений «Виборчий центр», обладнаний 25 високошвидкісними серверами і з'єднаний з автоматизованим центром обробки телефонних дзвінків.

Система перевірки результатів працює з даними, що надходять з кожної з 14 500 виборчих дільниць, порівнюючи інформацію, отриману факсом, телефоном і через глобальну супутникову мережу. У періоди пікового навантаження число її користувачів може досягати 900 осіб⁹³.

Вибравши деякі позитивні приклади зі світового досвіду запровадження системи електронного урядування ми з упевненістю можемо констатувати її практичні переваги:

- 1) *для громадян* — одержувати послуги, надані державними установами через мережу; мати до них доступ через мережу Інтернет; навчатися протягом усього життя і брати участь в управлінні державою;
- 2) *для бізнесу* — мати доступ до державних служб в Інтернеті, співпрацювати з державою з метою сприяння економічному розвитку;
- 3) *для державних структур* — підвищити свою оперативність, ефективність роботи; покращити відносини з клієнтами і залучити всіх громадян до процесу прийняття державних рішень, зосередивши свою увагу на стратегічних напрямках.

Аналіз світової практики створення проєктів електронного урядування дозволяє виділити деякі принципові положення щодо їх функціонування:

- сфокусованість на реальних потребах громадян і бізнесу;
- використання сучасних методів і рішень;
- оптимізація процедур відносин держави, громадян і бізнесу, відпрацьовування механізмів «цифрової демократії»;
- висока якість послуг;
- облік специфіки потреб різних соціальних груп населення, компетентність на найбільш важливих темах суспільства;
- надання державних послуг через різні канали, включаючи цифрове телебачення, центри суспільного доступу;
- підтримка проєктів центральних і місцевих органів влади, здійснення координації і вироблення стандартів, що дозволяють створювати вертикально і горизонтально інтегровані державні мережеві ресурси;
- ефективне вирішення питань захисту мереж та інформації;
- реалізація механізмів, що забезпечують захист прав особистості;
- оптимізація структури державного апарату і всієї системи державного управління, навчання державних службовців нових форм роботи;
- удосконалення управлінської культури. Створення системи стимулів і мотивації;
- визначення реальних і доступних для громадян інформаційних показників ефективності функціонування державного апарату і державних служб.

У той час, коли банки, страхові компанії і підприємства розпрібної торгівлі швидко скорочують витрати, переходячи до використання можливостей Інтернету, державні органи все ще зіштовхуються з проблемою надмірних витрат. Дотепер вони працюють напроцуд повільно і неефективно, і ця проблема тією чи іншою мірою властива багатьом країнам. У цьому, як правило, немає провини окремих працівників, що дотримуються застарілих процедур і користуються лише найпримітивнішими технічними засобами. У державних органів є унікальна можливість згодом очолити інформаційне суспільство шляхом його нормативної, організаційної і фінансової підтримки. Проникнення інформаційних технологій та інтернет-технологій у структури влади одночасно підпадає під виконавчу оперативну діяльність, і саме тут необхідна найбільш тісна співпраця з органами влади.

3. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОННОГО УРЯДУВАННЯ

Законодавство України

На сьогодні в нашій державі існує досить велика кількість нормативно-правових актів, що регулюють відносини у сфері інформаційних технологій. Проте значна частина з них потребує внесення змін та доповнень, оскільки тією чи іншою мірою не узгоджується між собою. Як уже зазначалося, чинне законодавство України, у свою чергу, не відповідає сучасному рівню розвитку інформаційних відносин та не в змозі адекватно вирішувати проблеми, що виникають.

На думку фахівців телекомунікаційної сфери, розробка спеціальних законів «для Інтернету» — справа зайва і навіть шкідлива. Спеціального правового регулювання потребують тільки такі специфічні моменти, які зустрічаються лише в Інтернеті і відсутні у реальному житті. Тож законодавці повинні зосередити свою увагу на заповненні «правових прогалин», що гальмують розвиток мережі. Зокрема, йдеться про електронний підпис, поняття електронного контракту, статус ЗМІ в Інтернеті, про захист авторських прав тощо. До цього спонукає, зокрема, стрімкий розвиток банківського сектора та інтернет-послуг.

Шодо правового забезпечення відносин у сфері інформаційних технологій, зокрема системи електронного урядування, то на сьогодні немає жодного нормативно-правового акта, який би чітко і всебічно регулював дане питання.

Відомо, що існують два моделі європейські закони, що рекомендуються для прийняття всім країнам, що мають намір інтегруватися в європейський електронний простір. Це закон про електронну комерцію і закон про електронний цифровий підпис. Деякі країни приймають ці закони без змін, інші ж вносять у них корективи, що відображають різні національні особливості.

22 травня 2003 року Верховна Рада України прийняла два важливі закони у сфері організації і функціонування електронного документообігу — це Закон України «Про електронні документи і електронний документообіг» та Закон України «Про електронний цифровий підпис» (обидва закони набрали чинності з 1 січня 2004 року). Законами встановлюються основні організаційно-правові засади електронного документообігу, використання електронних документів, визначається правовий статус електронного цифрового підпису та регулюються відносини, що виникають при використанні електронного цифрового підпису. Мета законів полягає у наданні електронним документам юридичної сили рівної паперовим. При цьому електронний цифровий підпис є тим інструментом, що дозволяє створити правові основи для електронного документообігу (в тому числі в мережі Інтернет), укладати угоди та ін. У Законі «Про електронний цифровий підпис» вказується, що електронний цифровий підпис — це вид електронного підпису, отриманого у результаті криптографічного пе-

ретворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа (стаття 1 Закону).

Забезпечення зазначених властивостей цифрового підпису для електронних документів ґрунтується на використанні криптографічних алгоритмів, у яких обов'язково застосовуються два параметри (числа), які називають ключами. Один з них особистий, використовується при підписанні і доступний тільки підписувачу, а другий, який називають відкритим, — при перевірці цифрового підпису.

Одне з проблемних питань, що повинні вирішити прийняті закони, — це робота центрів сертифікації ключів, які мають надавати послуги цифрового підпису. Відповідно до частини першої статті 8 Закону «Про електронний цифровий підпис», центр сертифікації ключів — це юридична особа незалежно від форми власності або фізична особа, яка є суб'єктом підприємницької діяльності, що надає послуги електронного цифрового підпису та засвідчила свій відкритий ключ у центральному засвідчувальному органі або засвідчувальному центрі з дотриманням вимог статті 6 цього Закону («Вимогою до сертифікації ключа»). Спеціалісти вважають, що кількість бажаних займатися такою діяльністю, можливо, буде досить незначною. Зокрема, тому, що фінансовий бар'єр виходу на ринок таких структур за нинішніх умов буде досить високим з огляду на специфіку їхніх функцій (надання засобів цифрового підпису, формування, розповсюдження, скасування, блокування та поновлення сертифікації ключів, генерація відкритих та особистих ключів тощо). А враховуючи те, що все повинно починатися практично з нуля, оскільки майже таким на даному етапі є ринок користувачів, «повернення» зроблених вкладень буде досить довгим.

При розробці Закону «Про електронні документи та електронний документообіг» широко використовувалися рекомендації Центру ООН шодо спрощених процедур і методів в органах управління торгівлі та транспорту, а також типовий Закон Комісії ООН з міжнародного торгового права. За допомогою впровадження електронного цифрового підпису створюються правові основи для електронного документообігу (в тому числі в мережі Інтернет) з метою укладення угод, створення платіжних систем, впровадження електронних цінних паперів тощо. Впровадження електронного обміну даних дозволить спростити та прискорити документообіг між суб'єктами господарювання, що вплине на конкурентоспроможність вітчизняної економіки, а також прискорить оформлення експортно-імпорتنих операцій.

Загалом, обидва законопроекти розроблені на основі європейських модельних законів, але не ідентичні їм. Наскільки внесені в них корективи життєдатні й ефективні — покаже час.

31 липня 2000 року Президент України прийняв Указ «Про заходи шодо розвитку національної складової глобальної інформаційної мережі Інтер-

нет та забезпечення широкого доступу до цієї мережі в Україні». Цим Указом встановлено, що розвиток національної складової інформаційної мережі Інтернет, забезпечення широкого доступу до цієї мережі громадян та юридичних осіб усіх форм власності в Україні, належне представлення в ній національних інформаційних ресурсів є одним з пріоритетних напрямів державної політики у сфері інформатизації, задоволення конституційних прав громадян на інформацію, побудови відкритого демократичного суспільства, розвитку підприємництва. Відповідно до даного Указу основними завданнями є забезпечення підтримки розвитку інфраструктури надання інформаційних послуг через мережу Інтернет та розвиток і впровадження сучасних комп'ютерних інформаційних технологій у системі державного управління. Указ Президента також зобов'язав Кабінет Міністрів України забезпечити встановлення до кінця 2000 року порядку оприлюднення інформації про діяльність органів державної влади України та завершення створення веб-сторінок центральними органами виконавчої влади, Радою міністрів Автономної Республіки Крим, обласними, Київською та Севастопольською місцевими державними адміністраціями. Певні положення даного акта вже реалізовані, але ще не всі.

Серед інших нормативно-правових актів, які регулюють правовідносини у сфері інформатизації, а саме щодо питань електронного урядування, важливим документом є Постанова Кабінету Міністрів України «Про порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади» від 4 січня 2002 року за № 3. Відповідно до зазначеного Порядку оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади здійснюється з метою підвищення ефективності та прозорості діяльності цих органів шляхом впровадження та використання сучасних інформаційних технологій для надання інформаційних та інших послуг громадськості, забезпечення її впливу на процеси, що відбуваються у державі. Оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади здійснюється шляхом:

- розміщення і періодичного оновлення міністерствами, іншими центральними та місцевими органами виконавчої влади інформації відповідно до вимог цього Порядку на власних веб-сайтах;
- створення Єдиного веб-порталу Кабінету Міністрів України, призначеного для інтеграції веб-сайтів органів виконавчої влади та розміщення інформаційних ресурсів відповідно до потреб громадян.

Порядком також передбачено, яка інформація повинна бути розміщена на веб-сайті органу виконавчої влади (для міністерства, іншого центрального органу виконавчої влади, а також для Ради міністрів Автономної Республіки Крим, обласної, Київської та Севастопольської міської держадміністрації). До такої інформації, відповідно до Порядку, відносяться: найменування органу; основні завдання та нормативно-правові засади діяльності; структура та керівництво органу; основні функції структурних підрозділів; зразки документів та інших матеріалів, необхідних для звернення громадян до органу; місцезнаходження апарату (органу); розклад роботи органу та час прийому керівництва; відомості про наявні

вакансії; державні інформаційні ресурси з питань, що належать до компетенції органу та ін. У свою чергу, Порядком передбачено, що Рада міністрів Автономної республіки Крим, обласні, Київська та Севастопольська міські держадміністрації зобов'язані додатково розмішувати інформацію про районні, районні у містах Києві та Севастополі держадміністрації, а також інформацію про територію відповідної адміністративно-територіальної одиниці. Також вказується, що на веб-сайті може розмішуватися інша інформація, яку керівництво органу виконавчої влади вважає за доцільне оприлюднити.

На сьогодні значну кількість положень цієї Постанови вже реалізовано, а деякі продовжують виконуватися.

Кабінет Міністрів України 12 квітня 2002 року прийняв Постанову № 522 «Про затвердження Порядку підключення до глобальних мереж передачі даних». Серед іншого, Державний комітет зв'язку та інформатизації за погодженням з Державним комітетом з питань регуляторної політики та підприємництва, Антимонопольний комітет і Міністерство оборони згідно з постановою повинні затвердити Порядок складання та ведення переліку підприємств (операторів), що надають послуги з доступу до глобальних мереж передачі даних органам виконавчої влади, іншим державним органам, підприємствам, установам та організаціям, які одержують, обробляють, поширюють і зберігають інформацію, що є об'єктом державної власності та охороняється відповідно до законодавства. Він, згідно з постановою, має передавати вимоги до програмно-технічних засобів, які забезпечують доступ до глобальних мереж передачі даних, якості окремих видів послуг з доступу до них, захисту інформації в зазначених мережах. Урядове рішення прийнято на виконання Указу Президента України від 24 вересня 2001 року № 891 «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних».

Серед нормативно-правових актів, які стосуються проблематики запровадження в Україні системи електронного урядування, 24 лютого 2002 року було прийнято Постанову Кабінету Міністрів України «Про заходи щодо створення електронної інформаційної системи «Електронний уряд».

Відповідно до Постанови передбачається створити належні нормативно-правові засади функціонування системи «Електронний уряд», забезпечити умови для більш швидкого та доступного надання інформаційних послуг громадянам та юридичним особам шляхом використання електронної інформаційної системи «Електронний уряд», яка забезпечує взаємодію органів виконавчої влади між собою, з громадянами та юридичними особами на основі сучасних інформаційних технологій, інтегрувати державні електронні інформаційні ресурси і системи в Єдиний веб-портал органів виконавчої влади.

Прораналізувавши хід подій у галузі інформатизації в Україні, різноманітні документи та матеріали, можна зробити висновок, що у цьому напрямку здійснюються певні заходи. Можливо, не настільки інтенсивно, як в інших державах, але можна стверджувати, що через деякий час Україна також буде характеризуватися неабиякими здобутками у цій сфері.

Основні міжнародні документи та нормативно-правові акти зарубіжних країн у галузі інформаційних технологій

Зрозуміло, що предмет дослідження даного питання повинен бути дещо звуженим: торкатися не інформаційних технологій взагалі, а саме сфери електронного урядування. Проте майже усі основні міжнародні правові акти та акти зарубіжних національних законодавств у сфері інформаційних технологій тією чи іншою мірою стосуються проблематики електронного урядування. Пропонуємо аналіз основних документів у цій сфері.

Перший у світі Закон «Про цифровий підпис» був прийнятий американським штатом Юта 1 травня 1995 року (Utah Digital Signature Act).

Слід також зауважити, що у даній сфері існує ряд проектів законодавчих актів, наприклад: Модельний закон «Про електронний цифровий підпис» СНД (проект); проект Закону Польщі «Про електронний підпис» (від 18 листопада 2000 року).

Важливе місце серед міжнародних документів посідає Типовий закон ЮНІСТРАЛ «Про електронні підписи», прийнятий Комісією ООН з права міжнародної торгівлі у Відні 5 червня 2001 року. Відповідно до п. а статті 2 («Визначення») Типового закону, під електронним підписом слід розуміти дані в електронній формі, які містяться в повідомленні про дані, додані до нього або логічно асоціюються з ним і які можуть бути використані для ідентифікації того, хто підписався, у зв'язку з повідомленням даних і вказівки на те, що той, хто підписався, згоден з інформацією, що міститься в повідомленні даних. У Типовому законі також передбачено рівний режим для технологій створення електронних підписів, дотримання вимог щодо наявності електронного підпису, вимоги до поведінки того, хто підписувався, вимоги до поведінки поставальника сертифікаційних послуг, випадки визнання іноземних сертифікатів і електронних підписів.

6—7 травня 1999 р. у Будапешті на 104 сесії Комітету міністрів Ради Європи було прийнято Декларацію про європейську політику у галузі нових інформаційних технологій. У вказаному документі говориться, що Комітет міністрів Ради Європи закликає уряди держав-учасниць щодо доступу до нових інформаційних технологій і участі в них у таких напрямках:

- сприяти максимально широкому доступу для всіх до нових інформаційних технологій і комунікаційних послуг, наприклад, шляхом створення широкої мережі пунктів доступу в громадських місцях;
- дати можливість усім особам відігравати більш активну роль у житті суспільства на національному, регіональному і місцевому рівнях шляхом використання нових інформаційних технологій з метою: забезпечення безперешкоди доступу до інформації про місцеві, регіональні адміністрації та юридичні служби і прямих зв'язків з ними; забезпечення доступу до офіційних текстів місцевих, регіональних і національних законів і нормативних актів, міжнародних договорів і рішень національних і міжнародних судових органів;
- сприяти вільному обміну інформацією, думками та ідеями з використанням нових інформаційних технологій;

- сприяти розробці і виробництву матеріалів культурного й освітнього призначення та їх широкому розповсюдженню;

- сприяти ефективному міжнародному співробітництву з метою отримання тієї користі, яку несуть розширення доступу і збільшення транспарентності;

- сприяти створенню рівних можливостей для використання нових інформаційних технологій усіма європейськими державами.

Важливе місце серед міжнародних актів у галузі інформаційних технологій посідає Окінавська хартія глобального інформаційного суспільства, прийнята 22 липня 2000 року. У ній закріплено намір щодо здійснення керівництва в активізації зусиль урядів стосовно зміцнення відповідної політики і нормативної бази, які б стимулювали конкуренцію і новаторство, забезпечення економічної і фінансової стабільності, сприяли співробітництву в оптимізації глобальних мереж, боротьбі зі зловживаннями, які підривають цілісність мережі, щодо скорочення розриву у цифрових технологіях, інвестування у людей і забезпечення глобального доступу й участі в цьому процесі (п. 4 Хартії). Для досягнення цих та інших цілей важливо будувати та здійснювати роботу, використовуючи такі ключові напрямки (п. 6 Хартії):

- проведення економічних і структурних реформ з метою створення середовища відкритості, ефективності, конкуренції і використання нововведень, які доповнювалися б заходами щодо адаптації на ринку праці, розвитку людських ресурсів і забезпечення соціального балансу;

- раціональне управління макроекономікою, яке б сприяло чіткішому плануванню з боку ділових кіл і споживачів, та використання переваг нових інформаційних технологій;

- розробка інформаційних мереж, які б забезпечували швидкий, надійний, безпечний і економічний доступ за допомогою конкурентних ринкових умов і відповідних нововведень стосовно мережевих технологій, їх обслуговування і застосування;

- розвиток людських ресурсів, здатних відповідати вимогам століття інформації, шляхом освіти і безперервного навчання та задоволення постійного попиту на спеціалістів у галузі ІТ в багатьох секторах нашої економіки;

- активне використання ІТ в державному секторі і сприяння наданню в режимі реального часу послуг, необхідних для підвищення рівня доступності влади для всіх громадян.

Директива Європейського Союзу про електронні підписи містить два визначення електронного підпису — власне електронний підпис, і «розширений» електронний підпис. Під електронним підписом у Директиві розуміють «дані в електронній формі, які прикладені або логічно приєднані до інших електронних даних і які використовуються як метод автентифікації» (п. 1 статті 2). Під розширеним електронним підписом слід

розуміти електронний підпис, який відповідає таким вимогам: а) він виключно стосується особи, яка підписалася; б) з його допомогою можна ідентифікувати особу, яка підписалася; с) він створений за допомогою засобів, які особа, що підписалася, може мати під своїм виключним контролем; д) він з'єднаний з даними, до яких він відноситься, таким чином, що є можливість виявити наступну модифікацію таких даних» (п. 2 статті 2).

Якщо говорити про міжнародні документи (включаючи нормативно-правові акти зарубіжних держав) у галузі інформаційних технологій, то можна стверджувати, що на сьогодні в світі існує досить масивна законодавча база, що регулює згадані питання. Таким чином, пропонуємо короткий перелік окремих законодавчих актів.

За останні роки у світі відбулися значні зрушення у сфері законодавчого закріплення використання електронних цифрових підписів і надання юридичної сили електронним документам. Найбільш цікавими у законодавчому плані видаються закони про цифрові (електронні) підписи Австрії, США, ФРН.

З 1 січня 2000 року в Австрії вступив в силу Закон «Про електронний підпис». У ФРН Закон «Про цифровий підпис» дє з 1997 року (остаточна редакція — березень 2002 року). 30 червня Президент США Клінтон за допомогою електронного підпису підписав Закон «Про електронні підписи в міжнародному комерційному обороті», Закон вступив в силу з 1 жовтня 2000 року.

Закон США «Про електронний підпис» стосується трансакцій у міжнародному і міжштатному обігу. Закони Австрії і ФРН поширюються (перважно) на трансакції всередині країни.

Американський Закон про електронний підпис дає таке визначення електронного підпису (п. 5 статті 106 Закону): термін «електронний підпис» означає звук, символ, або процес прислання чи логічно з'єднаний з контекстом чи іншим документом (записом), і який здійснюється чи одержується особою з метою підписання документа (запису). При цьому під «особою» розуміється (п. 8 статті 106 Закону): «фізична особа, корпорація, комерційний траст, маєток, траст, товариство з обмеженою відповідальністю, асоціація, спільне підприємство, урядове агентство, публічна корпорація або будь-яка інша юридична чи комерційна особа».

Відповідно до визначення, даного у статті 2 «Визначення понять» Закону ФРН «Про цифровий підпис», цифровий підпис — це створена за допомогою приватного ключа печатка до цифрових даних, яка за допомогою відповідного відкритого ключа, забезпеченого сертифікатом ключа підпису, виданим сертифікаційним центром або державною установою, дозволяє визначити власника ключа підпису і достовірність даних.

Відповідно до статті 2 австрійського Закону «Про електронний підпис», під електронним підписом розуміють електронні дані, які додані до інших електронних даних або логічно з'єднані з останніми, і служать для аутентифікації останніх або ідентифікації особи, яка поставила підпис. Ва-

жається, що австрійський Закон повністю ґрунтується на Директиві Європейського Союзу про електронні підписи, і Австрія стала першим членом Союзу, яка здійснила імплементацію даної Директиви.

У майбутньому, очевидно, слід очікувати уніфікації норм законодавства різних держав про електронний цифровий підпис, що дозволить ширше застосовувати технології цифрового підпису і пов'язані з ним технології (відмітки часу, системи «клієнт-банк», цифрова готівка і т. д.) в міжнародному обороті. Нині вживаються заходи у цьому напрямку, частково піднімаються питання про уніфікацію законодавства США і Європейського Союзу в цій галузі.

Слід також зауважити, що в умовах сучасного рівня світової глобалізації розвиток інформаційного суспільства в Україні не може відбуватися сепаративно від інших країн. Тому важливим елементом інтеграції України в європейський простір є врахування стандартів її стратегічних партнерів, зокрема Європейського Союзу, що проголошено пріоритетним напрямом зовнішньополітичного курсу держави. Щодо адаптації законодавства України до законодавства Європейського Союзу, то слід зазначити, що Постановою Кабінету Міністрів України від 16 серпня 1999 року була схвалена Концепція адаптації законодавства України до законодавства Європейського Союзу. Метою адаптації є досягнення відповідності правової системи України з правовою системою Європейського Союзу (*acquis communautaire*), яка включає акти законодавства Європейського Союзу (але не обмежується ними), прийняті в рамках Європейського співтовариства, з урахуванням критеріїв, що висуваються Європейським Союзом до держав, які мають намір вступити до нього.

Як уже згадувалося, чинне законодавство України не охоплює усі сфери правового регулювання відносин у галузі інформаційних технологій. Існує велика кількість нормативно-правових актів різної юридичної сили та галузевої належності, що регулює відносини у сфері ІКТ. Вони потребують узгодження та певної систематизації.

Відсутність комплексного підходу до формування законодавства України у сфері ІКТ обумовило несистемність законів і підзаконних актів у сфері інформаційних відносин, що ускладнює їх пошук, аналіз і узгодження для практичного застосування. До того ж для розбудови інформаційного суспільства в Україні необхідно запровадити відповідні правові засади згідно із законодавством ЄС. Існує думка, що ефективне функціонування сучасної економіки, побудованої на знаннях, є можливим тільки в умовах існування належної нормативно-правової бази, що потребує розроблення концепції розвитку і кодифікації законодавства з врахуванням чинних норм законодавства ЄС, прийняття нормативно-правових актів України, що стосуються окремих правових інститутів у сфері ІКТ.

Таким чином, існує необхідність у прийнятті базового закону та нових законодавчих актів у сфері ІКТ, а в перспективі — у прийнятті Інформаційного кодексу.

ЗАМІСТЬ ВИСНОВКІВ. ЗАВДАННЯ ЕЛЕКТРОННОГО УРЯДУВАННЯ ТА ПЕРСПЕКТИВИ ЙОГО ЗАПРОВАДЖЕННЯ В УКРАЇНІ

Оскільки у попередніх розділах йшлося здебільшого про аналіз поняття, природи та форм електронного урядування, його правове забезпечення у зарубіжних країнах, то в цьому розділі хотілося б зупинитися саме на перспективах запровадження та функціонування електронного урядування в Україні, а також на основних його завданнях (етапах) та їх теоретичному обґрунтуванні.

Незважаючи на те що Україна вже тринадцять років є незалежною державою, влада, як і раніше, залишається «акціонерним товариством закритого типу», особливо в частині, що стосується інформації. Звідси — корупція, розкрадання бюджетних коштів, свавілля місцевих чиновників та інші негативні економічні чинники. Багато в чому змінити ситуацію міг би перехід до нових інформаційних технологій. По суті, його можна назвати своєрідною інтелектуальною революцією, за якої змінюється не сама влада, а її функції в суспільстві: від свавільного управління до надання послуг платникам податків, у тому числі і з управлінні державою⁹⁴.

Отже, нові інформаційні технології виконують важливі функції:

- розширюють права громадян шляхом надання доступу до різноманітної інформації;
- збільшують можливості людей брати участь у процесі прийняття політичних рішень і стежити за діями урядів;
- надають можливість активно створювати інформацію, а не тільки її споживати;
- забезпечують засоби захисту приватного життя й анонімності особистих контактів і комунікацій.

О.А. Баранов виділяє чотири групи передумов формування та практичного запровадження електронного урядування, зокрема, для України: правові, технологічні, кадрові та організаційні.

Правові передумови:

- створення нормативно-правової бази застосування інформаційних комп'ютерних технологій, зокрема стосовно визначення та відповідного закріплення умов надання урядових послуг у режимі он-лайн та правового статусу електронного документа й електронного підпису; правового статусу й умов захисту персональних даних та правового статусу урядових інформаційних ресурсів;
- регламентації та уніфікації звернень, заяв, інших документів, що виконуються в процесі надання урядових послуг у режимі он-лайн.

Технологічні передумови:

- створення сучасної, мультисервісної телекомунікаційної мережі, особливо в містах;

⁹⁴ Галковська Т. «Електронна революція» і влада: хто кого? // Дзеркало тижня. — 2002. — № 33 (408), 31 серпня — 7 вересня.

Завдання електронного урядування та перспективи його запровадження в Україні

- інформатизація всіх внутрішніх управлінських процесів урядових структур;
- створення інтегрованого інформаційно-телекомунікаційного середовища урядових структур;
- забезпечення інтерактивності в урядових комп'ютерних інформаційних системах;
- максимальна уніфікація інформаційних процесів та процедур;
- максимальне використання існуючих систем збору, обробки та збереження накопиченої інформації.

Кадрові передумови:

- створення умов формування внутрішньої мотивації урядів, державних службовців для застосування комп'ютерних інформаційних технологій у процесі обслуговування населення та бізнесових структур;
- підвищення комп'ютерної грамотності населення, зокрема за рахунок впровадження інформаційних технологій у процес навчання середньої та вищої школи.

Організаційні передумови:

- проведення адміністративної реформи, організаційних перетворень в урядових структурах з урахуванням результатів аналізу та систематизації інформаційних відносин та потоків;
- модернізації урядової системи документообігу за умови використання комп'ютерних інформаційних технологій;
- розробка регламенту взаємодії урядових структур з метою сумісного обслуговування населення та бізнесових структур;
- організація пунктів колективного доступу населення до системи урядових послуг в режимі он-лайн;
- створення умов для інтеграції систем електронного урядування та систем безготівкового обігу грошей (електронні банківські смарт-карти)⁹⁵.

З метою становлення електронного урядування в Україні нам необхідно послідовно вирішити чотири завдання:

1. Організація електронного документообігу в органах державної влади і місцевого саморядування.

Цей етап передбачає досягнення таких результатів:

- *щодо технічного забезпечення:*
 - забезпечення всіх органів державної влади, органів місцевого саморядування комп'ютерами та їх підключення до локальної електронної мережі;
 - налагодження якості існуючого зв'язку;
 - вжиття заходів щодо забезпечення захисту інформації, методів фільтрації й запобігання розповсюдженню забороненої законодавством України інформації.

⁹⁵ Баранов О. Електронний уряд в Україні: передумови та наслідки // Доповідь у рамках конференції «Електронний уряд та електронна демократія». 12. 04. 2002.

У цьому напрямку на сьогодні у декількох відомствах досягнуто рівня, який може стати основою для реалізації електронного уряду (незважаючи на те що майже не існує проблем з комп'ютерним забезпеченням державних органів). Серед таких органів — Державна податкова адміністрація, Пенсійний фонд, МВС, Держкомстат, Ліцензійна палата, Торговельно-промислова палата, Держкоміприміністратива, Держстандарт, Міністерство освіти і науки, Державна митна служба.

• *щодо правового забезпечення:*

У цьому напрямку вже досягнуто позитивних результатів — два важливих закони — «Про електронний цифровий підпис» та «Про електронні документи та електронний документообіг», прийняті 22 травня 2003 року (набули чинності 1 січня 2004 року).

2. Інформування громадян про діяльність органів виконавчої влади і місцевого самоврядування через інформаційні технології.

Дане завдання передбачає наявність веб-сторінок у кожного органу влади, де повинні міститися вся необхідна інформація, що ілюструє призначення, компетенція того чи іншого органу, а також створення урядового веб-порталу, призначеного для інтеграції веб-сайтів органів виконавчої влади та розміщення інформаційних ресурсів відповідно до потреб громадян. Кабінет Міністрів України 4 січня 2002 року прийняв Постанову «Про порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади» за № 3, якою затвердив Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади, а також зобов'язав оприлюднювати через Інтернет органами виконавчої влади інформацію (зміст та обсяг) про свою діяльність. На сьогодні майже всі органи державної влади мають свої власні веб-сторінки. Це переважно стосується центральних та місцевих органів виконавчої влади, Верховної Ради України та ін. Проте існують проблеми щодо наявності сайтів в органах місцевого самоврядування, особливо на рівні районних, сільських рад. Позитивним кроком на шляху організації електронного документообігу, а також забезпечення інформування громадян, є створення і функціонування веб-порталу органів виконавчої влади (www.kmu.gov.ua).

3. Забезпечення можливості звернення громадян до органів державної влади через IT.

Це здійснюється шляхом подання інформаційного запиту громадянами до органів державної влади, органів місцевого самоврядування через Інтернет. Щоб ця система ефективно діяла, необхідно створити таке програмне забезпечення, яке б дозволяло простежити рух звернення з моменту його надходження до моменту його виконання, визначення типу (переліку) звернень, які підпадають чи не підпадають під такі, що потребують чи не потребують розгляду і виконання (є чи не є юридично значимі). До того ж необхідно внести зміни до Закону України «Про звернення громадян» у частині регламентації процедури звернення громадян через Інтернет (порядок подачі такого звернення, строки розгляду та ін.).

4. Надання адміністративних послуг через IT.

Це означає, що громадянин, заповнивши певну анкету (ресурсний картку тощо) безпосередньо на сайті певного органу або заповнивши анкету в електронній формі і надіславши її електронною поштою у відповідний орган влади, може отримати ту чи іншу адміністративну послугу, наприклад зареєструватися суб'єктом підприємництва тощо. Це завдання включає прийняття Закону «Про адміністративні послуги», у якому було б передбачено спосіб надання послуг — через Інтернет; визначення переліку адміністративних послуг, які повинні надаватися громадянам, у тому числі через Інтернет; встановлення відповідальності за ненадання або несвоєчасне надання тієї чи іншої адміністративної послуги через Інтернет; програмне забезпечення здійснення контролю за наданням адміністративних послуг з боку вищих органів влади щодо їм підпорядкованих.

Надання управлінських послуг органами державної влади і місцевого самоврядування через IT зробить «спликування» громадянства і держави прозорим і більш ефективним.

Таким чином, втілення інтернет-технологій у сферу державної влади, з одного боку, дозволить підвищити її ефективність, а з другого — зробить більш відкритою роботу органів державної влади. Робота в режимі електронного урядування принципово змінює атмосферу взаємодії чиновників і населення. Кожний громадянин отримує можливість відстежувати пошій у діяльності органів державної влади, органів місцевого самоврядування, знати про плани їхньої роботи, безпосередньо вступати у взаємодію з ними без черг та зайвої бюрократії. Електронне урядування — це автоматизація роботи з документами, із заявами громадян, довідками, ліцензіями, іншими формальними актами, які легалізують певну діяльність громадянина. Це також і можливість громадянина відслідковувати долю його запиту, скарги, пропозиції, вимоги. Офіційна установа перестає бути темним ящиком, у якому безслідно зникають усі вияви громадянської активності. Електронне урядування забезпечує, перш за все, прозорість роботи державного апарату, знижує, якщо не ліквідує, залежність громадянства чи організації від сваволі чиновника, а отже — запобігає корупції.

Створення і розвиток урядової мережевої інформаційної інфраструктури вимагає відповідної формалізації в нормативно-правових актах і необхідного бюджетного фінансування. Слід розуміти, що запровадження електронного урядування — це масштабний і довгостроковий проєкт. Створення інформаційної мережевої інфраструктури держави повинно супроводжуватися «реінжинірингом» (тобто інформаційною перебудовою) усієї системи управлінських процесів, насправді, означає подолання стереотипів бюрократичної культури. Можливо, реалізації концепції буде сприяти адміністративна реформа, мета якої — модернізація системи державного управління.

Отже, електронне урядування, яке на перший погляд, є лише механізмом з'єднання інформаційних технологій і уряду, насправді створює умови для формування нової філософії державного управління, тому для реального втілення цієї ідеї в життя необхідна розробка нової законодавчої бази. Насамперед ідеться про те, що до певної міри в Україні вже зроблено — надання правового статусу електронним документам і електронному підпису, проте ще не застосовується.

Потім необхідна адаптація нормативної бази, що регламентує діяльність в державних установах до особливостей, що зумовлені використанням комп'ютерних технологій. Вимагає дослідження і регулювання питання визначення правового статусу електронних інформаційних ресурсів, що будуть розміщуватися в комп'ютерних мережах державними органами як для міждомочого, так і для загальнодоступного використання. Але основні проблеми лежать у площині правової регламентації надання он-лайнних послуг населенню і бізнесу. Необхідно досить чітко виписати в законодавстві загальні умови надання таких послуг, а також особливості для окремих їхніх видів, регламентувати порядок звернень і стандартизувати форми заяв та інших документів, що будуть використовуватися. При цьому особливу увагу варто приділити питанню забезпечення законодавчих гарантій надання таких послуг. Без вирішення правових проблем ідея електронного урядування буде аматорством і приречена на провал⁹⁶.

Отже, перспективи запровадження електронного урядування у нашій державі, то вони, безперечно, існують. Громадянин буде знаходитися «біля керма», а державні послуги й інформація будуть надаватися в той час, у тому місці й у тому вигляді, як цього захочуть люди. Вдало реалізовані електронні адміністративні послуги будуть відкритими, загальнодоступними, орієнтованими на користувача, інтегрованими і ґрунтованими на принципі партнерства держави і приватного сектору. Вони не тільки залучать тих людей, що вже підключені до мережі Інтернет, але і зможуть привести в мережу тих, хто ще не знайомий з нею. Головне для досягнення цієї мети — надати додаткові послуги громадянам і приватним компаніям. У кінцевому рахунку, автоматизація державних служб може призвести до «прямой демократії» (без проміжних ланок).

Узагальнюючи все зазначене вище, можна зробити висновок, що суть електронного урядування зводиться до забезпечення, у першу чергу, громадянам якості функціонування чи діяльності органів влади без зайвої бюрократії. Усі передумови електронного урядування в основному зводяться до таких, як правові, організаційні, технологічні та кадрові. До переломов також можна віднести психологічний аспект — усвідомлення необхідності як громадянами, так і чиновниками запровадження електронного урядування.

Наслідками запровадження електронного урядування буде відкритість та прозорість діяльності органів державної влади та місцевого самоврядування; економія часу та матеріальних ресурсів; підвищення якості надання адміністративних послуг.

Для досягнення цих та інших цілей, для успішного втілення ідеї електронного урядування потрібно, безперечно, виконати багато поставлених перед собою завдань, про які вже говорилося вище. Але основне — це бажання, зацікавленість, чого часто так не вистає. Тому необхідно докласти максимум зусиль кожному з нас, щоб досягти бажаного, пам'ятаючи, що запровадження електронного урядування в Україні є надзвичайно важливим інструментом демократизації нашої суспільства.

ЕЛЕКТРОННІ ПРЕДСТАВНИЦТВА УРЯДІВ СВІТУ

Австрія

http://www.helr.gv.at	Австрійський урядовий портал
http://www.bmf.gv.at	Урядові сторінки Міністерства фінансів
http://www.austrija.gv.at	Офіційна сторінка уряду

Болгарія

http://portal.government.bg	Урядовий портал Болгарії (містить публічну інформацію та можливість здійснення е-платежів)
---	--

Чеська республіка

http://www.cvis.cz	Доступ до публічних документів
http://www.centralni-adresa.cz/cadp/index.htm	Інформаційна система публічного постачання та аукціонів.

Данія

http://www.danmark.dk	Сервісні сторінки для громадян
http://www.indberetning.dk	Сервісні сторінки для бізнесу

Естонія

http://www.tlk.ee	Національний урядовий сайт Естонії
http://www.gov.ee	Національний урядовий сайт Естонії

Фінляндія

http://www.vp.fi/vm/kehittaminen/tietohallinto/portaali.htm	Масштабний портал публічних послуг
http://www.oras.vp.fi	Інформація представлена на життєвих етапах

⁹⁶ Баранов О. Цифрове законодавство // Дзеркало тижня. — 2002. — № 20 (395), 1—7 червня.

Франція

http://www.service-public.fr	Портал публічних послуг (центральный рівень 1)
http://www.fonctionpublique.gouv.fr/tic	Сторінки е-уряду Франції
http://www.finances.gouv.fr	Міністерство економіки, фінансів та промисловості Франції.
http://www.intemet.gouv.fr	Програма інформаційного суспільства
http://www.atisa.rn.gouv.fr	Агентство інформаційно-комп'ютерних технологій

Німеччина

http://www.bund.de	Центральний доступ до веб-контенту адміністрації Німеччини
---	--

Італія

http://www.rafforum.net	Урядовий публічний адміністративний форум Італії
---	--

Люксембург

http://www.eluxepboudg.lu	Веб-сайт електронного уряду Люксембургу
---	---

Нідерланди

http://www.Overheid.nl	Веб-сайт е-уряду Нідерландів
---	------------------------------

Польща

www.mg.gov.pl	Міністерство економіки
www.krpm.gov.pl	Канцелярія Прем'єр-міністра

Португалія

http://www.infocid.pt	Портал публічних послуг Португалії
---	------------------------------------

Словенія

http://www.gov.si/mid	Міністерство інформаційного суспільства
http://www.gov.si/cvi	Урядовий центр інформатизації

Швеція

http://www.statistikonet.se/egov	Урядові веб-сайти Швеції
---	--------------------------

Швейцарія

http://e-gov.admin.ch	Сайт проекту
http://www.admin.ch	Федеральні служби Швейцарської конфедерації

Туреччина

http://www.bybs.gov.tr	Національний сайт електронного уряду
---	--------------------------------------

Великобританія

http://www.ukonline.gov.uk/online/	Публічний доступ до урядової інформації та послуг у режимі он-лайн.
---	---

Гонконг

http://www.esd.gov.hk/eng/default.asp	Електронні послуги, що пропонуються урядом Гонконгу.
---	--

Сінгапур

http://www.gov.sg	Урядовий портал
---	-----------------

ПАР

http://www.gov.za	Уряд ПАР в режимі он-лайн
---	---------------------------

США

http://www.firstgov.gov	Офіційні веб-сторінки уряду США
---	---------------------------------

ЧАСТИНА III

МІЖНАРОДНЕ ПРАВО
У СФЕРІ ІНФОРМАЦІЇ

**КОНВЕНЦІЯ РАДИ ЄВРОПИ ПРО ЗАХИСТ ОСІБ СТОСОВНО
АВТОМАТИЗОВАНОЇ ОБРОБКИ ДАНИХ ОСОБИСТОГО ХАРАКТЕРУ
№108**

(Прийнято 28 січня 1981 р.)
Страсбург, 28 січня 1981 року
European Treaty Series/108

ПРЕАМБУЛА

Держави-члени Ради Європи, які підписали цю Конвенцію, враховуючи, що метою Ради Європи є досягнення більшого єднання між її членами, зокрема на основі поважання верховенства права, а також прав і основних свобод людини, зважаючи на доцільність поширення гарантій прав і основних свобод кожної людини, і зокрема права на повагу до особистого життя з огляду на зростання транскордонного потоку даних особистого характеру, які піддаються автоматизованій обробці, підтверджуючи в той же час свою відданість свободі інформації незалежно від кордонів, визнаючи необхідність угодження основоположних цінностей поваги до особистого життя та безперешкодного обміну інформацією між народами, погодилися 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 національності або помешкання поважання її прав і основних свобод, і зокрема її права на недоторканність особистого життя, стосовно автоматизованої обробки даних особистого характеру, що її стосуються («захист даних»).

Стаття 2. Визначення

Для цілей цієї Конвенції:

- а) «дані особистого характеру» означають будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною («суб'єкт даних»);
- б) «файл даних для автоматизованої обробки» означає будь-який масив даних, що піддаються автоматизованій обробці;
- с) «автоматизована обробка» включає такі операції, що здійснюються повністю або частково за допомогою автоматизованих засобів: збіріння даних, виконання логічних і/або арифметичних операцій з цими даними, зміна, знищення, вибірка або поширення даних;

д) «**контролер файлу**» означає фізичну чи юридичну особу, державний орган, установу або будь-який інший орган, що має повноваження відповідно до внутрішнього права вирішувати щодо цілі файлу даних для автоматизованої обробки, категорій даних особистого характеру, що мають зберігатися, та операцій, які мають здійснюватися з ними.

Стаття 3. Сфера застосування

1. Сторони зобов'язуються застосовувати цю Конвенцію до файлів даних особистого характеру для автоматизованої обробки та до автоматизованої обробки даних особистого характеру у державному та приватному секторах.

2. Будь-яка держава під час підписання або здачі на зберігання своєї ратифікаційної грамоти або свого документа про прийняття, затвердження чи приєднання або в будь-який інший час після цього може повідомити заявою на ім'я Генерального секретаря Ради Європи про те, що вона:

- а) не застосовуватиме цю Конвенцію до певних категорій файлів даних особистого характеру для автоматизованої обробки, перелік яких буде заданий на зберігання. Однак у цей перелік вона не включає категорії файлів даних для автоматизованої обробки, які згідно з її внутрішнім правом підпадають під дію положень про захист даних. Відповідним чином, вона вносить поправки до цього переліку новою заявою у випадках, коли згідно з її внутрішнім правом під дію положень про захист даних підпадають нові категорії файлів даних особистого характеру для автоматизованої обробки;
- б) застосовуватиме також цю Конвенцію до інформації, яка стосується груп осіб, асоціацій, фондаций, 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) застосовуватиме також цю Конвенцію до файлів даних особистого характеру, які не піддаються автоматизованій обробці.

3. Будь-яка держава, що поширила сферу застосування цієї Конвенції будь-якою із заяв, передбачених у підпункті 2б або с вище, може повідомити у згаданій заяві, що таке поширення дії Конвенції стосується лише певних категорій файлів даних особистого характеру, перелік яких буде заданий на зберігання.

4. Будь-яка Сторона, що заявою, передбаченою у підпункті 2а вище, виключила зі сфери застосування цієї Конвенції певні категорії файлів даних особистого характеру для автоматизованої обробки, не може вимагати застосування Конвенції до таких категорій Стороною, яка зі сфери застосування цієї Конвенції їх не виключила.

5. Відповідним чином, Сторона, яка не поширила сферу застосування Конвенції, як це передбачено у підпунктах 2б і с вище, не може вимагати застосування цієї Конвенції по цих пунктах стосовно Сторони, яка поширила у такий спосіб сферу її застосування.

6. Заяви, передбачені у пункті 2 вище, набирають чинності з моменту набрання чинності Конвенцією стосовно держави, яка їх зробила, якщо такі заяви були зроблені під час підписання або здачі на зберігання її ратифікаційної грамоти 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 набирає чинності через три місяці від дати отримання такого повідомлення.

Глава II ОСНОВОПОЛОЖНІ ПРИНЦИПИ ЗАХИСТУ ДАНИХ

Стаття 4. Обов'язки Сторін

1. Кожна Сторона в межах свого внутрішнього права вживає необхідних заходів з метою запровадження основоположних принципів захисту даних, викладених у цій главі.

2. Такі заходи вживаються не пізніше моменту набрання чинності цією Конвенцією стосовно відповідної Сторони.

Стаття 5. Якість даних

Дані особистого характеру, що піддаються автоматизованій обробці:

- а) отримуються та обробляються сумлінно та законно;
- б) зберігаються для визначених і законних цілей та не використовуються у спосіб, неумісний з цими цілями;
- в) мають бути адекватними, відповідними і ненадмірними з точки зору цілей, заради яких вони зберігаються;
- г) мають бути точними та у разі необхідності мають поновлюватися;
- е) зберігаються у форматі, який дозволяє ідентифікувати суб'єктів даних не довше, ніж це необхідно для цілі, заради якої такі дані зберігаються.

Стаття 6. Особливі категорії даних

Дані особистого характеру, що свідчать про расову приналежність, політичні або релігійні чи інші переконання, а також дані особистого характеру, що стосуються здоров'я або статевого життя, не можуть піддаватися автоматизованій обробці, якщо внутрішнє право не забезпечує відповідних гарантій. Це правило застосовується також до даних особистого характеру, що стосуються засудження у кримінальному порядку.

Стаття 7. Захист даних

Для захисту даних особистого характеру, що зберігаються у файлах даних для автоматизованої обробки, вживаються відповідні заходи захисту, спрямовані на запобігання випадковому чи несанкціонованому знищен-

ню або випадковій втраті, а також на запобігання несанкціонованому доступу, зміненню або поширенню.

Стаття 8. Додаткові гарантії для суб'єкта даних

Будь-якій особі має бути надана можливість:

- а) встановлювати існування файлу даних особистого характеру для автоматизованої обробки, його головні цілі, а також особистість та постійне помешкання чи місце знаходження головної штаб-квартири контролера файлу;
- б) отримувати через розумні проміжки часу та без надмірної затримки або витрат підтвердження або спростування зберігання даних особистого характеру, що її стосуються, у файлі даних для автоматизованої обробки, а також отримувати такі дані у доступній для розуміння формі;
- с) вимагати у відповідних випадках виправлення або знищення таких даних, якщо вони оброблялися на порушення положень внутрішнього права, що запроваджують основоположні принципи, визначені у статтях 5 і 6 цієї Конвенції;
- д) використовувати засоби правового захисту у разі невиконання передбаченого у пунктах б і с цієї статті прохання про підтвердження або у відповідних випадках про надання, виправлення або знищення даних.

Стаття 9. Винятки та обмеження

1. Винятки з положень статей 5, 6 і 8 цієї Конвенції дозволяються тільки в межах, визначених цією статтею.
2. Відступ від положень статей 5, 6 і 8 цієї Конвенції дозволяється у випадках, коли такий відступ передбачається законодавством Сторони та є у демократичному суспільстві необхідним заходом, спрямованим на:
 - а) захист державної та громадської безпеки, валютно-кредитних інтересів держави або на боротьбу із кримінальними правопорушеннями;
 - б) захист суб'єкта даних або прав і свобод інших людей.
3. Обмеження на здійснення прав, визначених у пунктах б, с і д статті 8, можуть запроваджуватися законодавством стосовно файлів даних особистого характеру для автоматизованої обробки, що використовуються для цілей статистики або наукових досліджень, у випадках явної відсутності небезпеки порушення недоторканності 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 даних, визначені у цій главі.

Стаття 11. Розширення захисту

Жодне з положень цієї глави не тлумачиться як таке, що обмежує або іншим чином зашкоджує можливості Сторони забезпечувати суб'єктам даних ступінь захисту більш високий, ніж той, що передбачається цією Конвенцією.

Глава III ТРАНСКОРДОННІ ПОТОКИ ДАНИХ

Стаття 12. Транскордонні потоки даних особистого характеру та внутрішнє право

1. Стосовно передачі через національні кордони за допомогою будь-яких засобів даних особистого характеру, що піддаються автоматизованій обробці або що зібрані з метою їхньої автоматизованої обробки, застосовуються такі положення.
2. Сторона не може лише з метою захисту недоторканності особистого життя захищати або зумовлювати спеціальними дозволами транскордонні потоки даних особистого характеру, що передаються на територію іншої Сторони.
3. Однак кожна Сторона має право відступати від положень пункту 2:
 - а) якщо її законодавство містить конкретні положення для деяких категорій даних особистого характеру або файлів даних особистого характеру для автоматизованої обробки, у зв'язку із характером цих даних або цих файлів, за винятком випадків, коли положення іншої Сторони забезпечують аналогічний захист;
 - б) якщо передача даних здійснюється з її території на територію держави, що не є Договірною, через територію іншої Сторони, для запобігання порушенню такою передачею законодавства Сторони, згаданого на початку цього пункту.

Глава IV ВЗАЄМНА ДОПОМОГА

Стаття 13. Співробітництво між Сторонами

1. Сторони погоджуються надавати одна одній взаємну допомогу з метою виконання цієї Конвенції.
2. Для цього:
 - а) кожна Сторона призначає один або більше органів, назву та адресу яких вона повідомляє Генеральному секретареві Ради Європи;
 - б) кожна Сторона, яка призначила більше одного органу, зазначає у своєму повідомленні, згаданому в попередньому підпункті, сферу повноважень кожного з них.
3. Орган, призначений Стороною, на прохання органу, призначеного іншою Стороною:
 - а) надає інформацію про свої законодавство та адміністративну практику у галузі захисту даних;
 - б) у відповідності до свого внутрішнього права та з метою виключно захисту недоторканності особистого життя вживає всіх відпо-

відних заходів для надання достовірної інформації, що стосується конкретної автоматизованої обробки, яка здійснюється на його території, за винятком, однак, даних особистого характеру, що обробляються.

Стаття 14. Допомога суб'єктам даних, що мешкають за кордоном

1. Кожна Сторона надає допомогу будь-якій особі, що мешкає за кордоном, у здійсненні прав, наданих їй внутрішнім законодавством, що заповраджує принципи, визначені в статті 8 цієї Конвенції.

2. Якщо така особа мешкає на території іншої Сторони, їй надається можливість подати своє прохання через посередництво органу, призначеного цією Стороною.

3. Прохання про надання допомоги має містити всі необхідні відомості, що стосуються, крім іншого:

- а) прізвища, адреси та будь-яких інших відповідних відомостей, які визначають особу, що звертається з проханням;
- б) файлу даних особистого характеру для автоматизованої обробки, якого стосується прохання, або його контролера;
- с) 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 у відповідь на його власне прохання про надання допомоги, використовує цю інформацію тільки 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 ясної вираженої згоди суб'єкта даних, що мешкає за кордоном, у жодному випадку не дозволяється звертатися згідно з пунктом 2 статті 14 із проханням про надання допомоги від імені заінтересованої особи.

Стаття 16. Відхилення прохань про надання допомоги

Призначений орган, до якого звернене прохання про надання допомоги згідно зі статтею 13 або 14 цієї Конвенції, може відмовитися задовольняти таке прохання, якщо:

- а) прохання є несумісним із повноваженнями, якими наділені у галузі захисту даних органи, що відповідають за виконання прохання;
- б) прохання не відповідає положенням цієї Конвенції;
- с) виконання прохання може порушити суверенітет, безпеку або промалдський поряток Сторони, якою він був призначений, або права та основні свободи осіб, що перебувають 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 мешкають за кордоном, не може бути підставою для сплати жодних витрат або зборів, за винятком тих, що сплачуються на експертів і устних перекладачів. Витрати або збори на експертів і устних перекладачів сплачуються Стороною, яка призначила орган, що звертається з 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 мешканцями цієї Сторони.

3. Інші подробиці надання допомоги, що стосуються, зокрема, форм і процедур, а також використання мов, визначаються безпосередньо відповідними Сторонами.

Глава V КОНСУЛЬТАТИВНИЙ КОМІТЕТ

Стаття 18. Склад Комітету

1. Після набрання чинності цієї Конвенцією створюється Консультативний комітет.

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, що не є членом Ради Європи і не бере участі в Конвенції, бути представленою на тому чи іншому засіданні спостерігачем.

Стаття 19. Функції Комітету

Консультативний комітет:

- а) може вносити пропозиції з метою сприяння застосуванню Конвенції або його поліпшення;
- б) може вносити пропозиції про внесення поправок до цієї Конвенції відповідно до статті 21;
- с) надає свій висновок щодо будь-якої пропозиції про внесення поправок до цієї Конвенції, яка передається йому на розгляд відповідно до пункту 3 статті 21;
- д) може на прохання Сторони 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 упродовж дванадцяти місяців

після набрання цією Конвенцією чинності. Надані він збирається якнайменше один раз на два роки і у будь-якому випадку, коли одна третина представників Сторін вимагає його скликання.

2. Кворум засідання Консультативного комітету складає більшість представників Сторін.

3. Після кожного свого засідання Консультативний комітет подає Комітету міністрів Ради Європи доповідь про свою роботу та про стан виконання Конвенції.

4. З урахуванням положень цієї Конвенції Консультативний комітет складає свої власні правила процедури.

Глава VI ПОПРАВКИ

Стаття 21. Поправки

1. Поправки до цієї Конвенції можуть пропонуватися будь-якою Стороною, Комітетом міністрів Ради Європи чи Консультативним комітетом.

2. Будь-яка пропозиція про внесення поправки надсилається Генеральним секретарем Ради Європи державам-членам Ради Європи та кожній державі, що не є членом Ради, яка приєдналася до цієї Конвенції або якій було запропоновано приєднатися до неї відповідно до положень статті 23.

3. Крім того, будь-яка поправка, запропонована Стороною або Комітетом міністрів, надсилається Консультативному комітету, який подає Комітету міністрів свій висновок щодо цієї запропонованої поправки.

4. Комітет міністрів розглядає запропоновану поправку та будь-який висновок, поданий Консультативним комітетом, і може затвердити поправку.

5. Текст будь-якої поправки, затверджений Комітетом міністрів відповідно до пункту 4 цієї статті, надсилається Сторонам для прийняття.

6. Будь-яка поправка, затверджена відповідно до пункту 4 цієї статті, набирає чинності на тридцятий день після того, як усі Сторони поінформували Генерального секретаря про її прийняття.

Глава VII ЗАКЛЮЧНІ ПОЛОЖЕННЯ

Стаття 22. Набрання чинності

1. Цю Конвенцію відкрито для підписання державами-членами Ради Європи. Вона підлягає ратифікації, прийняттю або затвердженню. Ратифікаційні грамоти або документи про прийняття чи затвердження здаються на зберігання Генеральному секретареві Ради Європи.

2. Ця Конвенція набирає 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. Стосовно будь-якої держави-члена, яка висловлюватиме свою згоду на обов'язковість для неї цієї Конвенції після набрання нею чинності, Конвенція набирає чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати здачі на зберігання ратифікаційної грамоти або документа про прийняття чи затвердження.

Стаття 23. Приєднання держав, що не є членами Ради

1. Після набрання цією Конвенцією чинності Комітет міністрів Ради Європи може запропонувати будь-якій державі, яка не є членом Ради, приєднатися до цієї Конвенції у рішенні, що приймається більшістю голосів, передбаченою у статті 20d Статуту Ради Європи, і одноставним голосуванням представників Договірних Держав, які мають право засідати в Комітеті.

2. Стосовно будь-якої держави, що приєдналася до цієї Конвенції, Конвенція набирає чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати здачі на зберігання документа про приєднання Генеральному секретареві Ради Європи.

Стаття 24. Територіальне застосування

1. Будь-яка держава під час підписання або здачі на зберігання своєї ратифікаційної грамоти або свого документа про прийняття, затвердження чи приєднання може визначити територію (території), до якої застосовуватиметься ця Конвенція.

2. Будь-яка Держава може 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.

3. Будь-яка заява, зроблена відповідно до двох попередніх пунктів, може стосовно будь-якої території, визначеної в цій заяві, бути відкликана шляхом подання відповідного повідомлення на ім'я Генерального секретаря. Відкликання набирає чинності в перший день місяця, що настає після закінчення шестимісячного періоду від дати отримання такого повідомлення Генеральним секретарем.

Стаття 25. Застереження

Жодне застереження до положень цієї Конвенції не дозволяється.

Стаття 26. Денонація

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 та будь-яку державу, що приєдналася до цієї Конвенції, про:

- а) будь-яке підписання;
- б) здачу на зберігання будь-якої ратифікаційної грамоти або будь-якого документа про прийняття, затвердження чи приєднання;
- с) будь-яку дату набрання чинності цією Конвенцією відповідно до статей 22, 23 та 24;
- д) будь-яку іншу дію, будь-яке повідомлення або сповіщення, які стосуються цієї Конвенції.

На посвідчення чого представники, що нижче підписалися, належним чином на те уповноважені, підписали цю Конвенцію.

Вчинено у Страсбурзі двадцять восьмого дня січня місяця 1981 року англійською та французькою мовами, причому обидва тексти є однаково автентичними, в одному примірнику, який зберігатиметься в архіві Ради Європи. Генеральний секретар Ради Європи надсилає засвідчені копії цієї Конвенції кожній державі-члену Ради Європи та будь-якій державі, якій було запропоновано приєднатися до цієї Конвенції.

ДОДАТКОВИЙ ПРОТОКОЛ ДО КОНВЕНЦІЇ ПРО ЗАХИСТ ОСІБ СТОСОВНО АВТОМАТИЗОВАНОЇ ОБРОБКИ ДАНИХ ОСОБИСТОГО ХАРАКТЕРУ № 181 Страсбург, 08.11.2001

Преамбула

Сторони цього додаткового Протоколу до Конвенції про захист фізичних осіб стосовно автоматизованої обробки даних особистого характеру, відкритого для підписання 28 січня 1981 року у Страсбурзі (далі називається «Конвенція»);
переконані у тому, що органи нагляду, які виконують свої функції абсолютно незалежно, є складовою ефективного захисту фізичних осіб стосовно обробки даних особистого характеру;
беручи до уваги важливість потоків інформації між народами; беручи до уваги той факт, що зі збільшенням обмінів даними особистого характеру через державні кордони, необхідно забезпечити ефективний захист прав і основних свобод людини, і зокрема право на особисте життя, стосовно таких обмінів даними особистого характеру, погодилися про таке:

Стаття 1. Органи нагляду

1. Кожна Сторона наділяє один або більше органів відповідальністю забезпечувати дотримання положень національного законодавства, що вводять у дію принципи, викладені у главах II і III Конвенції та цього Протоколу.
2. а) У цьому відношенні зазначені органи повинні зокрема мати повноваження розслідування та втручання, а також право брати участь у процесуальних діях або привертати увагу компетентних судових органів до порушень положень національного законодавства, що вводять у дію принципи, зазначені у ч. 1 статті 1 цього Протоколу.
- б) Кожен орган нагляду розглядає претензії, подані будь-якою особою, щодо захисту її прав і основних свобод щодо обробки даних особистого характеру в межах їхньої компетенції.
3. Органи нагляду здійснюють свої функції абсолютно незалежно.
4. Спірні рішення органів нагляду можуть оскаржуватися в судовому порядку.
5. Відповідно до положень глави IV і без порушення положень статті 13 Конвенції органи нагляду співпрацюють один з одним у межах, необхідних для виконання їхніх обов'язків, зокрема шляхом обміну корисною інформацією.

Стаття 2. Транскордонні потоки даних особистого характеру, спрямовані до одержувача, який не підпадає під юрисдикцію Сторони цієї Конвенції

1. Кожна Сторона передає передачу даних особистого характеру одержувачеві, який підпадає під юрисдикцію держави чи організації, яка

не є Стороною цієї Конвенції, лише якщо така держава або організація забезпечує належний рівень захисту запланованої передачі даних.

2. Шляхом часткового обмеження положень ч. 1 статті 2 цього Протоколу кожна Сторона може дозволити передачу даних особистого характеру:

- а) якщо положення національного права дозволяють таку передачу через:
 - особливі інтереси суб'єкта даних або
 - інтереси, що мають легітимно переважне значення, особливо важливі публічні інтереси; або
- б) якщо гарантії захисту, які можуть зокрема виходити з договірних положень, забезпечуються оператором, що здійснює передачу, за умови, що відповідний компетентний орган вважає такі гарантії належними згідно норм національного права.

Стаття 3. Заключні положення

1. Положення Статей 1 і 2 цього Протоколу розглядаються Сторонами як додаткові статті Конвенції, і всі положення Конвенції застосовуються відповідно.

2. Цей Протокол відкрито для підписання Сторонами, які підписали Конвенцію. Після приєднання до Конвенції відповідно до встановлених нею умов, Європейське Співтовариство може підписати цей Протокол. Цей Протокол вимагає ратифікації, прийняття або схвалення. Сторона, які підписала цей Протокол, не може ратифікувати, прийняти чи схвалити його, якщо вона попередньо чи одночасно не ратифікувала, прийняла чи схвалила Конвенцію або не приєдналася до неї. Документи ратифікації, прийняття чи схвалення цього Протоколу подаються на зберігання Генеральному секретареві Ради Європи.

3. а) Цей Протокол набуває чинності у перший день місяця після завершення трьох місяців після дати, на яку п'ять Сторін, що підписали Конвенцію, виразять їхню згоду взяти на себе зобов'язання за цим Протоколом відповідно до положень ч. 2 статті 3.

б) Стосовно будь-якої іншої Сторони, яка підписала цей Протокол, що відповідно виражає її згоду взяти на себе визначені у ньому зобов'язання, цей Протокол набуває чинності у перший день місяця після завершення трьох місяців після дати передачі на збереження документа про ратифікацію, прийняття чи схвалення.

4. а) Після набуття чинності цим Протоколом, будь-яка держава, яка приєдналася до Конвенції, може також приєднатися до цього Протоколу.

б) Приєднання набуває чинності шляхом передачі на зберігання Генеральному секретареві Ради Європи документа про приєднання, який набирає чинності у перший день місяця після завершення трьох місяців після дати передачі такого документа на зберігання.

5. а) Будь-яка Сторона може в будь-який момент денонсувати цей Протокол, направивши попередження Генеральному секретареві Ради Європи.

б) Така денонсація набирає чинності у перший день місяця після завершення трьох місяців після дати отримання такого попередження Генеральним секретарем Ради Європи.

6. Генеральний секретар Ради Європи повідомляє держави-члени Ради Європи, Європейське Співтовариство і будь-яку іншу державу, яка приєдналася до Протоколу, про:

- а) будь-який факт підписання цього Протоколу;
- б) передачу на зберігання будь-якого документа про ратифікацію, прийняття чи схвалення цього Протоколу;
- с) будь-яку дату набрання чинності цим Протоколом відповідно до статті 3;
- д) будь-який інший акт, повідомлення чи інформацію, що стосується цього Протоколу.

На підтвердження чого особи, що нижче підписалися, будучи належним чином уповноваженими, підписали цей Протокол.

Вчинено у Страсбурзі цього 8-го дня листопада 2001 року англійською та французькою мовами, причому обидва тексти є однаково достовірними, у єдиному екземплярі, що передається на зберігання до архівів Ради Європи. Генеральний секретар Ради Європи передає засвідчені екземпляри кожній державі-члену Ради Європи, Європейському Співтовариству і будь-якій іншій державі, що запрошується приєднатися до цієї Конвенції.

ДОДАТКОВИЙ ПРОТОКОЛ ДО КОНВЕНЦІЇ ПРО ЗАХИСТ ФІЗИЧНИХ ОСІБ СТОСОВНО АВТОМАТИЗОВАНОЇ ОБРОБКИ ДАНИХ ОСОБИСТОГО ХАРАКТЕРУ, ЩО СТОСУЄТЬСЯ ОРГАНІВ НАГЛЯДУ ТА ТРАНСКОРДОННИХ ПОТОКІВ ДАНИХ

Пояснювальна записка
(схвалена 23 травня 2001 р.)

Текст цієї пояснювальної записки не є документом, у якому закріплене офіційне тлумачення цього Протоколу, однак його суть може полегшити застосування положень цього Протоколу. Цей Протокол було відкрито для підписання у Страсбурзі 8 листопада 2001 року з нагоди 109-ї сесії Комітету міністрів Ради Європи.

Вступ

1. Мета цього Протоколу полягає у вдосконаленні застосування принципів, що містяться у Конвенції Ради Європи про захист фізичних осіб стосовно автоматизованої обробки даних особистого характеру (ETS No.108, «Конвенція») шляхом надання двох самостійних положень, одне з яких стосується встановлення одного і більше органів нагляду кожної Стороною, а інше — транскордонних потоків даних особистого характеру до країн і організацій, які не є Сторонами цієї Конвенції.

2. Консультативний комітет, заснований статтею 18 Конвенції, підготував цей проект Протоколу на своєму 15-му засіданні, що відбувалося 16—18 червня 1999 року. Цей проект було подано Комітету міністрів за пропозицією Консультативного комітету для передачі на розгляд Парламентської Асамблеї. Консультативний комітет розглянув цей проект у світлі Висновків, прийнятих Асамблеєю 5 квітня 2000 року, а потім прийняв проект Протоколу на своєму 16-му засіданні, що проходило 6—8 червня 2000 року. Комітет міністрів схвалив цей додатковий Протокол 23 травня 2001 року.

КОМЕНТАРІ ЩОДО ПОЛОЖЕНЬ ПРОТОКОЛУ

Прембула

3. Вдосконалення процесу застосування принципів, викладених у Конвенції, стало необхідним у зв'язку з обміном даними особистого характеру між державами, які є Сторонами Конвенції, і державами або організаціями, які не є Сторонами Конвенції.

4. Таке збільшення потоку даних через державні кордони є наслідком все зростаючого обсягу міжнародного обміну інформацією у глобальному масштабі та технологічного прогресу і численних випадків його застосування. Саме тому потрібні постійні та одночасні зусилля, спрямовані на покращення ефективного захисту прав, що гарантуються Конвенцією. Ефективний захист, у свою чергу, вимагає міжнародної гармонізації не лише основних принципів захисту даних, а й, до певної міри, засобів їхнього впровадження у такій швидкозмінній і високотехнічній галузі, а також умов, на яких передача даних особистого характеру може здійснюватися через державні кордони.

5. Ефективне застосування принципів Конвенції робить необхідним і прийняття належних санкцій та засобів захисту (стаття 10). Більшість країн, які мають закони про захист даних, заснували органи нагляду, якими, як правило, є комісар, комісія, омбудсман чи генеральний інспектор. Такі органи нагляду з питань захисту даних забезпечують належні засоби захисту, якщо вони мають ефективні права та користуються справжньою незалежністю при виконанні своїх обов'язків. Вони стали важливою складовою у системі нагляду у сфері захисту даних у демократичному суспільстві.

6. Потік інформації знаходиться у самому центрі міжнародної співпраці. Однак ефективний захист особистого життя та даних особистого характеру також означає, що в принципі не повинно існувати транскордонних потоків даних особистого характеру до країн чи організацій, де захист таких даних не гарантується.

Стаття 1. Органи нагляду

Частина 1

7. Стаття 10 Конвенції вимагає закріплення належних засобів захисту у відповідних положеннях права кожної Сторони проти порушень положень національного законодавства, яким вводяться у дію принципи Конвенції. Однак це не є прямою вимогою до Сторін заснувати органи нагляду для здійснення моніторингу дотримання на їхній території положень, які вводять у дію принципи, викладені у главах II і III Конвенції і цьому Протоколі. Перша стаття цього Протоколу в цьому контексті має подвійну мету.

8. Вона спрямована на забезпечення ефективного захисту фізичної особи, вимагаючи від Сторін створити один або кілька органів нагляду, які б захищали права та свободи фізичної особи стосовно обробки даних особистого характеру. У конкретних умовах різних правових систем може бути потрібним більш ніж один орган нагляду. Ці органи можуть виконувати свої завдання без порушення компетенції правових та інших організацій, які відповідають за забезпечення дотримання положень національного права, що вводяться у дію принципи цієї Конвенції. Органи нагляду повинні мати відповідні технічні та людські ресурси (юристів, експертів з обчислювальної техніки) для вчинення негативних і ефективних дій на користь особи.

9. Ця Стаття також ставить на меті досягнути країною гармонізації норм, що регулюють діяльність органів нагляду, уже заснованих кожною Стороною цієї Конвенції. У принципі національне законодавство всіх Сторін Конвенції передбачає створення одного або більше органів нагляду. Однак, залежно від норм національних правових систем, їхній склад, повноваження та функціонування значно відрізняються у кожній країні.

10. Зазначена гармонізація спрямована не лише на вдосконалення рівня захисту даних кожною Стороною, а й на досягнення тіснішої співпраці між Сторонами без порушення системи співпраці, встановленої Конвенцією.

Частина 2

11. Сторони мають значну свободу щодо визначення повноважень зазначених органів для виконання ними їхніх завдань. Однак, відповідно до Протоколу, такі органи повинні мати принаймні повноваження розслідування та втручання, а також право участі у процесуальних діях або привернення уваги компетентних судових органів до порушень відповідних положень.

12. Такі органи повинні мати достатні повноваження для проведення розслідування, такі як можливість направити операторові запит про інформацію стосовно обробки даних особистого характеру та отримання їх. Така інформація має бути доступною, зокрема, у тих випадках, коли до органів нагляду звертається особа, яка прагне реалізувати свої права, що забезпечуються її національним законодавством, відповідно до статті 8 Конвенції.

13. Повноваження органу нагляду проводити розслідування може набувати різних форм у національному законодавстві. Наприклад, орган може бути наділений повноваженням зобов'язувати оператора файлів виправи-

¹ Або «контролерові файлів».

ти, стерти або знищити неточні або незаконно зібрані дані від власного імені або, якщо суб'єкт даних не може реалізувати такі права, від імені органу. Повноваження видавати приписи операторам, які не бажають передавати інформацію, що від них вимагається, у встановлені строки, мають бути частковим ефективним проявом повноваження здійснювати втручання. Це повноваження могло б включати можливість видавати висновки до проведення операцій з обробки даних або передавати справи на розгляд національних парламентів чи інших державних установ. Рекомендується, щоб орган нагляду мав повноваження інформувати громадськість за допомогою регулярних звітів, публікацій висновків або інших засобів інформування.

14. Здійснюючи захист індивідуальних прав, орган нагляду також є посередником між суб'єктом даних і оператором. У цьому контексті зається особливо важливим, щоб орган нагляду міг забезпечувати інформацію фізичним особам або користувачам даних щодо прав і зобов'язань, які стосуються захисту даних. Більше того, кожна особа повинна мати право подати претензії до органу нагляду щодо своїх прав і свобод стосовно обробки даних особистого характеру. Із причин, зазначених у пункті 7 Пояснювальної записки, подання таких претензій допомагає гарантувати право людини на належний захист правового захисту відповідно до статті 10 і ч. д статті 8 Конвенції. У положенні нагадується про те, що кожна особа має право на захист судового захисту. Однак національним законодавством може бути передбачено подання претензій до органу нагляду як умови використання такого засобу судового захисту.

15. Сторони повинні наділяти органи нагляду правом або участі у процесуальних діях, або привернення уваги судових органів до будь-яких порушень норм про захист даних. Це право є похідним від повноваження розслідування, що може допомогти такому органу розкрити порушення права особи на захист. Сторони можуть виконати зобов'язання щодо такого права, наділивши відповідний орган правом приймати рішення у справах.

16. Повноваження органу нагляду не обмежуються лише тими, що зазначені у ч. 2 статті 1. Слід пам'ятати про те, що Сторони мають інші засоби для забезпечення ефективної роботи органів нагляду. Асоціації могли б також подавати претензії до органів нагляду, зокрема, коли права осіб, яких вони представляють, обмежуються відповідно до статті 9 Конвенції. Орган нагляду міг би мати право проводити попередні перевірки легітимності операцій з обробки даних і підтримувати відкритість реєстру з обробки даних для громадськості. До органу нагляду могли б також звертатися з проханням надати висновки при підготовці законодавчих, регуляторних чи адміністративних заходів або кодексів поведінки, які стосуються обробки даних особистого характеру.

Частина 3

17. Органи нагляду не можуть ефективно гарантувати права і свободи фізичних осіб, якщо вони не виконують свої функції абсолютно незалежно

но². Кілька елементів забезпечують незалежність органу нагляду у виконанні ним своїх функцій. Цими елементами можуть бути склад органу, метод призначення його членів, тривалість повноважень і умови припинення виконання членами органу своїх функцій, забезпечення цих органів достатніми ресурсами або прийняття ними рішень, що не підпадають під дію зовнішніх наказів або приписів.

Частина 4

18. На противагу такій незалежності повинна забезпечуватися можливість оскаржувати спірні рішення органів нагляду в судовому порядку відповідно до принципу верховенства права.

19. Більше того, у випадках, коли орган нагляду не має судової компетенції, саме по собі втручання органу нагляду не перешкоджає особі звертатися з проханням надати їй захист у судовому порядку.

Частина 5

20. Посилення співпраці між органами нагляду повинно зробити внесок у рівень захисту при реалізації Сторонами цієї Конвенції. Ця співпраця доповнює взаємодопомогу, передбачену главою IV Конвенції та роботою Консультативного комітету. Її мета полягає у забезпеченні вищого рівня захисту відповідним особам. Все частіше люди зазнають безпосереднього впливу операцій з обробки даних, що не обмежуються межами однієї країни, а тому регулюються законами та знаходяться під наглядом органів більш ніж однієї країни. Прикладами цього є розвиток міжнародних електронних мереж і зростання транскордонних потоків даних у промислових підприємств та робочому середовищі. У такому контексті міжнародна співпраця між органами нагляду забезпечує можливість реалізації прав людини на міжнародному рівні, так само як і на національному.

Стаття 2. Транскордонні потоки даних особистого характеру, спрямовані до одержувача, який не підпадає під юрисдикцію Сторони цієї Конвенції

21. Стаття 12 Конвенції встановлює принцип вільного потоку даних особистого характеру між Сторонами, що підпадає під можливість обмеження її положень відповідно до підпункту 3. Це означає, зокрема, що принципи Конвенції було впроваджено.

22. Конвенція стосується транскордонних потоків даних особистого характеру до одержувача, який не підпадає під юрисдикцію будь-якої Сторони, лише опосередковано. Відповідно до ч. 3.b статті 12, країна може

² Стосовно процесуальних гарантій, викладених у статті 8 Європейської конвенції про захист прав і основних свобод людини, прецедентне право органів цієї Конвенції вже розглядає втручання незалежної організації, за певних обставин, як гарантію «ефективного нагляду» щодо потреби втручання державного органу влади при здійсненні прав, що забезпечується статтею 8 (Гаскін проти Сполученого Королівства (cf Gaskin vs United Kingdom), рішення від 7 липня 1989, серія А № 160, § 49).

відійти від принципу вільного обміну інформацією між її територією та одержувачем, який не підпадає під юрисдикцію будь-якої Сторони через іншу Сторону, щоб уникнути порушення законодавства Сторони походження інформації шляхом здійснення такої передачі даних. Тому не існує конкретних положень щодо транскордонних потоків даних стосовно держав чи організацій, які не є сторонами цієї Конвенції.

23. Це означає, що Сторони Конвенції можуть вносити у свої правові системи положення, які прямо дозволяють здійснення передачі дані особистого характеру одержувачеві, який не підпадає під юрисдикцію певної Сторони та має інший рівень захисту, ніж у Конвенції. У той час, коли готувався проект цього Протоколу, навіть не будучи під прямим зобов'язанням, деякі Сторони запровадили у свої національні правові системи норми щодо передачі даних одержувачеві, який не підпадає під юрисдикцію певної Сторони. Розбіжності у практиці, зокрема у світлі згаданої вище ч. 3, в статті 12, можуть призвести до значних обмежень на вільний обмін даними між Сторонами, що також суперечило б цілі цієї Конвенції. Тому необхідно, у контексті конкретних положень Рекомендації Ради Європи щодо захисту даних, встановлювати спільні норми щодо транскордонних потоків даних особистого характеру одержувачеві, який не підпадає під юрисдикцію певної Сторони.

24. Такий захід визнається, з одного боку, бажанням гарантувати ефективний захист даних особистого характеру поза межами державних кордонів, а з іншого — рішучою переконаністю Сторін забезпечити вільний обмін інформацією між народами відповідно до формулювань Преамбули цієї Конвенції.

Частина 1

25. Транскордонні потоки даних до одержувача, який не підпадає під юрисдикцію певної Сторони, мають відповідати умовам належного рівня захисту в країні чи організації, що одержує таку інформацію. Пункт 70 Пояснювальної записки до Конвенції посиляється на «Держави, які не підписали Конвенцію, із достатнім режимом захисту даних». Одержувач, який не підпадає під юрисдикцію будь-якої Сторони Конвенції, може розглядатися як такий, що має достатній режим захисту даних лише, якщо він забезпечує належний рівень захисту.

26. Належний рівень захисту повинен оцінюватися у світлі всіх обставин здійснення передачі даних.

27. Рівень захисту оцінюється на основі конкретних прикладів для кожної здійсненої передачі або категорії передач. Таким чином, мають переважити обставини передачі та, зокрема, вид даних, цілі та тривалість обробки, для якої передаються дані, країна походження та країна остаточного призначення, загальні та галузеві норми закону, що застосовується у відповідній країні чи організації, а також професійні правила та норми безпеки, що вони застосовують.

28. Оцінка належності може в подібний спосіб проводитися для всієї країни чи організації, дозволяючи таким чином здійснювати усі передачі у

Додатковий протокол № 181 до Конвенції про захист осіб...

такі пункти призначення. У цьому випадку належний рівень захисту визнається компетентними органами кожної Сторони.

29. Оцінка належного рівня захисту повинна враховувати принципи глави II Конвенції та цього Протоколу, а також рівень забезпечення цих принципів у країні чи організації, що отримує дані (тією мірою, якою вони стосуються конкретного випадку передачі), а також як суб'єкт даних може захищати свої інтереси в разі недоотримання норм у певному конкретному випадку.

30. Консультативний комітет Конвенції може на вимогу однієї зі Сторін давати свої висновки щодо належності рівня захисту даних у третій країні чи організації.

Частина 2, а

31. Сторони мають свободу у визначенні рівня відходу від принципів належного рівня захисту. Відповідні положення національного законодавства повинні, однак, поважати принцип, закладений у європейському праві про те, що положення про винятки тлумачаться обмежено, щоб уникнути перетворення винятку на правило. Таким чином, винятки можуть вноситися у національне законодавство з огляду на легітимні домінуючі інтереси. Це можуть бути бажання захистити важливі публічні інтереси, такі, як зазначено у контексті ч. 2 статті 8 Європейської конвенції з прав людини і ч. 2 статті 9 Конвенції ETS № 108; подання або захист законних претензій; або вибірка даних з публічного реєстру. Винятки можуть також робитися для конкретних інтересів суб'єкта даних, наприклад щодо виконання контракту з суб'єктом даних або у його інтересах, або для захисту його життєвого інтересу, або коли він дає свою згоду. У такому випадку перед наданням згоди суб'єкт даних має бути поінформований відповідним чином про заплановану передачу даних.

Частина 2, б

32. Кожна Сторона може передбачити передачу даних особистого характеру одержувачеві, який не підпадає під юрисдикцію будь-якої Сторони та не забезпечує належний рівень захисту, за умови, що особа, відповідальна за передачу, забезпечить належні гарантії. Ці гарантії повинні бути визнані належними компетентними органами нагляду відповідно до норм національного законодавства. Такими гарантіями, зокрема, можуть бути договірні положення, які мають обов'язкову дію для оператора, що здійснює передачу, та одержувача, який не підпадає під юрисдикцію будь-якої Сторони.

33. Зміст таких контрактів повинен включати відповідні елементи захисту даних. Більше того, у процедурному сенсі, згідно з договірними умовами, суб'єкт даних, наприклад, міг би мати контактну особу серед кадрового персоналу особи, відповідальної за здійснення передачі, чие завдання полягає у забезпеченні дотримання дійсних стандартів захисту. Такий суб'єкт може вільно і безкоштовно контактувати з такою особою у будь-який час та, де доцільно, отримувати допомогу в реалізації ним своїх прав.

Стаття 3. Закріплені положення

34. Відповідно до практики укладення міжнародних конвенцій у Раді Європи додатковий Протокол до Конвенції може бути підписаний лише Сторонами, які підписали саму Конвенцію. Європейського Співтовариства, які брали участь у розробці цього Протоколу, можуть підписати цей Протокол після приєднання до Конвенції відповідно до умов, викладених у ній.

35. Частина 2 статті 3 застосовується лише до держав-членів Ради Європи і Європейського Співтовариства. Частина 4 застосовується лише до держав, які не входять до Ради Європи, але можуть лише приєднатися до Протоколу, так само як і до самої Конвенції.

36. Частина 3 закріплює вимогу, що кількість ратифікацій, необхідних для набуття чинності цим Протоколом, має дорівнювати п'яти, що відповідає положенням статті 22 Конвенції.

37. Положення частин 3—6 відповідають заключним положенням Конвенції, а також традиційним заключним положенням, що містяться у конвенціях і протоколах Ради Європи.

КОНВЕНЦІЯ РАДИ ЄВРОПИ ПРО КІБЕРЗЛОЧИННИ № 185 (Прийнято 23 листопада 2001 р.)

Преамбула

Держави-члени Ради Європи та інші держави, які підписали цю Конвенцію,

вважаючи, що метою Ради Європи є досягнення більшої єдності між її членами;

визнаючи цінність налагодження співробітництва з іншими державами, які є Сторонами цієї Конвенції;

впевнені у першочерговій необхідності спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, крім іншого, шляхом створення відповідного законодавства і налагодження міжнародного співробітництва;

усвідомлюючи глибокі зміни, спричинені переходом на цифрові технології, конвергенцією і глобалізацією комп'ютерних мереж, яка продовжується;

стурбовані ризиком того, що комп'ютерні мережі та електронна інформація може також використовуватися для вчинення кримінальних правопорушень, і того, що докази, пов'язані з такими правопорушеннями, можуть зберігатися і передаватися такими мережами;

визнаючи необхідність співробітництва між державами і приватними підприємствами для боротьби проти кіберзлочинності і необхідність захисту законних інтересів в ході використання і розвитку інформаційних технологій;

вважаючи, що ефективна боротьба проти кіберзлочинності вимагає більшого, швидкого і ефективного функціонуючого міжнародного співробітництва у кримінальних питаннях; впевнені, що ця Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, і надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо надійного міжнародного співробітництва;

пам'ятаючи про необхідність забезпечити належний баланс між правохоронними інтересами і повагою до основних прав людини, як це передбачено Конвенцією Ради Європи про захист прав людини і основних свобод 1950 р., Міжнародною хартією ООН про громадянські і політичні права 1966 р. та іншими відповідними міжнародними угодами з прав людини, які підтверджують право кожного безперешкодно отримуватись поглядів, а також право на свободу слова, включаючи право на пошук, отримання й передачу будь-якої інформації та ідей, незважаючи на кордони, а також права на повагу до приватного життя;

також пам'ятаючи про захист особистої інформації, як це передбачено Конвенцією Ради Європи про захист осіб стосовно автоматичної обробки даних 1981 р.;

посилаючись на Конвенцію ООН про права дитини 1989 р. і Конвенцію МОП про найгірші форми дитячої праці 1999 р.;

беручи до уваги існуючі конвенції Ради Європи про співробітництво у кримінальній сфері і подібні угоди, що існують між державами-членами Ради Європи та іншими державами, і підкреслюючи, що ця Конвенція має на меті доповнення цих конвенцій для підвищення ефективності кримінальних розслідувань і переслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, і для надання можливості збирання доказів, що стосуються кримінального злочину, в електронній формі;

вітаючи нешодавні події, які сприяють міжнародному порозумінню і співробітництву у боротьбі з кіберзлочинністю, включаючи заходи ООН, ОЕСР, ЄС і «Великої вісімки»;

посилаючись на Рекомендацію № R (85) 10, що стосується практичного застосування Європейської конвенції про взаємодопомогу у кримінальних справах стосовно листів, які створюють необхідність переходження телекомунікацій, Рекомендацію № R (88) 2, про піратство у сфері авторських і суміжних прав, Рекомендацію № R (87) 15, яка регулює використання особистих даних у поліцейській галузі, Рекомендацію № R (95) 4 про захист особистих даних у сфері телекомунікаційних послуг, з особливим посиленням на телефонні послуги, а також на Рекомендацію № R (89) 9 про злочини, пов'язані з комп'ютерами, яка надає орієнтири для національного законодавства щодо визначення певних комп'ютерних злочинів і Рекомендацію № R (95) 13, що стосується проблем кримінально-процесуального права, пов'язаних з інформаційними технологіями;

посилаючись на Резолюцію № 1, прийняту європейськими міністрами юстиції на своїй 21-й Конференції (Прага, червень 1997 р.), яка рекомендувала Комітету міністрів підтримати роботу, що проводиться Європейським комітетом з проблем злочинності (ЄКПЗ) щодо кіберзлочинності для зближення положень внутрішньодержавних положень кримінального права і створення можливостей для застосування ефективних заходів розслідування таких правопорушень, а також на Резолюцію № 3, прийняту на 23-й Конференції європейських міністрів юстиції (Лондон, червень 2000 р.), яка заохочувала сторони переговорів до пошуку відповідних рішень для надання можливості якомога більшій кількості держав стати учасниками цієї Конвенції, і визнавала необхідність швидкодіючої і ефективної системи міжнародного співробітництва, яка б належним чином враховувала специфічні вимоги боротьби проти кіберзлочинності;

також посилаючись на План дій, прийнятий головами держав та урядів Ради Європи з нагоди їх Другого саміту (Страсбург, 10—11 жовтня 1997 р.), для пошуку спільних відповідей на розвиток нових інформаційних технологій, які базуються на стандартах і цінностях Ради Європи;

погодилися про таке:

Конвенція Ради Європи про кіберзлочини

Розділ I

ВИКОРИСТАННЯ ТЕРМІНІВ

Стаття 1. Визначення

Для цілей цієї Конвенції:

а) **«комп'ютерна система»** означає будь-який пристрій або групу взаємно поєднаних чи пов'язаних пристроїв, один чи більше з яких, відповідно до певної програми, виконують автоматичну обробку даних;

б) **«комп'ютерні дані»** означає будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою;

с) **«постачальник послуг»** означає:

- i) будь-яку державну або приватну установу, яка надає користувачам своїх послуг можливість комунікацій за допомогою комп'ютерної системи; та
- ii) будь-яка інша установа, яка обробляє або зберігає комп'ютерні дані від імені такої послуги або користувачів такої послуги.

д) **«дані про рух інформації»** означає будь-які комп'ютерні дані, пов'язані з комунікацією за допомогою комп'ютерної системи, які були створені комп'ютерною системою, яка складала частину ланки комунікації, і які зазначають походження, кінцевий пункт, шлях, час, дату, розмір і тривалість інформації або тип основної послуги.

Розділ II

ЗАХОДИ, ЯКІ МАЮТЬ ЗДІЙСНОВАТИСЯ НА НАЦІОНАЛЬНОМУ РІВНІ

Частина I

МАТЕРІАЛЬНЕ КРИМІНАЛЬНЕ ПРАВО

Заголовок I

Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем

Стаття 2. Незаконний доступ

Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисний доступ до цілої комп'ютерної системи або її частини без права на це. Сторона може вимагати, щоб [для встановлення кримінальної відповідальності] таке правопорушення було вчинене шляхом порушення заходів безпеки з метою отримання комп'ютерних даних, або з іншою недобросовісною метою,

або стосовно до комп'ютерної системи, поєднаної з іншою комп'ютерною системою.

Стаття 3. Нелегальне перехоплення

Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електронні випромінювання комп'ютерної системи, яка містить у собі такі комп'ютерні дані. Сторона може вимагати, щоб [для встановлення кримінальної відповідальності. — *Прим. пер.*] таке правопорушення було вчинене з недобросовісною метою або стосовно комп'ютерної системи, поєднаної з іншою комп'ютерною системою.

Стаття 4. Втручання у дані

1. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це.

2. Сторона може залишити за собою право вимагати, щоб [для встановлення кримінальної відповідальності] поведінка, описана у пункті 1, завдала серйозну шкоду.

Стаття 5. Втручання в систему

Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це.

Стаття 6. Зловживання пристроями

1. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це:

- а) виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином:
- і) пристроїв, включаючи комп'ютерні програми, створених або адаптованих для використання, в першу чергу, для вчинення будь-якого зі злочинів, перелічених у статтях 2—5;
- ii) комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до всієї комп'ютерної

системи або її частини з наміром використання її для вчинення будь-якого зі злочинів, перелічених у статтях 2—5; та володіння предметом, вказаним у параграфах (а)(1) або (2) вище, з наміром його використання для вчинення будь-якого зі злочинів, перелічених у статтях 2—5. Сторона може передбачити у законодавстві, що для встановлення кримінальної відповідальності необхідно володіти певною кількістю таких предметів.

2. Ця стаття не стосується як така, що встановлює кримінальну відповідальність у разі, якщо виготовлення, продаж, придбання для використання, розповсюдження чи надання для використання іншим чином або володіння, зазначені у пункті 1 цієї статті, не призначені для вчинення будь-якого зі злочинів, перелічених у статтях 2—5 цієї Конвенції, такі як дозволене впровадження або захист комп'ютерної системи.

3. Кожна Сторона може залишити за собою право не застосовувати частину 1 цієї статті за умови, що таке застереження не стосується продажу, розповсюдження або надання для використання іншим чином предметів, перелічених у параграфі 1(а)(2).

Заголовок 2 Правопорушення, пов'язані з комп'ютерами

Стаття 7. Підробка, пов'язана з комп'ютерами

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважалися або відповідно до них проводилися б дії, як з дійсними, незалежно від того, чи можна такі дані прямо прочитати і зрозуміти, чи ні. Сторона може вимагати наявності наміру обману або подібної нечесної поведінки для встановлення кримінальної відповідальності.

Стаття 8. Шахрайство, пов'язане з комп'ютерами

Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом:

- а) будь-якого введення, зміни, знищення чи приховування комп'ютерних даних;
- б) будь-якого втручання у функціонування комп'ютерної системи з шахрайською або нечесною метою здобуття, без права на це, економічних переваг для себе чи іншої особи.

Заголовок 3**Правопорушення, пов'язані зі змістом [інформації]****Стаття 9. Правопорушення, пов'язані з дитячою порнографією**

1. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності у відповідності до її внутрішнього законодавства за намісне вчинення, без права на це, таких дій:

- a) виготовлення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем;
 - b) пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем;
 - c) розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем;
 - d) одержання дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи;
 - e) володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації.
2. Для цілей пункту 1 вище «дитяча порнографія» включає в себе порнографічний матеріал, який візуально зображує:
- a) неповнолітню особу, задіяну у явно сексуальній поведінці;
 - b) особу, яка виглядає як неповнолітня особа, задіяну у явно сексуальній поведінці;
 - c) реалістичні зображення неповнолітньої особи, задіяної у явно сексуальній поведінці.
3. Для цілей пункту 2 вище термін «неповнолітня особа» включає в себе всіх осіб до 18 років. Сторона може, однак, передбачити нижчий віковий поріг, який має бути не меншим за 16 років.
4. Кожна Сторона може залишити за собою право не застосовувати, частково чи повністю, параграфи 1(d), 1(e), 2(b) та 2(c).

Заголовок 4**Правопорушення, пов'язані з порушенням авторських та суміжних прав****Стаття 10. Правопорушення, пов'язані з порушенням авторських та суміжних прав**

1. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення авторських прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Паризьким актом 24 липня 1971 р. щодо Бернської конвенції про захист літературних та художніх творів. Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про авторське право, за винятком будь-яких моральних прав, які надаються такими конвенціями,

у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.

2. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення суміжних прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Римською міжнародною конвенцією про захист виконавців, виробників фонограм і організації мовлення (Римська конвенція), Угодою про торговельні аспекти прав інтелектуальної власності і Угодою ВОІВ про виконання і фонограми, за винятком будь-яких моральних прав, які надаються такими конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.

3. Кожна Сторона може залишити за собою право не встановлювати кримінальну відповідальність відповідно до пунктів 1 і 2 цієї статті в обмежених випадках, за умови існування інших ефективних засобів впливу і за умови того, що таке застереження не порушує міжнародних зобов'язань Сторони відповідно до міжнародних документів, на які містяться посилання у пунктах 1 і 2 цієї статті.

Заголовок 5**Додаткова відповідальність і санкції****Стаття 11. Спроба і допомога або співучасть**

1. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за намісну спробу вчинити будь-який зі злочинів, передбачених у статтях 3—5, 7, 8, 9 (1) а та 9 (1) с цієї Конвенції. Частина у вчиненні будь-якого зі злочинів, передбачених у статтях 2—10 цієї Конвенції з метою вчинення такого злочину.

2. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за намісну спробу вчинити будь-який зі злочинів, передбачених у статтях 3—5, 7, 8, 9 (1) а та 9 (1) с цієї Конвенції.

3. Кожна Сторона може залишити за собою право не застосовувати, повністю або частково, пункт 2 цієї статті.

Стаття 12. Корпоративна відповідальність

1. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для забезпечення того, щоб юридична особа могла нести відповідальність за кримінальне правопорушення, встановлене відповідно до цієї Конвенції, яке було вчинене на її користь будь-якою фізичною особою, як індивідуально, так і як частиною органу такої юридичної особи. Така фізична особа має обіймати керівну посаду в рамках юридичної особи, на підставі:

- a) повноважень на представлення цієї юридичної особи;

- б) повноважень приймати рішення від імені цієї юридичної особи;
 - с) повноважень здійснювати контроль у рамках цієї юридичної особи.
2. Окрім випадків, уже передбачених у пункті 1, кожна Сторона вживає заходів для забезпечення того, щоб юридична особа могла понести відповідальність у разі, коли недостатній нагляд чи контроль, який мав здійснюватися особою, вказаною у пункті 1, створив можливість вчинення кримінального правопорушення, встановленого відповідно до цієї Конвенції, на користь цієї юридичної особи фізичною особою, яка діяла під її контролем.
3. Відповідно до юридичних принципів Сторони, відповідальність юридичної особи може бути кримінальною, цивільною або адміністративною.
4. Така відповідальність не впливає на кримінальну відповідальність фізичних осіб, які вчинили правопорушення.

Стаття 13. Санкції і заходи

1. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для забезпечення того, щоб кримінальні правопорушення, встановлені відповідно до статей 2–11, каралися ефективно, пропорційними і переконливими санкціями, включаючи позбавлення волі.
2. Кожна Сторона забезпечує, щоб юридичні особи, які несуть відповідальність відповідно до статті 12, каралися ефективно, пропорційними і переконливими кримінальними або некримінальними санкціями, включаючи грошові санкції.

Частина 2 ПРОЦЕДУРНЕ ПРАВО

Заголовок 1

Загальні положення

Стаття 14. Сфера процесуальних положень

1. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для визначення повноважень і процедур, передбачених цією частиною, з метою конкретних кримінальних розслідувань або переслідувань.
2. За винятком обставин, конкретно передбачених статтею 21, кожна Сторона застосовує повноваження і процедури, передбачені у пункті 1, до:
 - а) кримінальних правопорушень, встановлених відповідно до статей 2–11 цієї Конвенції;
 - б) інших кримінальних правопорушень, вчинених за допомогою комп'ютерних систем; та
 - с) збору доказів у електронній формі по кримінальному правопорушенню.
3. а) Кожна Сторона може залишити за собою право вживати заходів, які містяться у статті 20, тільки до правопорушень або до кате-

горій правопорушень, зазначених у застереженні, за умови, що обсяг таких правопорушень або категорій правопорушень не менший за обсяг правопорушень, до яких вона вживає заходів, які містяться у статті 21. Кожна Сторона розгляне можливість обмеження такого застереження з метою якомога ширшого застосування заходів, які містяться у статті 20.

б) Якщо Сторона внаслідок обмежень, встановлених її чинним законодавством під час прийняття цієї Конвенції, не може вживати заходів, передбачених у статтях 20 і 21, до комунікацій, які передаються всередині комп'ютерної системи постачальника послуг, причому така система і використовується на користь зарплатної групи користувачів, та не використовує мережі зв'язку загального доступу, і не пов'язана з іншою комп'ютерною системою, відкритою для загального доступу чи приватною, то така Сторона може залишити за собою право не вживати цих заходів до таких комунікацій. Кожна Сторона розгляне можливість обмеження такого застереження з метою якомога ширшого вживання заходів, які містяться у статтях 20 і 21.

Стаття 15. Умови і запобіжні заходи

1. Кожна Сторона забезпечує, щоб встановлення, імплементація і застосування повноважень і процедур, які містяться у цій частині, регулювалися умовами і запобіжними заходами, передбаченими її внутрішньодержавним правом, які б забезпечували адекватний захист прав і свобод людини, включаючи права, що випливають із зобов'язань за Конвенцією Ради Європи про захист прав людини і основних свобод 1950 р., Міжнародною хартією ООН про громадянські і політичні права 1966 р. та іншими відомими міжнародними угодами з прав людини, і які б включали в себе принципи пропорційності.

2. Такі умови і запобіжні заходи включатимуть, між іншим, як це є доцільним з огляду на природу відповідного повноваження або процедури, судовий або інший незалежний нагляд, підстави, які виправдовують застосування, і обмеження сфери застосування і терміну таких повноважень або процедур.

3. Тією мірою, як це відповідає суспільним інтересам, зокрема, належному управлінням правосуддя, Сторони розглядають вплив повноважень і процедур, які містяться у цій частині, на права, відповідальність і законні інтереси третіх сторін.

Заголовок 2

Загальні положення

Стаття 16. Термінове збереження комп'ютерних даних, які зберігаються

1. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для надання можливості своїм компетентним

органам видавати накази або іншим подібним шляхом спричинити термінове збереження зазначених комп'ютерних даних, включаючи дані про рух інформації, які зберігалися за допомогою комп'ютерної системи, зокрема у разі, коли існують підстави вважати, що такі комп'ютерні дані особливим чином вразливі до втрати чи модифікації.

2. Якщо Сторона застосовує пункт 1 вище шляхом ордеру особі, яким така особа зобов'язується зберігати зазначені комп'ютерні дані, які зберігаються і перебувають у власності або під контролем такої особи, то Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для того, щоб зобов'язати таку особу зберігати і підтримувати цілісність таких комп'ютерних даних протягом такого періоду, який буде необхідним для того, щоб компетентні органи мали можливість отримати дозвіл на їх розкриття, з максимальним терміном у 90 днів. Сторона може передбачити можливість наступного продовження терміну дії такого ордеру.

3. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для того, щоб зобов'язати особу, яка має зберігати комп'ютерні дані, зберігати конфіденційність факту проведення таких процедур протягом періоду, визначеного внутрішньодержавним законодавством.

4. Повноваження і процедури, на які містяться посилення у цій статті, регулюються положеннями статей 14 і 15.

Стаття 17. Термінове збереження і часткове розкриття даних про рух інформації

1. Кожна Сторона вживає стосовно даних про рух інформації, які мають зберігатися відповідно до статті 16, таких законодавчих та інших заходів, які можуть бути необхідними для:

- а) забезпечення того, щоб таке термінове збереження даних про рух інформації могло проводитися, незважаючи на те, що один чи більше поставальників послуг було залучено до передачі такої інформації; та
 - б) забезпечити термінове розкриття компетентному органіві Сторони або особі, призначеній таким органом, обсягу даних про рух інформації, достатнього для ідентифікації поставальників послуг і шлях, яким була передана інформація.
2. Повноваження і процедури, на які містяться посилення у цій статті, регулюються положеннями статей 14 і 15.

Заголовок 3

Порядок представлення

Стаття 18. Порядок представлення

1. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для надання повноважень своїм компетентним органам видавати накази:

а) особі, яка знаходиться на її території, — про надання зазначених комп'ютерних даних, якими така особа володіє або контролює і які зберігаються у комп'ютерній системі або на комп'ютерному носії інформації; та

б) поставальникові послуг, який пропонує свої послуги на території Сторони — про надання інформації про користувача послуг, пов'язаної з такими послугами, яка перебуває у власності або під контролем такого поставальника послуг.

2. Повноваження і процедури, на які містяться посилення у цій статті, регулюються положеннями статей 14 і 15.

3. Для цілей цієї статті «інформація про користувача послуг» означає будь-яку інформацію, у формі комп'ютерних даних чи у іншій формі, яка перебуває у поставальника послуг, відноситься до користувачів його послуг і не є даними про рух даних або власне даними змісту інформації [з якою працювали користувачі послуг] за допомогою яких можна встановити:

- а) тип комунікаційної послуги, яка використовувалася, її технічні положення і період користування послугою;
- б) особистість користувача послуг, поштову або географічну адресу, телефони та іншу інформацію про номер доступу, рахунки і платежі, яку можна отримати за допомогою угоди або домовленості про поставання послуг;
- в) будь-яку іншу інформацію про місце встановлення комунікаційного обладнання, яку можна отримати за допомогою угоди або домовленості про поставання послуг.

Заголовок 4

Обшук і арешт комп'ютерних даних, які зберігаються

Стаття 19. Обшук і арешт комп'ютерних даних, які зберігаються

1. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для надання повноважень своїм компетентним органам для обшуку або подібного доступу до:

- а) комп'ютерної системи або її частини і комп'ютерних даних, які зберігаються в ній; та
 - б) комп'ютерного носія інформації, на якому можуть зберігатися комп'ютерні дані, на її території.
2. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для забезпечення того, щоб у разі, коли її компетентні органи здійснюють обшук або подібний доступ до конкретної комп'ютерної системи або її частини відповідно до параграфа 1 (а), і мають підстави вважати, що дані, які розшукуються, зберігаються в іншій комп'ютерній системі чи її частині, яка знаходиться на її території, і до таких даних можна здійснити законний доступ чи вони є доступними першій системі, такі компетентні органи мали право терміново поширити обшук або подібний доступ на іншу систему.

3. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для надання своїм компетентним органам повноважень арештовувати або виняти подібні дії щодо комп'ютерних даних, до яких був здійснений доступ відповідно до параграфа 1 або [так у тексті]. Такі заходи включатимуть повноваження на:

- а) арешт або подібні дії щодо комп'ютерної системи чи її частини або комп'ютерного носія інформації;
 - б) копіювання і збереження копії таких комп'ютерних даних;
 - с) збереження цілісності відповідних збережених комп'ютерних даних; та
 - д) заборону доступу або вилучення цих комп'ютерних даних з комп'ютерної системи, до якої здійснювався доступ.
4. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для надання своїм компетентним органам повноважень вимагати від будь-якої особи, яка знає про функціонування комп'ютерної системи, або про заходи, які були здійснені для захисту комп'ютерних даних, які містяться у ній, надавати відповідну необхідну інформацію для проведення дій, які містяться у параграфах 1 і 2.
5. Повноваження і процедури, на які містяться посилення у цій статті, регулюються положеннями статей 14 і 15.

Заголовок 5

Збирання комп'ютерних даних у реальному масштабі часу

Стаття 20. Збирання даних про рух інформації у реальному масштабі часу

1. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для надання своїм компетентним органам повноважень:

- а) збирати або записувати технічними засобами на території такої Сторони; та
- б) зобов'язувати постачальника послуг, в межах його існуючих технічних повноважень:
 - і) збирати або записувати технічними засобами на території такої Сторони; або
 - ii) співпрацювати і допомагати компетентним органам у зборі або запису даних про рух інформації у реальному масштабі часу, які пов'язані з визначеною передачею інформації на її території, яка передається за допомогою комп'ютерних систем.

2. Якщо Сторона, через встановлені принципи її юридичної системи, не може вжити заходів, на які містяться посилення у параграфі 1 (а), вона замість цього може вжити таких законодавчих та інших заходів, які можуть бути необхідними для забезпечення збору або запису даних про рух інформації у реальному масштабі часу, які пов'язані з визначеною передачею інформації на її території, шляхом застосування технічних засобів на такій території.

3. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для того, щоб зобов'язати постачальника послуг зберігати конфіденційність факту і будь-якої інформації про використання будь-якого з повноважень, зазначених у цій статті.

4. Повноваження і процедури, на які містяться посилення у цій статті, регулюються положеннями статей 14 і 15.

Стаття 21. Переохочення даних змісту інформації

1. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними стосовно певних серйозних злочинів, які визнаються внутрішньодержавним законодавством, для надання повноважень своїм компетентним органам:

- а) збирати або записувати технічними засобами на території такої Сторони; та
 - б) зобов'язувати постачальника послуг в межах його існуючих технічних повноважень:
 - і) збирати або записувати технічними засобами на території такої Сторони; або
 - ii) співпрацювати і допомагати компетентним органам у зборі або запису даних змісту інформації у реальному масштабі часу, які належать до визначеної передачі інформації на її території, яка здійснюється шляхом комп'ютерної системи.
2. Якщо Сторона, через встановлені принципи її юридичної системи, не може вживати заходів, на які містяться посилення у параграфі 1 (а), вона замість цього може вжити таких законодавчих та інших заходів, які можуть бути необхідними для забезпечення збору або запису даних змісту інформації у реальному масштабі часу, які належать до визначеної передачі інформації на її території, шляхом застосування технічних засобів на такій території.
3. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для того, щоб зобов'язати постачальника послуг зберігати конфіденційність факту і будь-якої інформації про використання будь-якого з повноважень, зазначених у цій статті.
4. Повноваження і процедури, на які містяться посилення у цій статті, регулюються положеннями статей 14 і 15.

Частина 3 ЮРИСДИКЦІЯ

Стаття 22. Юрисдикція

1. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для встановлення юрисдикції стосовно будь-якого злочину, встановленого відповідно до статей 2—11 цієї Конвенції, у випадках, коли таке правопорушення вчинене:

- a) на її території; або
- b) на борту судна, яке плаває під прапором такої Сторони; або
- c) на борту літака, зареєстрованого відповідно до законів такої Сторони; або
- d) одним з її громадян, якщо таке правопорушення карається кримінальним законодавством у місці його вчинення, або якщо правопорушення вчинено поза межами територіальної юрисдикції будь-якої Держави.

2. Кожна Держава може залишити за собою право не застосовувати або застосовувати лише в окремих випадках або за окремих умов правила юрисдикції, викладені у параграфах 1(b) — 1(d) цієї статті або у будь-якій їх частині.

3. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для встановлення юрисдикції стосовно злочинів, встановлених відповідно до пункту 1 статті 24 цієї Конвенції, у випадках, коли підозрюваний правопорушник перебуває на її території і не передається іншій Стороні лише на підставі його громадянства після запиту про екстрадицію.

4. Ця Конвенція не виключає будь-якої кримінальної юрисдикції, здійсненої відповідно до внутрішньодержавного законодавства.

5. Якщо більш ніж одна Сторона заявляє про юрисдикцію стосовно підозрюваного правопорушення, встановленого відповідно до цієї Конвенції, зацікавлені Сторони, де це можливо, проводять консультації з метою визначення найбільш придатної для переслідування юрисдикції.

Розділ III МІЖНАРОДНЕ СПІВРОБІТНИЦТВО

Частина I ЗАГАЛЬНІ ПРИНЦИПИ

Заголовок I Загальні принципи міжнародного співробітництва

Стаття 23. Загальні принципи міжнародного співробітництва

Сторони співпрацюють між собою у найширших обсягах відповідно до принципів цього розділу шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства, з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами, і даними або з метою збирання доказів у електронній формі, які стосуються правопорушень.

Заголовок 2 Принципи екстрадиції

Стаття 24. Екстрадиція

1. a) Ця стаття застосовується до екстрадиції, що має місце між Сторонами у зв'язку з кримінальними правопорушеннями, встановленими відповідно до статей 2—11 цієї Конвенції, за умови, що вони підлягають покаранню позбавленням волі, максимальний строк якого становить щонайменше один рік, або більш суворому покаранню, відповідно до законодавства обох зацікавлених Сторін.

b) У випадках, коли відповідно до домовленості, укладеної на основі єдиного чи взаємного законодавства або договору про екстрадицію, включаючи Європейську конвенцію про екстрадицію (ETS No.24), які застосовуються між двома або більше сторонами, має застосовуватися різне мінімальне покарання, застосовується мінімальне покарання відповідно до такої домовленості чи угоди.

2. Кримінальні правопорушення, описані у пункті 1 цієї статті, вважаються такими, що включаються як правопорушення, які спричиняють екстрадицію, до будь-якої угоди про екстрадицію, яка існує між Сторонами. Сторони зобов'язуються включати такі правопорушення як такі, що спричиняють екстрадицію, до будь-якого договору про екстрадицію, який буде укладено між ними.

3. Якщо Сторона, яка здійснює екстрадицію відповідно до існуючого договору, отримує запит про екстрадицію від іншої Сторони, з якою в неї нема договору про екстрадицію, вона може вважати цю Конвенцію юридичною основою для екстрадиції щодо будь-якого кримінального правопорушення, на яке міститься посилення у пункті 1 цієї статті.

4. Сторони, які не здійснюють екстрадицію відповідно до існуючого договору, визнають для себе кримінальні правопорушення, на які міститься посилення у пункті 1 цієї статті, такими, що спричиняють екстрадицію.

5. Екстрадиція підлягає умовам, які містяться у законодавстві Сторони, яку запитують про екстрадицію, або у відповідних договорах про екстрадицію, включаючи підстави, на яких Сторона, яку запитують, може відмовити в екстрадиції.

6. Якщо в екстрадиції стосовно кримінального правопорушення, на яке міститься посилення у пункті 1 цієї статті, відмовлено виключно на підставі громадянства особи, стосовно якої надходить запит про екстрадицію, або тому, що Сторона, яку запитують, вважає, що вона має юрисдикцію стосовно такого правопорушення, то Сторона, яку запитують, на запит Сторони, яка запитує, надсилає справу своїм компетентним органам з метою переслідування правопорушення і належним чином повідомляє його результати Стороні, яка запитує. Такі органи приймають свої рішення і проводять свої розслідування і переслідування таким же чином, як і у випадку будь-якого іншого правопорушення подібної природи відповідно до законодавства такої Сторони.

7. а) Кожна Сторона під час підписання або передачі документа про ратифікацію, прийняття, затвердження чи приєднання повідомляє Генеральному секретареві Ради Європи назви й адреси всіх компетентних органів, які відповідають за надсилення чи отримання запитів про екстрадицію або тимчасовий арешт у випадку відсутності договору.
- б) Генеральний секретар Ради Європи створює і вносить відповідні зміни у реєстр компетентних органів, відповідно до призначених Сторонами. Кожна Сторона забезпечує правильність відомостей, які містяться у такому реєстрі.

Заголовок 3

Загальні принципи взаємної допомоги

Стаття 25. Загальні принципи взаємної допомоги

1. Сторони надають одна іншій взаємну допомогу у найширшому обсязі з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними або з метою збирання доказів у електронній формі щодо кримінального правопорушення.
2. Кожна Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для виконання зобов'язань, що містяться у статтях 27–35.
3. Кожна Сторона за надзвичайних умов може зробити запит про взаємну допомогу або про повідомлення, пов'язані з такою допомогою, які здійснюються терміновими засобами комунікації, включаючи факс і електронну пошту, у тому обсязі, у якому такі засоби комунікації можуть забезпечити належні форми безпеки і підтвердження достовірності (включаячи використання кодування, де це необхідно), за яким має слідувати формальне підтвердження, якщо таке вимагається Стороною, яку запитують. Сторона, яку запитують, приймає і відповідає на запит шляхом будь-якого з таких термінових засобів комунікації.
4. Якщо інше не передбачене статтями цього розділу, взаємна допомога надається відповідно до законодавства Сторони, яку запитують або відповідала договорів про взаємну допомогу, включаючи підстави, на яких Сторона, яку запитують, може відмовити у співробітництві. Сторона, яку запитують, не використовує право відмовити у взаємній допомозі щодо правопорушень, які містяться у статтях 2–11, тільки на підставі того, що запит стосується правопорушення, яке вона вважає фіскальним правопорушенням.

5. Якщо відповідно до положень цього розділу Сторони, яку запитують, дозволяється надавати взаємну допомогу за умови існування подвійного визнання правопорушення, ця умова вважається виконаною, незалежно від того, чи відносить її законодавство таке правопорушення до тієї ж категорії правопорушень або визначає його тією ж термінологією, як і Сторона, яка запитує, у разі, якщо поведінка, яка визначає правопору-

шення, стосовно якого запитується допомога, є злочинном відповідно до законодавства Сторони, яку запитують.

Стаття 26. Добровільно надана інформація

1. Сторона може в рамках свого законодавства без попереднього запиту надіслати іншій Стороні інформацію, отриману в ході її власного розслідування, якщо вона вважає, що розкриття такої інформації може допомогти Стороні, яка отримує інформацію, у відкритті або проведенні розслідування чи переслідування стосовно кримінальних злочинів, встановлених відповідно до цієї Конвенції або може спричинити запит про співробітництво від такої Сторони відповідно до цього розділу.
2. До надання такої інформації Сторона, яка надає інформацію, може вимагати, щоб вона залишалася конфіденційною або використовувалася за певних умов. Якщо Сторона, яка отримує інформацію, не може задовольнити вимоги такого запиту, вона повідомляє про це Сторону, яка надає інформацію, яка після цього визначає, чи надавати інформацію, незважаючи на це. Якщо Сторона, яка отримує інформацію приймає її за певних умов, вона має їх дотримуватися.

Заголовок 4

Процедури, пов'язані із запитами про взаємну допомогу в разі відсутності відповідних міжнародних угод

Стаття 27. Процедури, пов'язані із запитами про взаємну допомогу в разі відсутності відповідних міжнародних угод

1. У разі відсутності між Стороною, яка запитує, і Стороною, яку запитують, відповідних чинних договорів про взаємну допомогу чи угод на основі єдиного чи взаємного законодавства, застосовуються положення пунктів 2–10 цієї статті. Положення цієї статті не застосовуються у разі наявності такого договору, угоди або законодавства, якщо тільки зацікавлені Сторони не погоджуються застосовувати замість них, частково або повністю, вищевикладені положення цієї статті.

2. а) Кожна Сторона призначає центральний уповноважений орган або органи, які відповідають за надсилення та відповідь на запити про взаємну допомогу, виконання таких запитів або їх передачу уповноваженим органам, компетентним виконувати їх.
- б) Ці центральні уповноважені органи здійснюють прямі зносини між собою.
- в) Кожна Сторона під час підписання або передачі документа про ратифікацію, прийняття, затвердження чи приєднання повідомляє Генеральному секретареві Ради Європи назви й адреси всіх компетентних органів, призначених відповідно до цієї частини.
- г) Генеральний секретар Ради Європи створює і вносить відповідні зміни у реєстр компетентних органів, відповідно до призначе-

них Сторонами. Кожна Сторона забезпечує правильність відомостей, які містяться у такому реєстрі.

3. Запити про взаємну допомогу відповідно до цієї статті здійснюються згідно з процедурами, зазначеними Стороною, яка запитує, якщо тільки вони не суперечать законодавству Сторони, яку запитують.

4. Сторона, яку запитують, може, на додаток до підстав відмови, передбачених у пункті 4 статті 25, відмовити у допомозі, якщо:

- а) запит стосується правопорушення, яке Сторона, яку запитують, вважає політичним правопорушенням або правопорушенням, пов'язаним з політичним правопорушенням; або
- б) вона вважає, що виконання запиту може зашкодити її суверенітету, безпеці, суспільному порядку або іншим важливим інтересам.

5. Сторона, яку запитують, може відкласти свої дії щодо запиту, якщо такі дії можуть зашкодити кримінальному розслідуванню чи переслідуванню, яке здійснюється її уповноваженими органами.

6. До відмови або відкладення допомоги Сторона, яку запитують, після консультацій зі Стороною, яка запитує, розгляне, якщо це доцільно, можливість часткового задоволення запиту або його задоволення за умов, які вона вважає доречними.

7. Сторона, яку запитують, терміново інформує Сторону, яка запитує, про висновок розгляду щодо можливості виконання запиту про допомогу. Якщо у допомозі відмовлено чи вона відкладена, то вказується причини відмови чи відкладення. Сторона, яку запитують, також інформує Сторону, яка запитує, про будь-які причини, які унеможливають виконання запиту або можуть значною мірою затримати його виконання.

8. Сторона, яка запитує, може запросити Сторону, яку запитують, зберігати конфіденційним факт і зміст будь-якого запиту, зробленого відповідно до цього розділу, за винятком того обсягу, який є необхідним для виконання запиту. Якщо Сторона, яку запитують, не може виконати запит за умов його конфіденційності, вона терміново інформує про це Сторону, яка запитує. Остання визначає, чи необхідно виконати запит, незважаючи на неможливість збереження конфіденційності.

- 9. а) У термінових випадках запити про взаємну допомогу або про повідомлення, пов'язані з нею, можуть надсилатися безпосередньо судовими органами Сторони, яка запитує, до відповідних уповноважених органів Сторони, яку запитують. У будь-якому такому разі копія одночасно надсилається центральному уповноваженому органу Сторони, яку запитують, через центральний уповноважений орган Сторони, яка запитує.
- б) Будь-який запит або повідомлення відповідно до цього пункту може здійснюватися через Міжнародну організацію кримінальної поліції (Інтерпол).
- в) Якщо запит здійснено відповідно до підпункту (а), і державний орган не має компетенції розглядати такий запит, то він має

передати запит до компетентного державного органу і безпосередньо повідомити Сторону, яка запитує, про це.

д) Запити або повідомлення відповідно до цього пункту, які не включають у себе примусові дії, можуть передаватися безпосередньо компетентними органами Сторони, яка запитує, компетентним органам Сторони, яку запитують.

е) Кожна Сторона під час підписання або передачі документа про ратифікацію, прийняття, затвердження чи приєднання може повідомити Генерального секретаря Ради Європи про те, що з метою ефективності всі запити відповідно до цього пункту мають надсилатися її центральному органу.

Частина 2 КОНКРЕТНІ ПРИНЦИПИ

Заголовок 1

Взаємна допомога щодо тимчасових заходів

Стаття 29. Термінове збереження комп'ютерних даних, які зберігаються

1. Будь-яка Сторона може запитати іншу Сторону видати ордер чи іншим чином провести термінове збереження комп'ютерних даних, які зберігаються за допомогою комп'ютерної системи, яка перебуває на території такої іншої Сторони і стосовно якої Сторона, яка запитує, має намір надіслати запит про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних.

2. Запит про збереження відповідно до пункту 1 зазначає:

- а) назву компетентного органу, який робить запит про збереження;
- б) правопорушення, яке підлягає кримінальному розслідуванню або переслідуванню, і короткий опис відповідних фактів;
- в) комп'ютерні дані, які необхідно зберегти, та їх зв'язок з правопорушенням;
- г) будь-яку доступну інформацію для ідентифікації особи, яка зберігає такі комп'ютерні дані або розташування комп'ютерної системи;
- е) необхідність збереження; та
- ф) положення про те, що така Сторона має намір надіслати запит про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких комп'ютерних даних, які зберігаються.

3. Після отримання запиту від іншої Сторони, Сторона, яку запитують, вживає всіх належних заходів для термінового збереження зазначених даних відповідно до її внутрішньодержавного законодавства. Для цілей відповіді на запит, подальше визнання правопорушення не вимагається як підстава проведення такого збереження.

4. Сторона, яка вимагає подвійне визнання правопорушення як умову виконання запиту про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних, може стосовно правопорушень, які не є правопорушеннями, встановленими статтями 2—11 цієї Конвенції, зберігати за собою право відмовити у виконанні запиту про збереження відповідно до цієї статті у випадках, коли вона має підстави вважати, що на час розголошення умову щодо подвійного визнання правопорушення не можна задовольнити.

5. На додаток до цього, у виконанні запиту про збереження можна відмовити лише у випадках, коли:

- а) запит стосується правопорушення, яке Сторона, яку запитують, вважає політичним правопорушенням або правопорушенням, пов'язаним з політичним правопорушенням; або
- б) Сторона, яку запитують, вважає, що виконання запиту може зашкодити її суверенітету, безпеці, суспільному порядку або іншим важливим інтересам.
6. Якщо Сторона, яку запитують, вважає, що таке збереження не забезпечить майбутню доступність даних або загрожуватиме їхній конфіденційності чи іншим чином зашкодить розслідуванню, яке проводить Сторона, яка запитує, вона терміново інформує про це Сторону, яка запитує. Після цього остання визначає, чи необхідно виконувати запит, незважаючи на це.
7. Будь-яке збереження, проведене у відповідь на запит відповідно до пункту 1, проводиться не менш ніж 60 днів, для того, щоб надати можливість Стороні, яка запитує, надіслати запит щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних. Після отримання такого запиту дані зберігаються до винесення рішенням стосовно такого запиту.

Стаття 30. Термінове розкриття збережених даних про рух інформації

1. Якщо в ході виконання запиту, зробленого відповідно до статті 29, щодо збереження даних про рух інформації, які стосуються конкретної передачі інформації, Стороні, яку запитують, стає відомо, що початальник послуг в іншій Державі був залучений до передачі такої інформації, Сторона, яку запитують, терміново повідомляє Стороні, яка запитує, обсяг інформації про рух даних, достатній для ідентифікації такого початальника послуг і шляху передачі такої інформації.

2. У розкритті інформації про рух даних відповідно до пункту 1 може бути відмовлено тільки якщо:

- а) запит стосується правопорушення, яке Сторона, яку запитують, вважає політичним правопорушенням або правопорушенням, пов'язаним з політичним правопорушенням; або
- б) Сторона, яку запитують, вважає, що виконання запиту може зашкодити її суверенітету, безпеці, суспільному порядку або іншим важливим інтересам.

Заголовок 2

Взаємна допомога щодо повноважень на розслідування

Стаття 31. Взаємна допомога щодо доступу до комп'ютерних даних, які зберігаються

1. Будь-яка Сторона може запитати іншу Сторону провести обшук чи подібний доступ, арешт чи подібні дії або розголошення даних, які зберігаються за допомогою комп'ютерної системи, яка перебуває на території Сторони, яку запитують, включаючи дані, збережені відповідно до статті 29.

2. Сторона, яку запитують, відповідає на запит шляхом застосування відповідних міжнародних документів, угод і законодавства, на які містяться посилаєння у статті 23, а також відповідно до інших положень цього розділу.

3. На запит надається термінова відповідь, якщо:

- а) існують підстави вважати, що відповідні дані особливо вразливі для втрапи або змін; або
- б) міжнародні документи, угоди і законодавство, на які містяться посилаєння у пункті 2, передбачають термінове співробітництво.

Стаття 32. Транскордонний доступ до комп'ютерних даних, які зберігаються, за згодою або у випадку, коли вони є публічно доступними

Будь-яка Сторона може, не отримуючи дозволу іншої Сторони:

- а) здійснювати доступ до публічно доступних (відкриті джерело) комп'ютерних даних, які зберігаються, незважаючи на те, де такі дані знаходяться географічно; або
- б) здійснювати доступ або відновлювати шляхом комп'ютерної системи, яка перебуває на її території, комп'ютерних даних, які зберігаються і знаходяться в іншій Стороні, якщо Сторона отримувє законну і добровільну згоду особи, яка має законні повноваження розкривати дані такій Стороні за допомогою такої комп'ютерної системи.

Стаття 33. Взаємна допомога у збиранні даних про рух інформації у реальному масштабі часу

1. Сторони надають взаємну допомогу одна одній, щодо збирання даних про рух інформації у реальному масштабі часу, пов'язаних із зазначеною передачею інформації на їх території, яка передається за допомогою комп'ютерної системи. Відповідно до пункту 2, допомога регулюється умовами і процедурами, які передбачені внутрішньодержавним законодавством.

2. Кожна Сторона надає таку допомогу шнайменше щодо кримінальних правопорушень, стосовно яких проводиться збирання даних про рух інформації у реальному масштабі часу у випадку подібної внутрішньодержавної справи.

Стаття 34. Взаємна допомога у перехопленні даних змісту інформації

Сторони надають взаємну допомогу одна одній щодо перехоплення даних змісту інформації у зазначених передачах інформації, які здійсню-

ються за допомогою комп'ютерної системи, у обсягах, які дозволяються відповідними договорами між ними і внутрішньодержавним законодавством.

Заголовок 3

Цілодобова мережа

Стаття 35. Цілодобова мережа

1. Кожна Сторона призначає орган для здійснення контактів цілодобово впродовж тижня з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення. Така допомога включає сприяння або, якщо це дозволяється її внутрішньодержавним законодавством і практикою, праме:

- а) надання технічних порад;
 - б) збереження даних відповідно до статей 29 і 30; та
 - с) збирання доказів, надання юридичної інформації і встановлення місцезнаходження підозрюваних.
2. а) Орган Сторони, визначений нею для здійснення контактів, має можливість терміново встановлювати контакт з органом іншої Сторони для здійснення контактів.
- б) Якщо орган Сторони, визначений нею для здійснення контактів, не є частиною уповноваженого органу або органів такої Сторони, які відповідають за міжнародну взаємну допомогу або екстремію, то орган, визначений для здійснення контактів, забезпечує свою здатність проводити термінову координацію з таким уповноваженим органом або органами.
- с) Кожна Сторона забезпечує кваліфікований персонал і відповідне обладнання для сприяння роботі мережі.

Розділ IV

ПРИКІНЦЕВІ ПОЛОЖЕННЯ

Стаття 36. Підписання та набуття чинності

1. Ця Конвенція відкрита для підписання державами-членами Ради Європи та державами, які не є членами Ради Європи, але брали участь у розробці цієї Конвенції.
2. Ця Конвенція підлягає ратифікації, прийняттю або схваленню. Ратифікаційні грамоти або документи про прийняття або схвалення здаються на зберігання Генеральному секретареві Ради Європи.
3. Ця Конвенція набуває чинності в перший день місяця, який настає після закінчення тримісячного періоду від дати, на яку п'ять держав, серед яких принаймні три держави-члени Ради Європи, висловлять свою

згоду на обов'язковість для них цієї Конвенції згідно з положеннями пунктів 1 та 2.

4. Для будь-якої держави, яка підписала Конвенцію та згодом висловлює згоду на її обов'язковість для себе, ця Конвенція набуває чинності в перший день місяця, який настає після закінчення тримісячного періоду від дати висловлення такою державою згоди на обов'язковість для неї цієї Конвенції згідно з положеннями пунктів 1 та 2.

Стаття 37. Приєднання до Конвенції

1. Після набуття чинності цієї Конвенцією Комітет міністрів Ради Європи після консультацій з державами, які є Сторонами цієї Конвенції, та висловлення їхньої одностайної згоди може запросити будь-яку державу, яка не є членом Ради Європи та не брала участі в розробці цієї Конвенції, приєднатися до неї. Таке рішення ухвалюється більшістю, передбаченою у статті 20 д) Статуту Ради Європи, та одностайним голосуванням представників договірних держав, які мають право брати участь у засіданнях Комітету міністрів.

2. Для будь-якої держави, яка приєднується до Конвенції відповідно до вищевизначеного пункту 1, Конвенція набуває чинності в перший день місяця, який настає після закінчення тримісячного періоду від дати здачі на зберігання документа про приєднання Генеральному секретареві Ради Європи.

Стаття 38. Територіальне застосування

1. Будь-яка держава під час підписання або здачі на зберігання своєї ратифікаційної грамоти або документа про прийняття, схвалення або приєднання може визначити територію або території, до яких застосовуватиметься ця Конвенція.
2. Будь-яка Сторона у будь-який пізніший час шляхом направлення заяви на ім'я Генерального секретаря Ради Європи може поширити дію цієї Конвенції на будь-яку іншу територію, визначену в заяві. Для такої території Конвенція набуває чинності в перший день місяця, який настає після закінчення тримісячного періоду від дня одержання заяви Генеральним секретарем.
3. Будь-яка заява, зроблена згідно з двома попередніми пунктами щодо будь-якої території, визначеної у такій заяві, може бути відкликана шляхом направлення повідомлення Генеральному секретареві Ради Європи. Відкликання набуває чинності в перший день місяця, який настає після закінчення тримісячного періоду від дати отримання такого повідомлення Генеральним секретарем.

Стаття 39. Цілі Конвенції

1. Мета цієї Конвенції полягає у доповненні застосованих двосторонніх або багатосторонніх договорів або домовленостей між Сторонами, зокрема положень:

— Європейської конвенції про екстрадицію, відкритої для підписання у Парижі 13 грудня 1957 року (ETS № 24);

— Європейської конвенції про взаємну допомогу у кримінальних справах, відкритої для підписання у Страсбурзі 20 квітня 1959 року (ETS № 30);

— Додаткового протоколу до Європейської конвенції про взаємну допомогу у кримінальних справах, відкритого для підписання у Страсбурзі 17 березня 1978 року (ETS № 99).

2. Якщо дві або більше Сторін уже уклали угоду або договір щодо питань, які регулюються цією Конвенцією, або іншим чином встановлюють відносини з таких питань, або якщо вони зроблять це у майбутньому, вони також матимуть право застосовувати таку угоду чи договір або відповідно регулювати такі відносини. Однак у разі, якщо Сторони встановлюють свої відносини щодо питань, які регулюються цією Конвенцією, в інший спосіб, ніж передбачається нею, вони роблять це у такий спосіб, що не суперечить цілям та принципам Конвенції.

3. Ніщо в цій Конвенції не зачіпає інших прав, обмежень, зобов'язань та відповідальності Сторони.

Стаття 40. Заяви

Шляхом направлення письмового повідомлення на ім'я Генерального секретаря Ради Європи будь-яка держава під час підписання або здачі на зберігання своєї ратифікаційної грамоти або документа про прийняття, схвалення або приєднання може заявити, що вона користуватися можливістю запитати додаткові елементи, передбачені згідно зі статтями 2 та 3, пунктом 1 b) статті 6, статтею 7, пунктом 3 статті 9 та пунктом 9 e) статті 27.

Стаття 41. Умови щодо федеральних держав

1. Федеральна держава може залишити за собою право брати на себе зобов'язання, передбачені у розділі II цієї Конвенції, відповідно до її основних принципів регулювання відносин між центральними органами влади та державами, що входять до складу федерації, або іншими подібними територіальними одиницями за умови, що вона все-таки спроможна співпрацювати відповідно до розділу III.

2. Роблячи застереження відповідно до пункту 1, федеральна держава може не застосовувати умови такого застереження для того, щоб виключити або значно зменшити свої зобов'язання щодо передбачення заходів, згаданих у розділі II. Загалом вона забезпечує широкі та ефективні правоохоронні можливості щодо таких заходів.

3. Щодо положень цієї Конвенції, застосування яких входить до юрисдикції держав, що утворюють федерацію, або інших подібних територіальних одиниць, які згідно з конституційною системою федерації не зобов'язані вживати законодавчих заходів, федеральний уряд інформує

компетентні органи таких держав про згадані положення, представляючи свою позицію, та заохочує їх до вжиття відповідних заходів для введення в дію таких положень.

Стаття 42. Застереження

Шляхом направлення письмового повідомлення на ім'я Генерального секретаря Ради Європи будь-яка держава під час підписання або здачі на зберігання своєї ратифікаційної грамоти або документа про прийняття, схвалення або приєднання може заявити, що вона користуватися застереженням/застереженнями, передбаченими у пункті 2 статті 4, пункті 3 статті 6, пункті 4 статті 9, пункті 3 статті 10, пункту 3 статті 11, пункту 3 статті 14, пункту 2 статті 22, пункті 4 статті 29 та пункті 1 статті 41. Не може бути зроблено жодних інших застережень.

Стаття 43. Статус та відкликання застережень

1. Будь-яка Сторона, яка зробила застереження відповідно до статті 42, може повністю або частково відкликати його, направивши повідомлення на ім'я Генерального секретаря. Таке відкликання набуває чинності в день отримання такого повідомлення Генеральним секретарем. Якщо у повідомленні зазначається, що відкликання застереження має набутти чинності у визначений у повідомленні день та така дата є пізнішою, ніж дата отримання повідомлення Генеральним секретарем, відкликання набуває чинності у такий пізніший день.

2. Сторона, яка зробила застереження, згадане у статті 42, відкликає таке застереження повністю або частково, як тільки це дозволяють обставини.

3. Генеральний секретар Ради Європи може періодично запитувати Сторони, які зробили одне або декілька застережень, згаданих у статті 42, про можливість відкликання такого застереження/ таких застережень.

Стаття 44. Зміни та доповнення

1. Зміни та доповнення до цієї Конвенції можуть пропонуватися будь-якою Стороною. Вони направляються Генеральним секретарем Ради Європи державам-членам Ради Європи, а також державам, які не є членами Ради Європи, але брали участь у розробці цієї Конвенції, та всім державам, які приєдналися або були запрошені приєднатися до цієї Конвенції згідно з положеннями статті 37.

2. Будь-які зміни або доповнення, запропоновані Сторонами, передаються до Європейського комітету з проблем злочинності (ЄКПЗ), який надає Комітетові міністрів свою думку щодо таких запропонованих змін або доповнень.

3. Комітет міністрів розглядає запропоновану зміну або доповнення та думку, представлену Європейським комітетом з проблем злочинності (ЄКПЗ) та після консультацій із державами, які не є членами Ради Європи, але є Сторонами цієї Конвенції, може прийняти зміну або доповнення.

4. Текст будь-якої зміни або доповнення, прийнятого Комітетом міністрів згідно з пунктом 3 цієї статті, направляється Сторонам для прийняття.

5. Будь-які зміни та доповнення, прийняті відповідно до пункту 3 цієї статті набувають чинності після того, як усі Сторони повідомлять Генерального секретаря про їх прийняття.

Стаття 45. Вирішення спорів

1. Європейський комітет з проблем злочинності (ЄКПЗ) інформується про тлумачення та застосування цієї Конвенції.

2. У разі спору між Сторонами щодо тлумачення або застосування цієї Конвенції вони намагаються вирішити спір шляхом переговорів або будь-яких інших мирних засобів на свій вибір, включаючи подання спору до Європейського комітету з проблем злочинності (ЄКПЗ), до арбітражного суду, рішення якого є обов'язковим для виконання Сторонами, або до Міжнародного суду, за домовленістю заінтересованих Сторін.

Стаття 46. Консультатії Сторін

1. Сторони у разі необхідності регулярно консультуються з метою сприяння:

- а) ефективному використанню та застосуванню цієї Конвенції, включаючи виявлення будь-яких її проблематичних питань, а також наслідків будь-якої заяви або застереження, зробленого згідно з цією Конвенцією;
- б) обміну інформацією про суттєві зміни права, політики або технології, що стосуються кіберзлочинності, та збору інформації в електронній формі;
- в) розгляду можливих додатків до цієї Конвенції.

2. Європейський комітет з проблем злочинності (ЄКПЗ) регулярно інформується про результати консультатії, згаданих у пункті 1.

3. Європейський комітет з проблем злочинності (ЄКПЗ) у разі необхідності сприяє проведенню консультатії, згаданих у пункті 1, та вживає необхідних заходів для надання допомоги Сторонам у їхніх зусиллях щодо внесення змін або доповнень до Конвенції. Шонайпізніше через три роки після набуття чинності цією Конвенцією Європейський комітет з проблем злочинності (ЄКПЗ) у співпраці зі Сторонами проводить перегляд усіх положень Конвенції та, у разі необхідності, пропонує відповідні зміни та доповнення.

4. Витрати, пов'язані з виконанням положень пункту 1, сплачуються Сторонами у визначений ними спосіб, крім випадків, коли такі витрати сплачуються Радою Європи.

5. Секретаріат Ради Європи допомагає Сторонам у виконанні ними їхніх функцій за цією статтею.

Стаття 47. Денонації

1. Будь-яка Сторона може в будь-який час денонсувати цю Конвенцію шляхом направлення письмового повідомлення Генеральному секретареві Ради Європи.

2. Така денонація набуває чинності в перший день місяця, який настає після завершення тримісячного періоду від дня отримання повідомлення Генеральним секретарем.

Стаття 48. Повідомлення

Генеральний секретар Ради Європи повідомляє держави-члени Ради Європи та держави, які не є членами Ради Європи, але брали участь у розробці цієї Конвенції, а також усі держави, які приєдналися або були запрошені приєднатися до цієї Конвенції, про:

- а) будь-яке підписання;
- б) здачу на зберігання будь-якої ратифікаційної грамоти або документа про прийняття, схвалення або приєднання;
- в) будь-яку дату набуття чинності цією Конвенцією відповідно до статей 36 і 37;
- г) будь-яку заяву, зроблену відповідно до статей 40 та 41, або застереження, зроблене відповідно до статті 42;
- е) будь-який інший акт, повідомлення або інформацію, що стосується цієї Конвенції.

На посвідчення чого ті, що нижче підписали, належним чином на це уповноважені, підписали цю Конвенцію.

Вчинено в 2001 році англійською та французькою мовами, причому обидва тексти є рівно автентичними, в одному примірнику, який зберігається в архівах Ради Європи. Генеральний секретар Ради Європи надсилає завірнені копії цієї Конвенції кожній державі-члену Ради Європи, державам, які не є членами Ради Європи, але брали участь у розробці цієї Конвенції, а також усім державам, за прошенням приєдналися до неї.

ДЕКЛАРАЦІЯ ПРО ЄВРОПЕЙСЬКУ ПОЛІТИКУ В ГАЛУЗІ НОВИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

(прийнята на 104-й сесії Комітету міністрів Ради Європи
7 травня 1999 року, Будапешт)

[Генеральний директорат IV з питань освіти, культури, молоді, спорту та довкілля (Відділ вищої освіти та науково-дослідницької діяльності Директорату з питань освіти)]

Через пістологіття після заснування Ради Європи, яка зробила демократію, права людини та верховенство права незмінними пріоритетами післявоєнної Європи,

через десять років після основних політичних переворотів, які відкрили шлях до возз'єднання нашого континенту на основі ідеалів і принципів, які є спільним надбанням усіх європейських держав, у той час, коли цінності, на яких заснована Рада Європи, відкидаються та не визнаються у самому серці нашого континенту,

МИ, МІНІСТРИ ЗАКОРДОННИХ СПРАВ ДЕРЖАВ-ЧЛЕНІВ РАДИ Європи, ЯКІ ЗІБРАЛИСЯ НА 104-ТУ СЕСІЮ У БУДАПЕШТІ:

ЗНОВУ ПІДТВЕРДЖУЄМО НАШЕ РІШУЧЕ ПРАГНЕННЯ ПОВІСНИТИ ВИКОРИСТОВУВАТИ ПОТЕНЦІАЛ РАДИ Європи як політичного інституту особливієї важливості, здатного об'єднати всі країни Великої Європи із забезпеченням їм рівного становища у своїх постійних структурах, і
БЕРЕМО НА СЕБЕ ЗОБОВ'ЯЗАННЯ БУДУВАТИ ЦЮ ВЕЛИКУ ЄВРОПУ БЕЗ ЛІНІЙ РОЗМЕЖУВАННЯ. З цією метою ми будемо:

1. Продовжувати зміцнення стабільності нашого континенту на основі демократичних інституцій:
 - поважати всі зобов'язання, які ми взяли один перед одним, перед Радою Європи та перед нашими громадянами;
 - брати активну участь у діяльності організацій, заснованих для забезпечення дотримання цих зобов'язань;
 - надавати допомогу державам-членам, які здійснюють розбудову демократичних інституцій, розробляють політичні курси та втілюють правову реформу з метою досягти уніфікованих стандартів демократичного розвитку на території усього континенту;
 - продовжувати боротьбу проти тероризму, ворожого націоналізму та загроз територіальній цілісності держав.

2. Намататися зміцнити політично-правову та соціально-культурну єдність Великої Європи:

— розширювати спільну правову базу, яку поділяють держави-члени Ради Європи і яка зараз налічує 173 конвенції та більш ніж тисячу рекомендацій для урядів держав,

Декларація про європейську політику у галузі нових інформаційних технологій

— боротися проти факторів, які сіють розбрат, таких як расизм і ксенофобія, нетерпимість — чи то політична, чи культурна, чи релігійна — та дискримінація проти меншин,

— плекати суспільство культури, сформоване Європою та збагачене її різноманітним, впевнене у своєму самовизначенні та відкрите для зовнішнього світу,

— розробляти способи реалізації на спільні виклики, що постають перед сучасним суспільством, а саме розвиток нових інформаційних технологій, для яких визначено орієнтири європейської політики, викладені у Додатку I до цієї Декларації.

3. Підтверджувати верховенство людської особистості у нашій політиці:

- ефективно гарантувати основні права, забезпечені фізичним особам у наших державах-членах Європейською конвенцією про захист прав і основних свобод людини під наглядом Європейського суду з прав людини;

— сприяти цим правам і правам, що перебувають під захистом основних правових актів Ради Європи, зокрема через діяльність Комісара Ради Європи з прав людини, призначеного відповідно до Резолюції, що міститься в Додатку II;

— твердо протистояти будь-якому підходу, що може призвести до викривлення подвійних стандартів стосовно прав людини у всіх їхніх аспектах;

— розробити новий освітній підхід до питання демократичного промагання, заснованого на правах та обов'язках громадян, як вони визначені у цій Декларації та Програмі, що міститься в Додатку III.

4. Сприяти й надалі нашим спільним цінностям демократії та верховенства права через розвиток існуючого партнерства між:

— урядами держав-членів Ради Європи, поважаючи при цьому принцип рівності між державами та виражаючи сподівання на те, що всі країни Європи незбаром зможуть прийняти принципи, на яких заснована ця організація;

— національними урядами та парламентами, представленими у Комітеті міністрів і Парламентській Асамблеї, статутними органами Ради Європи, місцевими та регіональними органами влади, представленими у Раді Європи Конгресом місцевих і регіональних органів влади Європи, та структурами, які роблять можливим поєднання діяльності неурядових організацій та громадянського суспільства з міждержавною співпрацею;

— Радою Європи у межах її компетенції та іншими організаціями, включачи на регіональному рівні, які сприяють розвитку та структурній розбудові нашого континенту, зокрема Європейським Союзом та ОБСЄ.

— Ми рішуче нацелювані продовжувати рухатися у цьому напрямку і у XXI столітті, щоб зробити внесок у розвиток демократичної стабільності та співпраці у Європі. Відповідно ми зобов'язуємося:

— завершити реформування структур і діяльності Ради Європи та адаптувати їх до майбутніх викликів;

— шукати такі політично-економічні рішення, які дають можливість долати державні кордони та сприяти мирному і гармонійному співіснуванню націй, меншин, мовно-культурних і релігійних груп, які разом утворюють наш континент. У цьому дусі ми повинні реалізувати внесок Ради Європи у програму стабільності Південно-Східної Європи та працювати заради миру, так само як і задля дотримання прав людини та поваги до верховенства права на всій території Європи.

ДЕКЛАРАЦІЯ КОМІТЕТУ МІНІСТРІВ ПРО ПОЛІТИКУ У СФЕРІ НОВИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Додаток I

Комітет міністрів,
з нагоди 50-ї річниці заснування Ради Європи;

у відповідь на рішення Другого саміту Ради Європи розвивати європейську політику у сфері застосування нових інформаційних технологій з метою забезпечення поваги до прав людини, сприяння культурній різноманітності, підтримки свободи слова та самовираження, а також максимального розвитку освітньо-культурного потенціалу таких технологій; беручи до уваги всі відповідні міжнародні тексти у цій сфері, включаючи ті, що були прийняті після Другого саміту, зокрема тексти політичного характеру, укладені у м. Салонікі на 5-й європейській міністерській конференції з питань політики у сфері ЗМІ (грудень 1997 р.) та Резолюцію 53/70, схвалену Генеральною Радою Об'єднаних Націй (грудень 1998 р.); будучи свідомими глибоких змін, викликаних переведенням інформації у цифровий формат, конвергенцією та подальшою глобалізацією інформаційних мереж;

вітаючи можливість, запропоновані новими інформаційними технологіями щодо сприяння свободі слова та самовираження, політичному плюралізму та культурній різноманітності, а також здійснення внеску у розвиток більш демократичного та сталого інформаційного суспільства;

визнаючи потенціал нових інформаційних технологій у плані покращення відкритості, прозорості та ефективності на всіх рівнях — національному, регіональному та місцевому — урядування, управління та суспільства; усвідомлюючи також потенційні ризики, пов'язані з використанням цих технологій як фізичними особами, так і демократичним суспільством;
переконали у тому, що регуляторні рамки допоможуть розвивати ці можливості та уникати таких ризиків;

визнаючи важливу роль приватного сектора у створенні, розвитку та використанні нових інформаційних технологій та бажаючи сприяти роз-

Декларація про європейську політику у галузі нових інформаційних технологій

випитку партнерства між публічним і приватним секторами для максимального збільшення переваг цих технологій для суспільства;

переконаний у тому, що справді демократичне інформаційне суспільство, засноване на основних цінностях Ради Європи, може бути встановлене за допомогою політичних рамок, які заохочують доступ і участь, компетенції та здатність, творчі навички і культурну різноманітність, а також забезпечують захищеність.

закликає уряди держав-членів, які діють, де належно, разом з публічними та приватними партнерами,

(i) Стосовно доступу та участі у нових інформаційних технологіях:

— сприяти найширшому можливому доступу до всіх нових інформаційно-комунікаційних послуг, наприклад через широке розповсюдження точок доступу в громадських місцях;

— забезпечувати усіх осіб можливістю відігравати важливу роль у громадському житті на національному, регіональному та місцевому рівнях через використання нових інформаційних технологій для:

— забезпечення простого та прямого доступу до інформації про місцеві, регіональні та національні адміністративні та судові послуги;

— забезпечення доступності офіційних текстів місцевих, регіональних і національних нормативно-правових актів, міжнародних угод і рішень національних і міжнародних судових органів;

— заохочувати вільний обмін інформацією, ідеями та поглядами за допомогою використання нових інформаційних технологій;

— заохочувати розробку, виробництво та розподіл освітньо-культурних матеріалів і їх широке розповсюдження;

— заохочувати ефективне міжнародне співробітництво для забезпечення переваг вдосконаленого доступу та підвищеної прозорості;

— сприяти встановленню однакових можливостей для використання нових інформаційних технологій у всіх європейських країнах.

(ii) Стосовно компетентності та здатності використовувати нові інформаційні технології:

— сприяти широкому розумінню нових інформаційних технологій і їхнього потенціалу в усіх суспільних сферах;

— допомагати людям розвивати навички у використанні нових інформаційних технологій;

— через проведення практичних занять на всіх рівнях системи освіти, офіційних і неофіційних, і через використання на практиці;

— через визначення нових професійних вимог і програм практичної підготовки;

— щоб таким чином дати людям можливість активного та свідомого використання цих технологій для їхніх потреб;

— сприяти кращому та ширшому використанню нових інформаційних технологій у викладанні та навчанні, приділяючи особливу увагу питанням гендерної рівності;

— заохочувати використання інформаційних мереж у сфері освіти, щоб сприяти взаєморозумінню між народами як на рівні людей, так і на рівні установ.

(iii) Стосовно творчих навичок і галузей культури:

— сприяти використанню нових інформаційних технологій як форми художнього та літературного вираження та засобу формування творчих партнерств, зокрема у мистецтві, науці та промисловості;

— стимулювати розвиток природних творчих здібностей кожної людини через навчання комп'ютерної грамотності та розвиток навчальних програм за допомогою нових інформаційних технологій;

— працювати у контексті конвергенції та наявної глобалізації інформаційних мереж з галузями культури для спрямування їхньої діяльності на розвиток творчих здібностей;

— заохочувати спільну роботу галузей культури Європи для вдосконалення творчих здібностей, і таким чином забезпечити культурне різноманіття, разом із забезпеченням якості продукції та послуг інформаційних мереж.

(iv) Стосовно мовно-інформаційного різноманіття:

— заохочувати розвиток широкого спектра комунікаційно-інформаційних мереж, а також мовно-інформаційного різноманіття таким чином, щоб сприяти політичному плюралізму, культурній різноманітності та стабільному розвитку;

— сприяти повному використанню, включаючи меншинами, можливостей, що пропонуються новими інформаційними технологіями, для обміну думками та самовираження;

— визнавати корисність цих технологій у забезпеченні всіх країн і регіонів Європи можливості виражати своє культурне різноманіття;

— заохочувати забезпечення культурних, освітніх та інших продуктів і послуг різними мовами та сприяти якнайширшому різноманіттю цих продуктів і послуг;

— забезпечити, наскільки можливо, щоб інформаційні системи на адміністративному та правовому рівнях пропонували матеріал, підготовлений з належною увагою до регіональних і лінгвістичних критеріїв згідно з конкретними потребами відповідних меншин.

(iv) Стосовно захисту прав і свобод:

— забезпечувати повагу до прав і людської гідності, а саме свободи самовираження, захист прав меншин, захист приватного життя та даних особистого характеру, а також захист особи проти всіх форм расової дискримінації при використанні та розробці нових інформаційних технологій, через регулювання і саморегулювання та через розвиток технічних стандартів і систем, етичних кодексів та інших заходів;

— вживати заходів на національному та міжнародному рівнях, спрямованих на ефективне розслідування та покарання злочинів у сфері інфор-

маційних технологій та боротьбу з існуванням безпечних схованок таких правопорушників;

— забезпечувати ефективний захист власників прав, чий роботи поширюються за допомогою нових комунікаційно-інформаційних послуг;

— заохочувати встановлення міжнародних стандартів і гарантій, які мають суттєве значення для гарантування достовірності документів, які передаються електронним шляхом, і договорів, які мають юридично обов'язкове значення;

— сприяти розвитку цих рамок захисту, включаючи розробку кодексів поведінки, із включенням до них етичних принципів щодо використання нових інформаційних технологій.

РЕКОМЕНДАЦІЯ № R (81) 19
КОМІТЕТУ МІНІСТРІВ
ДЕРЖАВАМ-ЧЛЕНАМ РАДИ ЄВРОПИ
ПРО ДОСТУП ДО ІНФОРМАЦІЇ, ЩО ПЕРЕБУВАЄ
У РОЗПОРЯДЖЕННІ ДЕРЖАВНИХ ОРГАНІВ¹

*(Схвалено Комітетом міністрів 25 листопада 1981 р.
на 240-й сесії засідання міністрів)*

Комітет міністрів згідно з положеннями Статті 15.б Статуту Ради Європи;

беручи до уваги, що завдання Ради Європи полягає у досягненні більшої єдності держав-членів;

беручи до уваги Рекомендації Асамблеї № 854 про доступ громадськості до документів державних органів і вільного доступу до інформації; беручи до уваги важливість отримання громадськості у демократичному суспільстві достатньої інформації про питання суспільного значення; беручи до уваги, що доступ громадськості до інформації є передумовою посилення довіри громадськості до органів управління;

беручи до уваги у зв'язку з цим необхідність докласти максимальні зусилля для забезпечення найбільш повного можливого доступу громадськості до інформації, що перебуває в розпорядженні державних органів, рекомендує урядам держав-членів керуватися у законодавстві та практиці принципами, що додаються до цієї рекомендації.

ДОДАТОК ДО РЕКОМЕНДАЦІЇ
№ R (81) 19

Принципи, що подано нижче, поширюються на фізичних та юридичних осіб. При впровадженні цих принципів необхідно брати до уваги інтенси розумного та дієвого управління. У випадках, коли ці інтереси потребують коригування чи виключення одного або більше принципів, чи то в особливих випадках, чи у певних сферах державного управління, однак необхідно докласти максимальних зусиль для досягнення найбільш можливого ступеня доступу до інформації.

1. Кожна особа, яка перебуває під юрисдикцією держави-члена, має право отримувати на свою вимогу інформацію, що знаходиться у розпорядженні державних органів, за винятком законодавчих органів і органів судової влади.

¹ Під час прийняття Рекомендації № R (81) 19 відповідно до статті 10.2.с Регламенту зустрічей засідання міністрів представники Італії та Люксембургу зберегли право своїх урядів на те, щоб або дотримуватися, або не дотримуватися цієї Рекомендації.

II. Для доступу до інформації необхідно забезпечувати ефективні та належні засоби.

III. У доступі до інформації не може бути відмовлено на підставі того, що особа, яка звернулася, не має спеціальної зацікавленості у цьому питанні.

IV. Доступ до інформації забезпечується на основі рівності.

V. Зазначені принципи підлягають обмеженню лише у випадках, необхідних демократичному суспільству для захисту легітимних суспільних інтересів (як, наприклад, національна безпека, суспільна безпека, громадський порядок, економічний добробут країни, попередження злочинів або попередження розголошення інформації, отриманої конфіденційно), а також для захисту приватного життя та інших легітимних приватних інтересів, але беручи при цьому до уваги особливу зацікавленість кожної особи в інформації, що знаходиться у розпорядженні державних органів, і стосується її особисто.

VI. Кожне звернення про надання інформації має розглядатися у розумні строки.

VII. Державний орган, який відмовляється надати інформацію, має пояснити причину відмови відповідно до закону або практики.

VIII. Кожна відмова про надання інформації може бути оскаржена.

ПОЯСНЮВАЛЬНА ЗАПІСКА

Вступ

1. Загально визнано, що демократична система може функціонувати найефективніше, лише коли громадськість є повністю поінформованою. Вільше того, через соціальні й технологічні досягнення сучасне життя стало таким складним, що державні органи часто володіють величезними об'ємами документів та інформації, які можуть мати загальний інтерес і важливість. Для забезпечення належного рівня участі кожного у громадському житті необхідно, щоб громадськість, підпадаючи під неминучі винятки та обмеження, мала доступ до інформації, що знаходиться у розпорядженні державних органів усіх рівнів.

2. Діяльність державних органів глибоко позначається на щоденному житті кожної людини. Для захисту прав фізичних осіб найбільше значення має їхня обізнаність з інформацією, що знаходиться у розпорядженні державних органів, зокрема інформацією, яка стосується їх самих чи їхніх інтересів, а також щоб доступ до інформації спирався на принцип рівності.

3. Необхідно зазначити, що доступ до інформації громадськості також в інтересах самих державних органів, оскільки це може допомогти встановити тісніші відносини між органами управління та особою і таким чином посилити довіру громадськості до органів управління.

4. Беручи до уваги важливість цих загальних ідей, було проведено колокіум на тему «Свобода інформації та обов'язок державних органів забезпечува-

ти доступ до інформації». Цей колоквіум було організовано Радою Європи у м. Ізраї 21—23 вересня 1976 року у співпраці з факультетом права Університету м. Ізраї. Висновки цього колоквіуму розглядалися Координаційним комітетом з прав людини на його 3-му засіданні (8—12 травня 1978 року), і було вирішено заснувати комітет експертів для вивчення пропозицій, висловлених членами-членами. Цей комітет запропонував підготувати рекомендацію до пропозиції, Парламентська Асамблея Ради Європи схвалила 1 лютого 1979 року Рекомендацію № 854 (1979) про доступ громадськості до інформації, що знаходиться у розпорядженні державних органів, і свободу доступу до інформації, у якій було рекомендовано Комітету міністрів:

«запропонувати державам-членам, які ще цього не зробили, запровадити систему свободи інформації, тобто доступу до інформації, що знаходиться у розпорядженні державних органів, що включає права пошуку та отримання інформації від державних органів і відомств, право вивчати та привласнювати інформацію, яка стосується персонально особи, право на приватну інформацію № 854 (1979) було направлено Комітетом міністрів на розгляд Координаційного комітету з прав людини у травні 1979 року.

6. Рішенням № СДН/9/161179 від 16 листопада 1979 Координаційний комітет з прав людини доручив Комітету експертів з державних органів і доступу до інформації «продовжити дослідження питання про доступ до інформації, що знаходиться у розпорядженні державних органів, включаючи права на пошук і отримання інформації від державних органів і відомств і беручи до уваги право на приватну інформацію і право на негтайний судовий розгляд цих питань з наміром підготувати відповідну рекомендацію урядам держав-членів».

Комітету експертів з державних органів і доступу до інформації було доручено не займатися питанням «права вивчати та привласнювати інформацію, яка стосується персонально особи», як зазначено у пункті 13 (а) Рекомендації № 854 (1979) Парламентської Асамблеї Ради Європи. На думку Координаційного комітету, це право порушувало важливі проблеми, що стосувалися захисту фізичних осіб проти дій органів управління, а тому це право слід розглядати окремо.

7. Проект Рекомендації про доступ до інформації, що знаходиться у розпорядженні державних органів, було підготовлено Комітетом експертів з державних органів і доступу до інформації у ході двох засідань, проведених у 1980 році. Його було також досліджено Координаційним комітетом з прав людини на його 9-му засіданні (4—8 травня 1981 року). Текст було подано Комітету міністрів і прийнято 25 листопада 1981 року [на 340-му засіданні засідателів міністрів].

Загальні коментарі

8. Комітет експертів підготував Рекомендацію, у Додатку до якої містяться вісім принципів доступу до інформації, що знаходиться у розпоряд-

женні державних органів. Урядам держав-членів рекомендується керуватися цими принципами у законодавстві та практиці. Термін «принципи» було використано для того, щоб дати державам-членам стільки свободи, скільки можливо, в обранні ними засобів для забезпечення того, що органи управління будуть суттєво дотримуватися принципів, викладених у Додатку до Рекомендації.

Ці принципи слід розуміти як визначення загального стандарту, а не утримання держав-членів від визнання додаткових або ширших прав і гарантій надання доступу до інформації або від розширення сфери їх застосування. Так само ніщо у цій Рекомендації не слід тлумачити як таке, що означає обмеження прав чи гарантій надання доступу до інформації, які вже можуть бути визначені державами-членами.

9. У вступі до принципів чітко сказано про те, що вони застосовуються як до фізичних, так і юридичних осіб, оскільки обидві категорії однаково зацікавлені у тому, щоб мати доступ до інформації.

10. У вступі міститься загальне положення, що застосовується до всіх принципів. Його завдання — забезпечити впровадження принципів таким чином, щоб це відповідало вимогам розумного та ефективного управління. Для того щоб зробити застосування принципів більш гнучким, було додано положення, яким передбачається можливість коригування або незастосування певних принципів у окремих випадках або певних сферах державного управління, однак наголошуючи при цьому на бажаності досягнення найвищого можливого рівня доступу до інформації.

КОМЕНТАРІ ДО ДОДАТКА

Принцип I

11. Принцип I визначає основний предмет Рекомендації, а саме право на отримання інформації, навіть якщо особа, зацікавлена у цьому, не є стороною в адміністративній процедурі. Захист громадянина у такій процедурі є предметом Рекомендації № (77) 31 про захист особи стосовно дій органів управління, схвалені Комітетом міністрів Ради Європи 28 вересня 1977 року. Цей загальний принцип поширюється на осіб, які мають прямі відносини з державними органами відповідно до концепції юрисдикції.

12. Термін «державний орган» включає всі державні органи будь-якого рівня. Однак сфера застосування Рекомендації не поширюється на законодавчі органи та органи судової влади.

Принцип II

13. Існують різні системи для забезпечення доступу до інформації. Вони залежать від структури та практики діяльності системи управління. Принцип II, таким чином, не означає рекомендацію певної системи забезпечення доступу. Важливо те, що для отримання необхідної інформації по-

трібно забезпечувати належні та ефективні засоби.

14. Відповідно, вибір між існуючими можливостями надання доступу до інформації має зробити кожна держава-член самостійно. Кожна з них має прийняти рішення щодо того, чи такі засоби мають впроваджуватися за допомогою закону, формального кодексу норм і правил, спеціального положення чи іншими методами.

15. Засоби отримання інформації можуть включати вивчення інформації, надання письмової чи усної відповіді або забезпечення копій. Жодному із засобів не надається перевага, однак який засіб має бути ефективним з огляду на існуючі обставини та природу інформації.

Принцип III

16. Право доступу до інформації ставить на меті допомогти громадянськості бути повністю поінформованою щодо питань суспільного життя. Для цих цілей забезпечення інформацією не повинно залежати від встановлення факту спеціальної зацікавленості в інформації.

Принцип IV

17. Цей принцип є суттєво важливим положенням щодо недискримінації. Він має забезпечити те, що відповідно до положень Принципу V, інформація буде надаватися кожному, хто її потребує, на однакових підставах і в однаковому обсязі.

РЕКОМЕНДАЦІЯ № R (89) 9

КОМІТЕТУ МІНІСТРІВ

ДЕРЖАВАМ-ЧЛЕНАМ РАДИ ЄВРОПИ

ЩОДО КОМП'ЮТЕРНИХ ПРАВОПОРУШЕНЬ

*(Схвалено Комітетом міністрів 13 вересня 1989 року
на 428-му засіданні засідальників міністрів)*

Комітет міністрів згідно зі статтею 15.b Статуту Ради Європи, беручи до уваги, що завдання Ради Європи полягає у досягненні більшої єдності держав-членів;

визнаючи важливість належного та швидкого реагування на нову проблему злочинів, пов'язаних із використанням електронно-обчислювальної техніки;

беручи до уваги той факт, що злочини, пов'язані з використанням електронно-обчислювальної техніки, часто мають транскордонний характер; усвідомлюючи потребу в подальшій гармонізації законодавства і практики та вдосконалення міжнародної правової співпраці, рекомендує урядам держав-членів:

1. Брати до уваги при перегляді чинного та ініціюванні нового законодавства звіт про злочини, пов'язані з використанням електронно-обчислювальної техніки, підготовлений Європейським комітетом з питань злочинності, та, зокрема, орієнтири для національних законодавців.

2. Звітувати Генеральному секретареві Ради Європи протягом 1993 року про будь-які розробки у їхньому законодавстві та юридичній практиці і випадки міжнародної правової співпраці щодо злочинів, пов'язаних із використанням електронно-обчислювальної техніки.

РЕКОМЕНДАЦІЯ № R (91) 10
КОМІТЕТУ МІНІСТРІВ
ДЕРЖАВАМ-ЧЛЕНАМ РАДИ ЄВРОПИ
ЩОДО ПЕРЕДАЧІ ТРЕТІМ ОСОБАМ ІНФОРМАЦІЇ
ОСОБИСТОГО ХАРАКТЕРУ,
ЯКА ЗНАХОДИТЬСЯ В РОЗПОРЯДЖЕННІ ОРГАНІВ ВЛАДИ¹

*(Схвалено Комітетом міністрів 9 вересня 1991 року на 461-му засіданні
заступників міністрів)*

Комітет міністрів згідно зі статтею 15.b Статуту Ради Європи, беручи до уваги, що завдання Ради Європи полягає в досягненні більшої єдності держав-членів;

зауважуючи, що автоматизована обробка даних дала державним органам можливість зберігати такі дані в електронному вигляді, включаючи дані особистого характеру, які вони збирають для цілей виконання своїх функцій;

услідуючи те, що нові автоматизовані методи зберігання таких даних полегшують доступ третіх сторін до них, що сприяє кращому розповсюдженню інформації серед громадськості, яке заохочується Комітетом міністрів у його Рекомендації № R(81)19 щодо доступу до інформації, що знаходиться у розпорядженні державних органів, а також у його Декларації від 29 квітня 1982 року про свободу самовираження та інформації; вважаючи, однак, що автоматизація даних, які збираються та зберігаються державними органами, вимагає розглянути її вплив на дані особистого характеру або файли з даними особистого характеру, що збираються та зберігаються державними органами для цілей виконання ними своїх функцій;

Зауважуючи зокрема, що автоматизація даних особистого характеру або файлів з даними особистого характеру підвищила ризик посягання на приватне життя, оскільки вона дає можливість ширшого доступу за допомогою інтервованих засобів передачі даних до даних особистого характеру та файлів з даними особистого характеру, що знаходяться у розпорядженні державних органів, а також передачі таких даних або файлів з даними особистого характеру третім сторонам;

¹ При прийнятті цієї Рекомендації та відповідно до статті 10.2.c Регламенту за-сідань заступників міністрів:

представник Ірландії зберіг право уряду на дотримання або недотримання принципів 6.2, 6.3.2 і 7.1 Додатку до цієї Рекомендації;

представники Норвегії та Сполученого Королівства зберегли право своїх урядів на дотримання або недотримання принципів 6.2 і 6.3.2 Додатка до цієї Рекомендації;

представник Швеції зберіг право уряду на дотримання або недотримання принципів 6.2 Додатка до цієї Рекомендації.

Рекомендація № R (91) 10 Комітету Міністрів державам-членам Ради Європи...

пам'ятаючи у зв'язку з цим про підвищення тенденцій з боку приватного сектора до експлуатації комерційних переваг даних особистого характеру чи файлів з даними особистого характеру, що знаходяться у розпорядженні державних органів, а також про нову політику державних органів, що передбачає передачу даних особистого характеру та файлів з даними особистого характеру за допомогою електронних засобів зв'язку третім сторонам на комерційній основі;

будучи рідше налаштованими сприяти поширенню принципів захисту даних, що спираються на Конвенцію про захист фізичних осіб стосовно обробки даних особистого характеру від 28 січня 1981 року, для того щоб передати державними органами даних особистого характеру чи файлів з даними особистого характеру третім сторонам, зокрема за допомогою електронних засобів зв'язку, здійснювалася на основі закону та супроводжувалася забезпеченням відповідних гарантій суб'єктові даних;

Зауважуючи зокрема, що ці принципи захисту даних мають знайти своє відображення у новому контексті автоматизації, що нині характеризує передачу даних особистого характеру та файлів з даними особистого характеру третім сторонам відповідно до правових положень, що регулюють доступ третіх сторін до даних особистого характеру та файлів з даними особистого характеру;

рекомендує урядам держав-членів:

i) брати до уваги принципи, що містяться у Додатку до цієї Рекомендації, у випадках, коли дані особистого характеру або файли з даними особистого характеру, що збираються або зберігаються державними органами, надаються третім сторонам;

ii) приділяти належну увагу принципам, що містяться в Додатку до цієї Рекомендації, у їхньому праві та практиці, з огляду на автоматизацію та передачу третім сторонам за допомогою електронних засобів зв'язку даних особистого характеру та файлів з даними особистого характеру;

iii) забезпечувати широке розповсюдження принципів, що містяться у Додатку до цієї Рекомендації серед державних органів;

iv) донести принципи, що містяться у Додатку до цієї Рекомендації, до відома державних органів, створених відповідно до законодавства про захист даних або законодавства про доступ до інформації публічного сектора.

ДОДАТОК
ДО РЕКОМЕНДАЦІЇ № R (91) 10

1. Сфера застосування та тлумачення термінів

1.1. Принципи, що містяться у цій Рекомендації, застосовуються до автоматизованої обробки даних особистого характеру, які збираються державними органами та можуть передаватися третім сторонам.

1.2. Держави-члени можуть розширити сферу застосування цієї Рекомендації для включення до неї даних, що стосуються груп, підприємств, асоціацій та інших організацій, незалежно від того, чи вони володіють

правосуб'єктністю, а також даних, що знаходяться у неавтоматизованій формі.

У цій Рекомендації поняття вживаються у такому значенні:

1.3. Поняття «дані особистого характеру» означають будь-яку інформацію, яка стосується визначеної особи або особи, яку неможливо визначити (суб'єкт даних). Фізична особа не може вважатися такою, яку можна визначити, якщо визначення вимагає нерозумної кількості часу, коштів і праці.

Поняття «державні органи» означає будь-яку адміністративну, інституційну, заклад чи інший орган, який виконує публічні функції, завдяки чому, що його було наділено публічними повноваженнями.

Національне право може давати ширше визначення поняття «державні органи».

Поняття «файли, доступні третім сторонам» означає файли, що знаходяться у розпорядженні державних органів і містять дані особистого характеру, які можуть повідомлятися громадськості чи третім сторонам, які мають особливий інтерес і які повідомляються відповідно до загальних законів про доступ до інформації публічного сектора або свободи інформації, конституційних положень, а також спеціальних законів, нормативних актів і прецедентів, що дозволяють третім сторонам мати доступ до інформації, що знаходиться у розпорядженні державних органів, включаючи за допомогою офіційного оприлюднення.

Поняття «повідомлення інформації» означає надання доступу до файлів чи даних особистого характеру, наприклад дозволяючи ознайомлення з ними, передаючи ці дані каналами зв'язку, поширюючи їх або забезпечуючи доступ до них, незалежно якими засобами.

Поняття «третя сторона» означає фізичних і юридичних осіб, яким передаються дані особистого характеру державними органами, за винятком інших державних органів.

Національне право може давати ширше визначення поняття «третя сторона».

2. Повага до приватного життя та принцип захисту даних

2.1. Повідомлення, зокрема засобами електронного зв'язку, даних особистого характеру чи файлів з даними особистого характеру третім сторонам має супроводжуватися гарантіями, що приватне життя суб'єкта даних не буде порушуватися в незаконному порядку.

Зокрема, дані особистого характеру та файли з даними особистого характеру не повинні повідомлятися третім сторонам, окрім випадків, коли:

- a) це передбачено спеціальним законом; або
- b) громадянська має доступ до них відповідно до правових положень, що регулюють доступ до інформації публічного сектора; або
- c) повідомлення здійснюється відповідно до національного законодавства про захист інформації; або
- d) суб'єкт даних вільно та поінформовано надав свою згоду.

2.2. Якщо нормами національного права не передбачено забезпечення належних гарантій суб'єкта даних, дані особистого характеру або файли з

даними особистого характеру не можуть повідомлятися третім сторонам для цілей, що не відповідають тим, для яких ці дані були зібрані.

2.3. Національне законодавство про захист даних має застосовуватися до обробки третіми сторонами даних особистого характеру, що повідомляються їм державними органами.

3. Дані чутливого характеру

3.1. Дані особистого характеру, що підпадають під будь-яку з категорій, визначених статтею 6 Конвенції про захист фізичних осіб стосовно автоматизованої обробки даних особистого характеру, не повинні зберігатися у файлі чи частині файлу, загальнодоступних третім сторонам.

Будь-які винятки з цього принципу мають бути чітко передбачені законом із забезпеченням відповідних гарантій суб'єктові даних.

3.2. Положення принципу 3.1 не обмежують можливість зберігання у файлах, доступних третім сторонам, категорій даних, які за інших обставин вважалися б чутливими, однак є доступними третім сторонам, оскільки ці дані стосуються таких суб'єктові даних у публічному житті, які виконують функції, що належать до публічної сфери.

4. Загальнодоступні дані

4.1. Цілі, для яких дані будуть збиратися та зберігатися у файлах, доступних третім сторонам, а також публічний інтерес, що виправдовує надання доступу до них, мають зазначатися відповідно до норм національного права та практики.

4.2. Перед або в будь-який час протягом збору даних суб'єкти даних мають бути поінформовані відповідно до норм національного права та практики про обов'язковість чи необов'язковість збору таких даних, про правову основу та цілі збору й обробки даних особистого характеру, а також публічний інтерес, що виправдовує надання доступу до них.

4.3. Державні органи мають уникати повідомлення третім сторонам даних особистого характеру, які зберігаються у файлах, доступних громадськості, та які стосуються суб'єктів даних, чий безпека та приватне життя можуть особливо постраждати.

5. Доступ і повідомлення даних особистого характеру за допомогою електронних засобів

5.1. Автоматизована обробка даних особистого характеру, які зберігаються у файлах, доступних третім сторонам, повинна здійснюватися відповідно до норм національного права.

Норми національного права мають встановити умови, що регулюють повідомлення або доступ до цих даних, і, зокрема, передбачати умови, що регулюють автоматизоване повідомлення або ознайомлення з цими даними у режимі реального часу.

5.2. При автоматизованому повідомленні інформації слід використовувати технічні засоби, розроблені для обмеження електронних запитів і пошуку інформації з метою запобігти неуповноваженому ознайомленню

та отримання даних особистого характеру або файлів, які містять такі дані.

6. Обробка третіми сторонами даних особистого характеру, що походять з файлів, доступних третім сторонам

6.1. У випадках, коли суб'єкт даних зобов'язаний надати свої дані для збереження у файлах, доступних третім сторонам, обробка даних особистого характеру третіми сторонами має здійснюватися або за умови отримання прямої та поінформованої згоди суб'єкта даних, або відповідно до встановлених законом вимог.

У випадках, на які поширюється вимога отримати згоду, суб'єкт даних повинен мати можливість у будь-який час скасувати свою згоду.

6.2. У випадках, коли збереження даних особистого характеру у файлах, доступних третім сторонам, не є обов'язковим, суб'єкт даних має бути поінформований до або під час збору інформації про свої права:

- а) не зберігати свої дані у файлах, доступних третім сторонам; або
- б) зберігати свої дані в такому файлі та дозволити їх повідомлення, однак, без здійснення їх обробки третіми сторонами; або
- с) заперечувати проти того, щоб треті сторони і надалі мали можливість обробляти його дані; або
- д) знищувати свої дані у будь-який час.

6.3. Якщо третя сторона створює файл, у якому містяться дані особистого характеру, отримані з файлів, доступних третім сторонам, такий файл повинен підпадати під вимоги норм національного законодавства про захист даних, включаючи права суб'єкта даних.

Зокрема, суб'єкт даних повинен мати можливість дізнаватися про існування нового файлу, ціль його створення та права суб'єкта на те, щоб стерти його дані з такого файлу.

7. Взаємодієднання та підключення файлів

7.1. Окрім випадків, коли це дозволено нормами національного права із забезпеченням належних гарантій суб'єктові даних, взаємодієднання, зокрема за допомогою під'єднання, об'єднання або завантаження, файлів з даними особистого характеру, що складаються з даних особистого характеру, які походять з файлів, доступних третім сторонам, а також підключення та взаємодієднання файлів або даних особистого характеру, що знаходяться у розпорядженні третіх сторін, де один або більше файлів знаходяться у розпорядженні державних органів, для збагачення наявних файлів або даних, мають бути забороненими.

8. Транскордонні потоки даних

8.1. Принципи цієї Рекомендації поширюються на транскордонну передачу даних особистого характеру, які збираються державними органами та можуть бути повідомленими третім сторонам.

8.2. Транскордонна передача даних особистого характеру третім сторонам, які проживають у державі, що ратифікувала Конвенцію № 108 і має,

таким чином, закон про захист даних, не повинна підпадати під спеціальні умови захисту приватного життя.

8.3. У випадках, коли дотримується принцип рівнозначного захисту, не повинні встановлюватися обмеження на транскордонну передачу даних особистого характеру третім сторонам, які проживають у державі, що не ратифікувала Конвенцію № 180, але має законодавчі положення, які відповідають принципам зазначеної Конвенції та цієї Рекомендації.

8.4. Якщо інше не передбачено нормами національного права, транскордонна передача даних особистого характеру третім сторонам, які проживають у державі, законодавчі положення якої не відповідають Конвенції № 108 або цій Рекомендації, не повинна, як правило, здійснюватися, окрім випадків, коли:

- а) вжито необхідні заходи, включаючи договірний характеру, для отримання принципів зазначеної Конвенції та цієї Рекомендації, а суб'єкт даних має можливість заперечувати проти такої передачі даних; або
- б) суб'єкт даних вільно та поінформовано надав свою письмову згоду та має можливість у будь-який час скасувати її.

8.5. Слід вживати заходів для уникнення автоматизованої транскордонної передачі даних особистого характеру або файлів, що містять такі дані, третім сторонам без відома суб'єктів даних.

9. Координація або співпраця

9.1. У випадках, коли загальне законодавство, що регулює доступ до інформації публічного сектора, передбачає заснування органу нагляду для впровадження такого законодавства, і одночасно існує загальне законодавство про захист даних з окремим органом, відповідальним за впровадження цього законодавства, відповідні державні органи мають узгодити механізм, спрямований на полегшення обміну інформацією щодо умов, якими регулюється передача даних особистого характеру, що походять з файлів, доступних третім сторонам.

РЕКОМЕНДАЦІЯ № R (95) 13 КОМІТЕТУ МІНІСТРІВ ДЕРЖАВАМ-ЧЛЕНАМ РАДИ ЄВРОПИ СТОСОВНО ПРОБЛЕМИ КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНОГО ПРАВА ЩОДО ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

(Схвалено Комітетом міністрів 11 вересня 1995 року на 543-му
засіданні засідуючих міністрів)

Комітет міністрів згідно зі статтею 15.b Статуту Ради Європи, беручи до уваги, що завдання Ради Європи полягає у досягненні більшої єдності держав-членів; беручи до уваги безпрецедентний розвиток інформаційних технологій та їх застосування у всіх сучасних суспільних галузях; усвідомлюючи, що розвиток електронних інформаційних систем прискорить трансформацію традиційного суспільства в інформаційне суспільство шляхом створення нового простору для всіх видів засобів спілкування та відносин; усвідомлюючи вплив інформаційних технологій на спосіб організації суспільства та спілкування і взаємини між людьми; усвідомлюючи те, що все більша частина економічно-соціальних зв'язків відбувається через або за допомогою електронно-інформаційних систем; будучи стурбованими ризиком того, що електронно-інформаційні системи та електронна інформація можуть використовуватися для вчинення кримінальних правопорушень; зважаючи на те, що докази кримінальних правопорушень можуть зберігатися та передаватися через ці системи; зауважуючи, що кримінально-процесуальні закони держав-членів час-то ще не забезпечують належні повноваження для пошуку та збору доказів у цих системах у ході кримінальних розслідувань; пам'ятаючи про те, що нестача спеціальних повноважень може завадити слідчим органам у належному виконанні ними їхніх завдань перед лицем наявного розвитку інформаційних технологій; визнаючи потребу адаптації легітимних засобів, що забезпечуються слідчим органам кримінально-процесуальними законами, до специфічного характеру розслідувань, що проводяться в електронних інформаційних системах; виражаючи свою стурбованість потенційним ризиком того, що держави-члени не зможуть надати взаємну правову допомогу належним чином на вимогу знати у межах їхньої території електронні докази, що знаходяться в електронних інформаційних системах; переконані у необхідності зміцнити внутрішню співпрацю та досягнути вишого рівня сумісності кримінально-процесуальних законів у цій сфері; пам'ятаючи про Рекомендацію № R (81) 20 Комітету міністрів щодо гармонізації законів, що стосуються вимоги письмових доказів і прийнят-

Рекомендація № R (95) 13 Комітету Міністрів держав-членів Ради Європи...

ності відтворення електронних документів і записів, Рекомендацію № R. (85) 10 щодо судових доручень про зняття інформації з телекомунікаційних систем, Рекомендацію № R (87) 15 щодо використання особистих даних у поліцейському секторі та Рекомендацію № R (89) 9 щодо злочинів, пов'язаних з використанням електронно-обчислювальної техніки, рекомендує урядам держав-членів:

- i) при перегляді їхнього внутрішнього законодавства та практики керуватися принципами, що викладені у додатку до цієї рекомендації; та
- ii) забезпечити поширення цих принципів серед слідчих органів та інших професійних організацій, зокрема у сфері інформаційних технологій, які можуть бути залікавленими у їхньому застосуванні.

ДОДАТОК ДО РЕКОМЕНДАЦІЇ № R (95) 13 ЩОДО ПРОБЛЕМ КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНОГО ПРАВА, ПОВ'ЯЗАНИХ З ІНФОРМАЦІЙНИМИ ТЕХНОЛОГІЯМИ

1. Рекомендується чітко визначити та застосовувати принципи правової різниці між обшуком комп'ютерних систем, конфіскацією даних, що у них зберігаються, та зняттям інформації у ході її передачі.
2. Рекомендується, щоб кримінально-процесуальні закони дозволяли слідчим органам проводити обшук комп'ютерних систем і конфіскувати дані на схожих умовах і відповідно до традиційних повноважень обшуку та конфіскації. Рекомендується інформувати особу, відповідальну за систему, про проведений обшук і вид інформації, який було конфісковано. Засоби правового захисту, що забезпечуються в цілому проти обшуку та конфіскації, мають так само застосовуватися і у випадку обшуку комп'ютерних систем чи конфіскації даних, що у них знаходяться.
3. Під час проведення обшуку рекомендується, щоб слідчі органи мали повноваження, які підпадають під дію відповідних засобів безпеки, поширювати такий обшук і на інші комп'ютерні системи у їхній юрисдикції, якщо такі системи підключені до мережі, та конфіскувати інформацію в таких системах за умови необхідності негайних дій.
4. У випадках, коли інформація, отримана шляхом автоматичної обробки даних, функціонально відповідає традиційному документу, рекомендується застосовувати такі самі положення кримінально-процесуального законодавства, що стосуються обшуку та конфіскації документів.
5. З огляду на конвергенцію інформаційних і комунікаційних технологій, рекомендується, щоб закони, які стосуються ведення технічного спостереження для цілей кримінального розслідування, такі як зняття інформації з телекомунікаційних систем, були переглянуті зі внесенням у разі необхідності відповідних поправок для забезпечення можливості їх застосування.

6. Рекомендуються, щоб закон дозволяв слідчим органам користуватися у ході розслідування злочинів усіма необхідними технічними засобами для забезпечення збору інформації, що надходить у потоці даних.

7. У випадках, коли інформацію отримано у ході кримінального розслідування та, зокрема, шляхом її зняття з телекомунікаційних мереж, дані, які підпадають під правовий захист, і проходять обробку в комп'ютерній системі, мають бути належним чином захищені.

8. Рекомендуються переглянути кримінально-процесуальне законодавство з огляду на те, щоб зробити можливим зняття інформації з телекомунікаційних мереж і збір інформації, що надходить у потоці даних, у ході розслідування тяжких злочинів проти конфіденційності, цілісності та доступності телекомунікаційних чи комп'ютерних систем.

9. При належному дотриманні законних прав і забезпеченні захисту більшість правових систем дозволяють слідчим органам наказувати іншим особам передавати їм об'єкти, що перебувають під їхнім контролем і які потрібні для того, щоб служити доказами. Таким самим чином рекомендується внести положення щодо повноваження наказувати особам надавати будь-які конкретні дані, що перебувають під їхнім контролем у комп'ютерній системі у формі, що вимагається слідчими органами.

10. При належному дотриманні законних прав і забезпеченні захисту рекомендується, щоб слідчі органи мали повноваження наказувати особам, які мають дані у комп'ютерній системі, що перебувають під їхнім контролем, надавати їм усю інформацію, необхідну для забезпечення доступу до комп'ютерної системи та даних, що зберігаються у них. Рекомендується, щоб кримінально-процесуальним законом передбачалося, що схожий наказ може видаватися іншим особам, які володіють знаннями щодо функціонування комп'ютерної системи чи засобів захисту даних, що знаходяться у них.

11. Рекомендуються встановити конкретні вимоги до операторів промисловості, користуватися всіма необхідними технічними засобами, що дають можливість слідчим органам знімати інформацію з телекомунікаційних систем.

12. Рекомендуються встановити конкретні вимоги до сервіс-провайдерів, які пропонують телекомунікаційні послуги промисловості чи то через громадські, чи то через приватні мережі, забезпечувати інформацію для ідентифікації користувача при наявності відповідного розпорядження компетентного слідчого органу.

13. Рекомендуються визнати загальну потребу збирати, зберігати та представляти електронні докази у такий спосіб, щоб це якнайкраще забезпечувало та відображало їхню цілісність і незаперечну достовірність як для цілей внутрішнього переслідування, так і для міжнародної співпраці. Таким чином, рекомендується вдосконалити процедури та технічні методи обробки електронних доказів, зокрема, у такий спосіб, щоб забезпечити їхню сумісність між державами. Рекомендується, щоб положення кримінально-процесуального законодавства щодо доказів, які стосуються тра-

диційних документів, застосовувалися у такий же спосіб і до інформації, що зберігається у комп'ютерній системі.

14. Рекомендуються розглянути заходи мінімізації негативних наслідків використання криптографії при розслідуванні кримінальних злочинів без впливу на її легітимне застосування у більшій, ніж строго необхідній мірі.

15. Рекомендуються постійно слідкувати за ризиками, пов'язаними з розвитком і застосуванням інформаційних технологій щодо вчинення кримінальних злочинів. Для забезпечення постійної поінформованості компетентних органів про нові явища у сфері злочинів, пов'язаних із використанням електронно-обчислювальної техніки, та розробки відповідних контрзаходів рекомендується продовжити збір і аналіз інформацію про ці злочини, включаючи інформацію про способи вчинення та їхні технічні аспекти.

16. Рекомендуються розглянути можливість встановлення спеціалізованих відділів для розслідування злочинів, боротьба проти яких вимагає спеціальних знань у галузі інформаційних технологій. Рекомендується розробляти навчальні програми, які дали б можливість персоналу, який займається питаннями кримінального правосуддя, скористатися такими знаннями.

17. Рекомендуються, щоб повноваження поширювати розслідування на інші комп'ютерні системи, застосовувалося і у випадках, коли система розташована в іноземній юрисдикції за умови необхідності негативних дій. Для уникнення можливих порушень державного суверенітету чи норм міжнародного права, рекомендується встановити недвозначні правові норми для таких розширеного обшуку та конфіскації. Таким чином, існує нагальна потреба у проведених переговорів про укладення міжнародних договорів щодо того, як, коли та до якої міри такий обшук та конфіскація можуть бути дозволеними.

18. Рекомендуються встановити прискорені та адекватні процедури, а також систему зв'язку, відповідно до яких слідчі органи можуть звертатися до іноземних органів із проханням негайно зібрати докази. Для цього органи, до яких надходить такий запит, мають бути уповноваженими проводити обшук комп'ютерної системи та конфісковувати інформацію з наміром її подальшої передачі. Рекомендується, щоб органи, до яких надійшов відповідний запит, були уповноваженими забезпечувати дані щодо потоку інформації, яка має відношення до конкретної телекомунікаційної системи, знімати інформацію з конкретної телекомунікаційної системи та встановлювати її джерело. Для цих цілей існує потреба доповнення наявних засобів взаємної правової допомоги.

**РЕКОМЕНДАЦІЯ № R (99) 5
КОМІТЕТУ МІНІСТРІВ
ДЕРЖАВАМ-ЧЛЕНАМ РАДИ ЄВРОПИ
ЩОДО ЗАХИСТУ НЕДОТОРКАНОСТІ ПРИВАТНОГО ЖИТТЯ
В ІНТЕРНЕТІ, ЯКОЮ ЗАТВЕРДЖЕНІ
КЕРІВНІ ПРИНЦИПИ ЗАХИСТУ ОСОБИ СТОСОВНО ЗБОРУ
ТА ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ
НА ІНФОРМАЦІЙНИХ МАЙСТРАЛЯХ**

*(Затверджено Комітетом міністрів від 23 жовтня 1999 року на 660-му
засіданні Постійних представників при Раді Європи)*

Прембула

Комітет Міністрів на підставі повноважень, визначених статтею 15.b Статуту Ради Європи (994_001), враховуючи те, що ціль Ради Європи полягає в досягненні більшої єдності між його членами;

беручи до уваги розвиток нових технологій, нових засобів передачі інформації й інтерактивних послуг;

розуміючи, що такий розвиток вплине на діяльність суспільства у цілому і на взаємини між людьми, зокрема, надаючи розширені можливості передачі й обміну інформацією на національному і міжнародному рівнях;

усвідомлюючи переваги, що отримують користувачі нових технологій при такому розвитку;

враховуючи, однак, те, що технологічний розвиток і широкое розповсюдження збору та обробки персональних даних на інформаційних маїстралях тягне за собою небезпеку порушення недоторканності приватного життя особи;

беручи до уваги те, що технологічний розвиток також створює можливість внести вклад у дотримання основних прав і свобод і, особливо, права особи на недоторканність приватного життя при обробці персональних даних;

усвідомлюючи необхідність розвитку методів, що забезпечують анонімність суб'єктів даних і конфіденційність інформації, яка циркулює на інформаційних маїстралях, при дотриманні прав і свобод інших осіб;

усвідомлюючи, що передача інформації, за допомогою використання нових інформаційних технологій, не повинна порушувати права й основні свободи людини, зокрема права на недоторканність приватного життя і таємниці листування, як це гарантовано статтею 8 Європейської конвенції про права людини (995_004);

усвідомлюючи, що збір, обробка, а особливо передача персональних даних з використанням нових інформаційних технологій по інформаційних маїстралях регулюються положеннями Конвенції про захист осібистості при автоматизованій обробці персональних даних (Страсбург 1981, серією європейських договорів № 108) (994_326) і, як правило, приватними

рекомендаціями із захисту даних. Рекомендації № R (90) 19 про захист персональних даних, використовуваних при платежах та інших суміжних операціях. Рекомендацією № R (91) 10 про передачу третім особам персональних даних, що знаходяться у віданні державних організацій, і Рекомендацією № R (95) 4 про захист персональних даних у сфері телекомунікацій, особливо в телефонії;

враховуючи те, що варто поінформувати користувачів і постачальників послуг Інтернету про основні положення згаданої вище Конвенції (994_326) при зборі та обробці персональних даних на інформаційних маїстралях;

рекомендує урядам держав-членів Ради Європи широко розповсюдити Додаток до даних рекомендацій, особливо серед користувачів та постачальників послуг Інтернету, а також для всіх органів, відповідальних за нагляд та забезпечення захисту даних.

**ДОДАТОК ДО РЕКОМЕНДАЦІЇ № R (99) 5
КОМІТЕТУ МІНІСТРІВ
ДЕРЖАВАМ-ЧЛЕНАМ РАДИ ЄВРОПИ
ПО ЗАХИСТУ НЕДОТОРКАНОСТІ ПРИВАТНОГО ЖИТТЯ
В ІНТЕРНЕТІ**

Керівні принципи щодо захисту особистості при зборі та обробці персональних даних на інформаційних маїстралях, що можуть бути включені чи додані до кодексів поведінки

1. Вступ

У даному документі викладені принципи забезпечення недоторканності приватного життя для користувачів і постачальників послуг Інтернету¹. Ці принципи можуть бути враховані в кодексах поведінки.

Користувачі повинні бути інформовані про обов'язки постачальників послуг Інтернету, і навпаки. Тому доцільно, щоб користувачі і постачальники послуг прочитали весь цей документ, хоча для полегшення використання він поділений на декілька частин. Вас може стосуватись одна або більше частин даного керівництва.

Використання Інтернету покладає відповідальність на всі ваші дії і створює небезпеку для недоторканності приватного життя. Важливо поводити себе так, щоб забезпечити власний захист і підтримувати нормальні відносини з іншими. Даний документ пропонує деякі практичні методи забезпечення недоторканності приватного життя, але вам також слід знати ваші права та обов'язки, визначені законом.

Пам'ятайте, що повага до недоторканності приватного життя — це основне право, яке має захищатися законом, зокрема законодавством по захисту даних, і тому варто уточнити Ваш юридичний статус.

¹ Див. главу IV, п.1

II. Користувачам

1. Пам'ятайте, що Інтернет — не безпечна мережа. Однак існують і розробляються різні засоби, що дозволяють підвищити захист ваших даних². Тому використовуйте всі доступні засоби для захисту ваших даних та ліній зв'язку, як, наприклад, легально доступні засоби шифрування для конфіденційної електронної пошти, так і коди доступу до вашого власного персонального комп'ютера³.

2. Пам'ятайте, що будь-яка ваша трансакція, будь-яке відвідування сайту залишає в Інтернеті сліди. Подібні «електронні сліди» можуть бути використані без вашого відома, для створення профілю про вас і ваших інтересів. Якщо ви не бажаєте такого збору інформації, то варто використовувати новітні технічні досягнення, що дозволяють проінформувати вас про будь-який випадок можливості «слідів», і відмовитися від подальших дій. Також ви можете подати інформаційний запит про методи забезпечення недоторканності приватного життя, наданих різними програмами і сайтами, і віддати перевагу тим із них, які реєструють мінімум даних про користувача або можуть бути доступні анонімно.

3. Найкращий спосіб забезпечення недоторканності приватного життя — це анонімний доступ і анонімне використання послуг, анонімні засоби здійснення платежів. Там де це можливо, з'ясовуйте наявність технічних засобів забезпечення анонімності⁴.

4. Повна анонімність не завжди можлива через законодавчі обмеження. У такому випадку, якщо це дозволено законом, ви можете використовувати псевдонім, що дозволить знати ваші персональні дані тільки постачальникові послуг Інтернету.

5. Повідомляйте вашому постачальникові послуг Інтернету чи будь-кому тільки ті дані, які необхідні для виконання певних дій, про які ви поінформовані. Особлива обережність необхідна при використанні кредитних карток і номерів рахунків, які в Інтернеті можуть легко стати об'єктом зложивань.

6. Пам'ятайте, що ваша адреса електронної пошти є інформацією персонального характеру і сторонні особи можуть її використовувати, наприклад, для вклучення в довідники чи списки користувачів. Не соромтеся запитувати про призначення такого довідника. При бажанні ви можете зажадати виключення даних про себе з подібних довідників і списків.

7. З обережністю ставтеся до сайтів, де у вас просять інформацію особистого характеру більшу, ніж це потрібно для доступу чи здійснення трансакції, чи де не говорять, для чого така інформація необхідна.

8. Пам'ятайте, що ви несете відповідальність перед законом за обробку даних, наприклад, якщо ви незаконно завантажили чи вивантажили дані.

² Термін «дані» відноситься до «персональних даних» і означає будь-яку інформацію про вас чи про інших осіб.

³ Наприклад, використовуйте паролі і регулярно змінюйте їх.

⁴ Наприклад, при використанні інтернет-кіосків, препейд карт, доступу чи платіжних карт.

Усі ці дії можуть бути відстежені навіть при використанні вами псевдоніма.

9. Не розсилайте електронні поштові повідомлення зловмисного змісту. Це може призвести до переслідування згідно із законом.

10. Ваш постачальник послуг Інтернету несе відповідальність за правильне використання персональних даних. Запитайте вашого постачальника послуг Інтернету про те, як, з якою метою і які дані про вас він накопичує, обробляє і зберігає. Періодично відновлюйте такий запит. Напопайте на зміні постачальника ваших даних, якщо вони несправильні, чи на видаленні, якщо вони надлишкові, просторочені чи більше не вимагаються. Вимагайте, щоб постачальник сповістив про таку модифікацію всі сторони, яким ваші персональні дані передавались⁵.

11. Якщо вас не влаштовує те, як ваш постачальник послуг Інтернету накопичує, використовує, зберігає і поширює дані, і при цьому він нічого не змінює, задумайтеся про зміну постачальника послуг. Якщо ви вважаєте, що постачальник не забезпечує захист персональних даних, ви можете поінформувати компетентні органи або розпочати передбачені законом дії.

12. Намагайтеся бути в курсі ризиків недоторканності приватного життя та безпеки в Інтернеті і методів зниження таких ризиків.

13. Відправляючи персональні дані в іншу країну ви повинні врахувати, що там вони можуть виявитися менш захищеними. У випадку, якщо йдеться тільки про ваші персональні дані, ви маєте право приймати будь-яке рішення. Однак, якщо ви передаєте не власні персональні дані в іншу країну, вам слід подати запит до, наприклад, компетентних органів, які відповідають за захист даних у вашій країні, про те, чи припустима така передача⁶. Вам варто зажадати приймаючу сторону вжити заходів⁷, необхідних для забезпечення захисту персональних даних.

III. Постачальникам послуг Інтернету

1. Використовуйте відповідні процедури і доступні технології, переважно сертифіковані, для забезпечення недоторканності приватного життя особистості (навіть якщо вони не є користувачами Інтернету), особливо шляхом забезпечення цілісності і конфіденційності поряд із забезпеченням фізичної і логічної безпеки мережі і послуг, наданих у мережі.

⁵ Закони про захист даних, відповідно до статті 5 Конвенції Ради Європи про захист особистості при автоматизованій обробці персональних даних (№ 108) (994/326), повинні передбачати відповідальність за точність і актуальність даних з боку особи, що здійснює їх обробку.

⁶ Закони багатьох європейських держав забороняють передачу даних у країни, де не забезпечений адекватний чи еквівалентний рівень захисту. Однак допускаються винятки, зокрема, якщо суб'єкт даних дозволив передачу його/її даних у таку країну.

⁷ Ці заходи захисту можуть бути розроблені і/чи представлені в контракті на транс-кордонну передачу даних.

2. Попередньо інформуйте користувачів при їхній підписці на послугу чи початком обслуговування про ризики недоторканності приватного життя при використанні Інтернету. Подібні ризики можуть бути пов'язані з порушенням цілісності даних, конфіденційності, безпеки чи мережі зі схожим та нагромадженням збором персональних даних.

3. Інформуйте користувача про технічні засоби, що він/вона можуть використовувати на законній підставі для зниження ризиків порушення безпеки даних і їхньої передачі, наприклад про дозволені засоби шифрування і цифрового підпису. Пропонуйте подібні технічні засоби на комерційній основі, не зловживаючи цінами.

4. Перед підпискою користувачів і наданням доступу до Інтернету інформуйте їх про можливість анонічного доступу до мережі з анонімною оплатою послуг (наприклад, препейд карти доступу). Через законодавчі обмеження повна анонімність не завжди може бути можлива. У такому випадку, якщо закон дозволяє, надавайте можливість користувачеві використовувати псевдоніми. Інформуйте користувачів про програмні засоби анонічного пошуку і перегляду інформації в Інтернеті. Проєктуйте свою систему таким чином, щоб уникнути чи мінімізувати використання персональних даних.

5. Не читайте, не змінюйте чи не видаляйте повідомлення, передані іншим особам.

6. Не допускайте ніякого втручання у вміст переданих даних, якщо тільки це не передбачено законом і не здійснюється державними органами.

7. Накопичуйте, обробляйте і зберігайте персональні дані користувачів тільки тоді, коли це необхідно для ясних, точно визначених і законних цілей.

8. Не передавайте персональні дані, якщо така передача не підкріплена законодавчо⁸.

9. Не зберігайте персональні дані довше, ніж це необхідно для цілей обробки⁹.

10. Не використовуйте персональні дані для власної рекламної чи маркетингової діяльності, якщо поінформований про ваші наміри користувач заперечує проти цього чи якщо у випадку обробки переданих чи спеціальних категорій даних, він/вона не дав чіткої згоди.

11. Ви відповідаєте за належне використання персональних даних. На вашій вступній сторінці подавайте чітку інформацію про вашу політику в частині забезпечення недоторканності приватного життя. Ця інформація повинна мати посилення на детальне роз'яснення такої політики. Перш

⁸ У цілому закони про захист даних дозволяють передачу третім особам за певних умов, зокрема про спеціальні категорії даних і даних про графік, у випадку якщо особа, якої вони стосуються, дала чітку згоду; про інші дані, там, де їхня передача необхідна для реалізації законних цілей, чи де особа, якої стосуються дані, була поінформована і не заперечує.

⁹ Наприклад, не зберігаєте дані про рахунки довше, ніж це необхідно за законом.

ніж користувач почне користатися вашими послугами, коли він/вона видає ваш сайт чи при будь-якому його/її запиті, поінформуйте його/її про те, хто ви, які персональні дані ви накопичуєте, обробляєте і зберігаєте, як ви це робите, з якою метою і як довго ви їх зберігаєте. Якщо необхідно, подайте запит щодо згоди користувача. При запиті користувача негайно випрадійте його неправильні дані і видаляйте їх, якщо вони надлишкові, просторочені чи більше не вимагаються, і припиняйте їх обробку за вимогою користувача. Повідомляйте третю сторону, з якою ви взаємодієте, про будь-яку модифікації. Уникайте прихованого збору персональних даних.

12. Інформація, надана користувачеві, повинна бути точною та актуальною.

13. Ретельно подумайте перед опублікуванням персональних даних на вашому сайті! Подібна публікація може порушити недоторканність приватного життя інших людей і, крім того, може бути заборонена законом.

14. Перед передачею даних в іншу країну подайте запит до, наприклад, компетентних органів вашої країни, чи дозволена така передача¹⁰. Вам слід просити приймаючу сторону вжити необхідних заходів захисту персональних даних.

IV. Пояснення і засоби правового захисту

1. Там, де в тексті використовується термін «постачальник послуг Інтернету», усе сказане стосується й інших учасників Інтернету, таких як постачальники доступу (access providers), контент-провайдери (content providers), постачальники мережних послуг (network providers), розроблювачі програмних засобів навігації, оператори електронних дошок оголошень і т. ін.

2. Важлива гарантія того, що ваші права поважаються. Механізми відповідних дій, які пропонуються групами користувачів Інтернету (Internet user groups), асоціаціями постачальників послуг Інтернету (Internet service provider association), органами влади, відповідальними за захист даних, чи іншими органами, які є надзвичайно важливими гарантіями виконання даних рекомендацій.

Встановіть контакт зі згаданими організаціями й органами у випадку, якщо необхідні пояснення і засоби правового захисту.

3. Ці рекомендації поширюються на всі типи інформаційних магистралей.

¹⁰ Див. примітку 6.

РЕКОМЕНДАЦІЯ № (2001) 8 КОМІТЕТУ МІНІСТРІВ

ДЕРЖАВАМ-ЧЛЕНАМ РАДИ ЄВРОПИ ЩОДО САМОРЕГУЛЮВАННЯ ЗМІСТУ ЕЛЕКТРОННОЇ ІНФОРМАЦІЇ (САМОРЕГУЛЮВАННЯ ТА ЗАХИСТ СПОЖИВАЧІВ ВІД НЕЛЕГАЛЬНОГО АБО ШКІДЛИВОГО ЗМІСТУ ІНФОРМАЦІЇ У НОВИХ КОМУНІКАЦІЯХ ТА ІНФОРМАЦІЙНИХ ПОСЛУГАХ)

*(Схвалено Комітетом міністрів 5 вересня 2001 року на 762-му
засіданні заступників міністрів)*

Комітет міністрів згідно зі статтею 15.b Статуту Ради Європи, беручи до уваги, що завдання Ради Європи полягає у досягненні більшої єдності держав-членів для цілей охорони та впровадження ідеалів і принципів, що є їхнім спільним надбанням;

беручи до уваги Декларацію Ради Європи про європейську політику в галузі нових інформаційних технологій, схвалену з нагоди 50-ї річниці заснування Ради Європи у 1999 році;

пам'ятаючи про захист, який держави-члени зобов'язалися надавати основному праву на свободу слова та самовираження, як воно гарантовано статтею 10 Конвенції про захист прав і основних свобод людини, нагляд за дотриманням якої покладено на Європейський Суд з прав людини;

підтверджуючи знову, що свобода слова та самовираження є необхідною для соціально-економічного та культурно-політичного розвитку кожної людини, а також є умовою гармонійного і прогресивного розвитку соціально-культурних груп, націй та міжнародного співтовариства, як це виражено в Декларації про свободу слова та інформації 1982 року;

підкреслюючи, що безперервний розвиток нових комунікаційно-інформаційних послуг має сприяти праву кожного, незалежно від кордонів, на самовираження, пошук, отримання й передачу інформації та поглядів на користь кожної особи та демократичної культури будь-якого суспільства;

підкреслюючи, що свобода використання нових комунікаційно-інформаційних послуг не повинна завдавати шкоди людській гідності, правам людини та основним свободам інших, особливо меншин;

пам'ятаючи про свої Рекомендації № R (89) 7 щодо принципів поширення відеограм, які містять сцени насильства, жорстокості та порнографії, Рекомендацію № R (92) 19 щодо відеої р расистського змісту, Рекомендацію № R (97) 19 про зображення жорстокості в електронних ЗМІ, Рекомендацію № R (97) 20 про звернення, які виражають ненависть, і пункт «а» статті 4 Міжнародної конвенції ООН про усунення всіх форм расової дискримінації 1965 року;

пам'ятаючи про різницю в підходах національного кримінального права до незаконного змісту інформації, а також різницю у визначенні потенційно шкідливої інформації, особливо для неповнолітніх та їхнього фізичного, куль-

Рекомендація № R (2001) 8 Комітету Міністрів державам-членам Ради Європи...

турного і морального розвитку, що надалі визначається, як «шкідлива інформація»;

пам'ятаючи про те, що організації з питань саморегулювання могли б, згідно з умовами та традиціями, бути залученими до моніторингу дотримання певних норм, можливо, у рамках співрегулювання, так, як це визначено у конкретній країні;

усвідомлюючи ініціативи з саморегулювання, спрямовані на усунення незаконної інформації та захист користувачів від шкідливої інформації, які виявляють переважки комунікаційно-інформаційного сектору, інколи у співпраці з державою, а також існування технічних стандартів та принципів, які дають користувачам можливість вибирати та фільтрувати інформацію; прагнучи сприяти та посилювати саморегулювання та захист користувачів від незаконної та шкідливої інформації, рекомендує урядам держав-членів:

1. Впроваджувати у їхнє національне законодавство та (або) практику принципи, що містяться в Додатку до цієї Рекомендації;
2. Широко розповсюджувати цю Рекомендацію та принципи, які містяться в Додатку до неї, де потрібно, з рекламою; і
3. Довести їх до відома засобів масової інформації, представників комунікаційно-інформаційного сектору, користувачів та їх асоціацій, а також регуляторних органів у галузі масової інформації та нових комунікаційно-інформаційних послуг і відповідних державних органів.

ДОДАТОК ДО РЕКОМЕНДАЦІЇ № (2001) 8 ПРИНЦИПИ ТА МЕХАНІЗМИ САМОРЕГУЛЮВАННЯ І ЗАХИСТУ КОРИСТУВАЧІВ ВІД НЕЗАКОННОЇ ТА ШКІДЛИВОЇ ІНФОРМАЦІЇ, ЩО ЗАБЕЗПЕЧУЄТЬСЯ НОВИМИ КОМУНІКАЦІЙНО-ІНФОРМАЦІЙНИМИ ПОСЛУГАМИ

Глава I. Організації, які здійснюють саморегулювання

1. Державам-членам рекомендується заохочувати заснування організацій, що представляють суб'єктів інтернет-сектору, наприклад провайдерів інтернет-послуг, контент-провайдерів і користувачів.
2. Державам-членам рекомендується заохочувати такі організації до заснування регулятивних механізмів у межах їхніх повноважень, зокрема щодо введення етичних кодексів і моніторингу дотримання норм цих кодексів.
3. Державам-членам рекомендується заохочувати такі організації у сфері масової інформації, які мають стандарти саморегулювання, до застосування таких стандартів настільки, наскільки можливо, до нових комунікаційно-інформаційних послуг.

4. Державам-членам рекомендується заохочувати такі організації до участі у відповідних законодавчих процесах, наприклад, через консультатції, слухання та здійснення експертного аналізу, а також впровадження відповідних норм, зокрема, шляхом моніторингу дотримання цих норм.

5. Державам-членам рекомендується заохочувати співпрацю між такими організаціями на території всієї Європи та на міжнародному рівні.

Глава II. Контент-дескриптори

6. Державам-членам рекомендується заохочувати визначення комплексу контент-дескрипторів у найширшому можливому географічному масштабі та у співпраці з організаціями, зазначеними у главі I, для нейтрального маркування змісту інформації, щоб користувачі самі могли приймати власні рішення щодо такої інформації.

7. Такі контент-дескриптори повинні позначати, наприклад, інформацію жорсткого та порнографічного характеру, а також інформацію, що спонукає до вживання тютюну чи алкоголю, рекламу послуг з азартних ігор чи створене можливості для неконтрольованих і анонімних контактів між неповнолітніми та дорослими.

8. Рекомендується заохочувати контент-провайдерів до застосування таких контент-дескрипторів, щоб дати користувачам можливість розпізнавати та відфільтровувати таку інформацію, незалежно від її походження.

Глава III. Засоби відбору інформації за змістом

9. Державам-членам рекомендується заохочувати розробку широкого спектра засобів пошуку та параметрів фільтрування, що забезпечують користувачів можливістю відбирати інформацію за змістом на основі контент-дескрипторів.

10. Користувачі здійснюють фільтрування на добровільних засадах.

11. Державам-членам рекомендується заохочувати контент- і сервіс-провайдерів до використання засобів доступу на певних умовах щодо інформації, зміст якої може бути шкідливим для неповнолітніх. Таким засобами можуть бути системи верифікації віку, персональні ідентифікаційні коди, паролі, системи кодування та декодування або доступ за допомогою карток з електронним кодом.

Глава IV. Системи скарг на зміст інформації

12. Державам-членам рекомендується заохочувати встановлення систем скарг на зміст інформації, наприклад гарячих ліній, що мають забезпечуватися провайдерми інтернет-послуг, контент-провайдерами, асоціаціями користувачів та іншими організаціями. Рекомендується, щоб такі системи скарг на зміст інформації, де необхідно для забезпечення адекватного реагування проти незаконного змісту інформації, доповнювалися гарячими лініями державних органів влади.

13. Державам-членам рекомендується заохочувати розробку спільних мінімальних вимог та практики стосовного таких систем скарг на зміст

інформації. Рекомендується, щоб ці вимоги включали, наприклад, таке:

- а) забезпечення конкретної та постійної адреси в Інтернеті;
- б) цілодобова доступність систем скарг на зміст інформації;
- с) забезпечення громадськості інформацією про відповідальних осіб і відділи в організаціях, що пропонують системи скарг на зміст інформації;
- д) забезпечення громадськості інформацією про норми та практику, що стосується обробки скарг на зміст інформації, включаючи співпрацю з правоохоронними органами щодо потенційно незаконного змісту інформації;
- е) надання відповідей користувачам стосовно обробки їхніх скарг на зміст інформації;
- ф) забезпечення зв'язку з іншими системами скарг на зміст інформації за кордоном.

14. Державам-членам рекомендується встановлювати на національному рівні належні рамки співпраці між організаціями, відповідальними за обробку скарг на зміст інформації, та органами державної влади щодо потенційно незаконного змісту інформації. Для цих цілей державам-членам рекомендується визначити правові обов'язки та переважні права організацій, що пропонують системи скарг на зміст інформації, при доступі, копіюванні, збиранні та пересиланні інформації потенційно незаконного змісту правоохоронним органам.

15. Державам-членам рекомендується сприяти співпраці між організаціями, які приймають скарги на зміст інформації, на всій території Європи та на світовому рівні.

16. Державам-членам рекомендується вживати всіх необхідних правових та адміністративних заходів для транскордонної співпраці між відповідними правоохоронними органами стосовно скарг і розслідувань щодо інформації потенційно незаконного змісту, яка надходить із-за кордону.

Глава V. Медіація та арбітраж

17. Державам-членам рекомендується заохочувати створення на національному рівні добровільні, справедливі, доступні та ефективні органи та процедури для позасудової медіації, а також механізми арбітражного вирішення спорів, які стосуються питань, пов'язаних зі змістом.

18. Державам-членам рекомендується заохочувати співпрацю на всій території Європи та міжнародному рівні, відкритий доступ кожного до таких процедур медіації та арбітражу, незалежно від кордонів, і взаємного визнання та впровадження позасудових рішень, досягнутих за допомогою таких процедур, відповідно до національних норм громадського правопорядку і основних процесуальних гарантій.

Глава VI. Інформація для користувачів та поширення такої інформації

19. Державам-членам рекомендується заохочувати розробку марок змісту інформації, що поширюється через Інтернет, наприклад для позначення уря-

дової інформації, інформації освітнього характеру та інформації, зміст якої є прийнятним для дітей, щоб дати користувачам можливість розпізнавати та знаходити таку інформацію.

20. Державам-членам рекомендується заохочувати поширення інформації серед широкої громадськості про механізми саморегулювання, контент-дескриптори, засоби фільтрування інформації, засоби обмеження доступу, системи скарг на зміст інформації та процедури позасудової media-ції та арбітражу.

РЕКОМЕНДАЦІЯ № R (2002) 2 ПРО ДОСТУП ДО ОФІЦІЙНИХ ДОКУМЕНТІВ

*(ухвалена Комітетом міністрів 21 лютого 2002 року
на 784-му засіданні заступників міністрів)*

Комітет міністрів, відповідно до пункту b статті 15 Статуту Ради Європи,

вважаючи, що метою Ради Європи є досягнення більшого єднання між її членами задля забезпечення та реалізації ідеалів та принципів, що є їхнім спільним надбанням;

пам'ятаючи, зокрема, про статтю 19 Загальної декларації прав людини, статті 6, 8 та 10 Європейської конвенції з прав людини та основних свобод, Конвенції ООН про доступ до інформації, участь громадськості в процесі вироблення рішень та доступі до правосуддя в питаннях, коли йдеться про захист довкілля (ухвалена в Аартусі, Данія, 25 червня 1998 року) та Конвенцію про захист осіб стосовно автоматизованої обробки даних особистого характеру від 28 січня 1981 року (ETS № 108); Декларацію про свободу вираження поглядів та інформації, ухвалену 28 січня 1982 року, а також Рекомендацію № R (81) 19 про доступ до інформації, яка знаходиться в розпорядженні органів державної влади, Рекомендацію № R (91) 10 про повідомлення третім сторонам даних персонального характеру, які зберігаються в державних органах, Рекомендацію № R (97) 18 щодо захисту даних персонального характеру, які збираються та записуються для статистичних цілей а також Рекомендацію № R (2000) 13 стосовно європейської політики в питанні доступу до архівів;

зважаючи на важливість у плюралістичному та демократичному суспільстві відкритості органів державної влади та готовності їх надавати інформацію щодо питань, які становлять суспільний інтерес;

зазначаючи те, що широкий доступ до офіційних документів на основі рівноправності та відповідно до чітких правил:

— дозволяє громадянам виробити адекватне бачення та сформуувати критичні погляди щодо стану суспільства, у якому вони живуть, та щодо органів влади, які ними керують, тим самим заохочуючи громадян до поінформованої участі в питаннях, що становлять спільний інтерес;

— сприяє більшій дієвості та ефективності адміністративних органів і допомагає підтримувати їхню цілісність, усуваючи ризик корупції;

— є чинником, що підтверджує легітимність органів управління як державних служб і посилює довіру громадськості до органів державної влади; стверджуючи, відповідно, що держави-члени повинні докласти максимум зусиль з тим, щоб забезпечити громадянам доступ до інформації, яка міститься в офіційних документах, за умови охорони інших прав та законних інтересів;

підкреслюючи, що викладені нижче принципи є мінімальним стандартом і їх слід сприймати без упередження тими національними законодав-

ствами та підзаконними актами, у яких уже зарез визначається більш широке право доступу до офіційних документів;

важачи, що, оскільки в центрі уваги цього документа є індивідуальні запити щодо доступу до офіційних документів, органи державної влади повинні взяти на себе зобов'язання проводити активну політику в питаннях спілкування з громадянами з тим, щоб надати в розпорядження громадян всю інформацію, яка може вважатися необхідною у відкритому демократичному суспільстві,

рекомендує урядам держав-членів керуватися в їхньому національному законодавстві та практичній діяльності принципами, що викладені в цій Рекомендації.

I. Дефініції

Для цілей цієї Рекомендації:

«**органи державної влади**» означають

- i) уряд та адміністрацію на національному, регіональному або місцевому рівнях;
- ii) фізичну або юридичну особу, яка виконує функції урядування або наділена адміністративними повноваженнями відповідно до національного законодавства.

«**офіційні документи**» означають будь-яку інформацію, яка є записаною в будь-якому вигляді, вироблена або отримана органами державної влади і пов'язана з будь-якою державною або адміністративною функцією, за винятком документів, які перебувають на стадії підготовки.

II. Поле застосування

1. Ця рекомендація застосовується лише до офіційних документів, які знаходяться в розпорядженні органів державної влади. Однак держави-члени мають розглянути у світлі національного законодавства та практики, наскільки викладені в цій Рекомендації принципи можуть бути застосовані до інформації, що знаходиться в розпорядженні органів законодавчої та судової влади.

2. Ця Рекомендація не впливає на право доступу або обмеження в доступі, які передбачені в Конвенції про захист осіб стосовно автоматизованої обробки даних особистого характеру.

III. Загальні принципи доступу до офіційних документів

Держави-члени повинні гарантувати кожній особі після здійснення нею запити право на доступу до офіційних документів, які є в розпорядженні органів державної влади. Цей принцип має застосовуватися без жодної дискримінації, у тому числі й за ознакою державної належності.

IV. Можливі обмеження в доступі до офіційних документів

1. Держави-члени можуть обмежити право доступу до офіційних документів. Обмеження повинні бути чітко визначені в законодавстві, бути необхідними в демократичному суспільстві і пропорційними з метою захисту:

- i) національної безпеки, оборони та міжнародних зв'язків;
 - ii) охорони громадського порядку;
 - iii) запобігання, розшуку та розслідування кримінальної діяльності;
 - iv) приватного життя та інших законних приватних інтересів;
 - v) комерційних та інших економічних інтересів, як приватних, так і державних;
 - vi) рівності сторін у судовому провадженні;
 - vii) природи;
 - viii) інспекцій, контролю та нагляду з боку органів державної влади;
 - ix) державної економічної, монетарної та обмінної політики;
 - x) конфіденційності обговорень всередині органу державної влади або ж між декількома органами державної влади під час внутрішнього процесу вироблення документа.
2. У доступі до документа може бути відмовлено, якщо оприлюднення вміщеної в офіційному документі інформації призводить або може призвести до порушення одного з інтересів, які викладені в пункті I, незважаючи на переважачий інтерес громадськості в такому оприлюдненні.
3. Держави-члени повинні розглянути можливість встановлення часових строків, після закінчення яких припиняється застосування викладених у пункті I обмежень.

V. Запити про доступ до офіційних документів

1. Особа, яка звертається із запитом про офіційний документ, не повинна пояснювати причини, через які вона бажає отримати доступ до офіційного документа.

2. Формальності під час здійснення запити мають бути зведені до мінімуму.

VI. Процедура розгляду заяв про доступ до офіційних документів

1. Запит про доступ до офіційного документа має бути розглянутий будь-яким органом державної влади, у розпорядженні якого перебуває цей документ.

2. Запити про доступ до офіційних документів повинні розглядатися на основі рівноправності.

3. Кожен запит про доступ до офіційного документа має бути розглянутий у короткий термін. Рішення має бути ухвалене, повідомлене та виконане впродовж визначеного строку, який може бути встановлений заздалегідь.

4. Якщо орган державної влади не має у своєму розпорядженні запитованого офіційного документа, він повинен, наскільки це видється можливим, вказати особі, що робить запит, на компетентний орган державної влади.

5. Орган державної влади повинен, наскільки це видається можливим, допомогти особі, яка робить запит, визначити запитуваний документ, однак такий орган не зобов'язаний виконувати запит, якщо йдеться про документ, який не може бути визначений.

6. У запиті про доступ до офіційного документа може бути відмовлено, коли такий запит є вочевидь безглуздим.

7. Орган державної влади, який відмовляє у доступі до цілого офіційного документа або до його частини, повинен навести причини відмови.

VII. Форми доступу до офіційних документів

1. У разі, коли надається доступ до офіційного документа, орган державної влади повинен дозволити ознайомитися з оригіналом документа або ж надати його копію, враховуючи, наскільки це є можливим, преференції, що висловлені особою, яка звертається із запитом.

2. Якщо до якоїсь частини вміщеної в офіційному документі інформації застосовується обмеження, то орган державної влади повинен, тим не менш, надати всю іншу інформацію, що міститься в документі. Кожен випадок не відкриття інформації повинен бути чітко визначеним. Однак у разі, коли версія документа з вирізнаними фрагментами тексту є помилковою за змістом або взагалі позбавлена змісту, то в доступі до документа може бути відмовлено.

3. Орган державної влади може надати доступ до офіційного документа, спрямовуючи особу, яка звертається із запитом, до альтернативних джерел, з яких можна легко отримати інформацію.

VIII. Оплата за доступ до офіційних документів

1. Ознайомлення на місці з офіційним документом повинне бути, у принципі, безкоштовним.

2. Видача копії офіційного документа може бути платною для особи, яка звернулася із запитом, однак ціна має бути розумною і не перевищувати дійсних витрат з боку органів державної влади.

IX. Процедура перегляду

1. Заявник, якому було відмовлено в його запиті про офіційний документ — про окремі його частини або про документ у цілому, запит якого був відхилений або залишився без відповіді впродовж терміну, про який ішлося в принципі VI.3, повинен мати доступ до процедури перегляду в судовому порядку або ж в іншій незалежній та неупередженій встановленій законом інстанції.

2. Заявник повинен завжди мати доступ до швидкої та недорогої процедури перегляду з боку органу державної влади або до перегляду відповідно до викладеного вище пункту 1.

X. Долаткові заходи

1. Держави-члени повинні вжити необхідних заходів з тим, щоб:

- i) інформувати громадян про їхнє право на доступ до офіційних документів та про те, у який спосіб вони можуть ним скористатись;
- ii) забезпечити, щоб офіційні посадові особи проходили необхідну підготовку з питань їхніх зобов'язань та обов'язків з огляду на

запровадження цього права;

iii) забезпечити, щоб заявники могли користуватися цим правом.

2. З цією метою органи державної влади повинні, зокрема:

- i) ефективно вести документацію в такий спосіб, щоб доступ до документів був легким;
- ii) застосовувати чіткі і визначені процедури для збірвання та знищення власних документів;
- iii) наскільки це видається можливим, оприлюднювати інформацію щодо проблематики або діяльності, які належать до їхньої компетенції, наприклад, шляхом підготовки переліку або реєстру документів, що знаходяться в їхньому розпорядженні.

XI. Інформація, яка оприлюднюється з ініціативи органів державної влади

Органи державної влади повинні за своєю власною ініціативою і тоді, коли це є доцільним, вживати необхідних засобів задля оприлюднення інформації, яка є в їхньому розпорядженні в разі, якщо оприлюднення такої інформації здійснюється в інтересах підтримки відкритості адміністративних органів та ефективності взаємодії між різними адміністраціями або ж заохочує широкі кола громадськості до участі в питаннях, що створюють громадський інтерес.

**РЕКОМЕНДАЦІЇ
РАДИ З ЕКОНОМІЧНОГО СПІВРОБІТНИЦТВА ТА РОЗВИТКУ,
ЩО СТОСУЮТЬСЯ ОСНОВНИХ ПОЛОЖЕНЬ
ПРО ЗАХИСТ НЕДОТОРКАНОСТІ ПРИВАТНОГО ЖИТТЯ
І МІЖНАРОДНИХ ОБМІНІВ ПЕРСОНАЛЬНИМИ ДАНИМИ**

(Прийнято 23 вересня 1980 р.)

РАДА ОЕСР,

керуючись статтями 1(c), 3(a) і 5(b) Конвенції про Організацію з економічного співробітництва та розвитку від 14 грудня 1960 р.,

з огляду на те, що, незважаючи на можливі розходження в національних законах і напрямках політики, країни-члени однаковою мірою зацікавлені в захисті недоторканності приватного життя й індивідуальних свобод, а також у знаходженні балансу між такими важливими, але суперечними один одному цінностями, як недоторканність приватного життя і свобода обміну інформацією;

що автоматизовані системи обробки даних і міжнародні обміни персональними даними створюють нові форми відносин між країнами і вимагають розробки сумісних між собою правил і практичних методів роботи; що міжнародні обміни персональними даними сприяють економічному і соціальному розвитку;

що внутрішні закони про захист недоторканності приватного життя і міжнародних обмінів персональними даними можуть ускладнити ці міжнародні обміни;

маючи намір розвивати вільні обміни інформацією між країнами-членами й уникати необґрунтованого створення перешкод на шляху розвитку економічних і соціальних відносин між країнами-членами, рекомендує країнам-членам:

1. Враховувати у своїх внутрішніх законодавствах принципи захисту недоторканності приватного життя й індивідуальних свобод, викладені в Основних положеннях, що містяться в Додатку до даних Рекомендацій, що є невід'ємною частиною згаданих Рекомендацій.
2. Намагатися уникати створення — в ім'я захисту недоторканності приватного життя — необґрунтованих перешкод на шляху міжнародних обмінів персональними даними.
3. Співпрацювати в реалізації Основних положень, викладених у Додатку.
4. Якомога швидше домовитися про розробку конкретних процедур для проведення консультацій і розвитку співпраці з метою практичного виконання даних Основних положень.

**ДОДАТОК
ДО РЕКОМЕНДАЦІЙ РАДИ ОЕСР
від 23 вересня 1980 р.
ОСНОВНІ ПОЛОЖЕННЯ ПРО ЗАХИСТ НЕДОТОРКАНОСТІ
ПРИВАТНОГО ЖИТТЯ І МІЖНАРОДНИХ ОБМІНІВ
ПЕРСОНАЛЬНИМИ ДАНИМИ**

**Частина I
ОСНОВНІ ПОЛОЖЕННЯ**

Визначення

1. В цілях Основних положень:

- а) «**розпорядник даних**» означає особу, яка відповідно до внутрішнього законодавства уповноважена приймати рішення про зміст і використання персональних даних незалежно від того, чи здійснюється збір, збереження, обробка і поширення таких даних нею самою чи особою, що діє від її імені як агент;
- б) «**персональні дані**» означають будь-яку інформацію, що стосується індивідуума («суб'єкта даних»), чия особистість або відома, або може бути встановлена;
- в) «**міжнародні обміни персональними даними**» означають передачу персональних даних через національні кордони.

Сфера застосування Основних положень

2. Ці Основні положення застосовуються до персональних даних як у державному, так і в приватному секторі, які у зв'язку з процедурою їх обробки або у зв'язку з їхнім характером чи контекстом їх використання, містять загрозу порушення недоторканності приватного життя й індивідуальних свобод.

3. Ці Основні положення не слід тлумачити як документ, що створює перешкоди для:

- а) застосування до різних категорій персональних даних різноманітних охоронних заходів залежно від їхнього характеру або контексту, у якому ці дані збираються, зберігаються, чи обробляються та поширюються;
- б) вилучення зі сфери застосування цих Основних положень персональних даних, що явно не несуть у собі загрози для недоторканності приватного життя й індивідуальних свобод;
- в) застосування цих Основних положень тільки до персональних даних, що піддаються автоматизованій обробці.

4. Винятки з Принципів, записаних у частинах II і III цих Основних положень, у тому числі тих, що стосуються національного суверенітету, національної безпеки і державної політики («державного порядку»), повинні бути:

- а) якомога менш численними;
- б) доведені до відома громадськості.

5. У країнах з федеративним устроєм реалізація цих Основних положень може бути укладена поділом владних повноважень усередині федерації.

6. Ці Основні положення варто розглядати як мінімальний набір стандартів, поряд з яким можуть застосовуватися додаткові заходи захисту недоторканності приватного життя й індивідуальних свобод.

Частина II ОСНОВНІ ПРИНЦИПИ, ЩО ЗАСТОСОВУЮТЬСЯ НА НАЦІОНАЛЬНОМУ РІВНІ

Принципи обмеження обсягу даних, що збираються

7. Обсяг персональних даних, що збирається, повинен мати межі; усі ці дані повинні бути отримані законним і чесним шляхом — якщо можливо, то з відомою чи згоди суб'єкта даних.

Принципи якості даних

8. Персональні дані повинні відповідати цілям, у яких вони будуть використовуватися; тією мірою, якою це необхідно відповідно до згаданих цілей, персональні дані повинні бути точними, повними і регулярно поновлюваними.

Принципи конкретизації цілі

9. Цілі, заради яких збираються персональні дані, повинні бути визначені не пізніше моменту збору зазначених даних, а їх наступне використання має обмежуватися досягненням згаданих або подібних (сумісних) цілей, що повинні вказуватися щоразу, коли ці цілі змінюються.

Принципи обмеження використання даних

10. Персональні дані не повинні розголошуватися, надаватися в користування чи іншим чином використовуватися в інших цілях, окрім тих, що перелічені в пункті 9, за винятком випадків, коли:

- а) суб'єкт даних дав на те свою згоду;
- б) це дозволено законом.

Принципи гарантування безпеки

11. Персональні дані повинні бути захищені належними механізмами захисту від ризиків, пов'язаних зі втратою, несанкціонованим доступом, знищенням, використанням чи зміною розголошенням даних.

Принципи відкритості

12. Процес розвитку, а також практика і політика щодо персональних даних повинні здійснюватися в рамках загальної політики відкритості. У постійній готовності повинні бути кошти для встановлення факту наявності і характеру персональних даних, основних цілей їхнього викорис-

тання, а також особистості та звичайного місцезнаходження розпорядників даних.

Принципи індивідуальної участі

13. Індивідуум повинний мати право:

- а) одержувати від розпорядника даних або іншим чином, підтвердження того, чи є в розпорядника даних персональні дані, що стосуються згаданого індивідуума;
- б) одержувати персональні дані, що його стосуються:
 - у розумний термін;
 - без надмірних витрат;
 - у межах розумної процедури;
 - у зручній для розуміння формі;
- в) у випадку відмови задовольнити запит на надання інформації, поданий відповідно до пунктів (а) і (б), одержувати роз'яснення про мотиви відмови й опротестовувати таку відмову;
- г) опротестовувати дані, що стосуються його; у разі задоволення протесту вимагати, щоб такі дані були знищені, виправлені чи доповнені.

Принципи відповідальності

14. Розпорядник даних повинен нести відповідальність за вжиття заходів, що забезпечують дотримання перелічених вище принципів.

Частина III ОСНОВНІ ПРИНЦИПИ ЗАСТОСУВАННЯ НА МІЖНАРОДНОМУ РІВНІ: СВОВОДА ОБМІНУ І ЗАКОНОНІ ОБМЕЖЕННЯ

15. Країни-члени повинні враховувати можливі наслідки, що можуть мати виникнути для інших країн у результаті використання персональних даних усередині країни чи їх реекспорт.

16. Країни-члени повинні вживати розумних і належних заходів для забезпечення того, щоб міжнародні обміни персональними даними, у тому числі їхній транзит через територію кожної країни-члена, були безперешкодними і безпечними.

17. Кожній із країн-членів варто утримуватися від введення обмежень на обміни персональними даними між собою й іншою країною-членом, за винятком випадків, коли остання ще не почала дотримуватися пунктів цих Основних положень, а також під загрозою того, що реекспорт таких даних може призвести до порушення чинних у першій країні внутрішніх законів про недоторканність приватного життя. Країна-член може також вводити обмеження щодо тих категорій персональних даних, щодо яких її внутрішніми законами про недоторканність приватного життя передбачені конкретні правила, пов'язані з характером таких даних, у випадку якщо інша країна-член не забезпечує їхнього еквівалентного захисту.

18. Країнам-членам варто уникати прийняття законів, політичних напрямків і практичних правил в ім'я захисту недоторканності приватного життя й індивідуальних свобод, що можуть створити перешкоди для міжнародних обмінів персональними даними, але тією мірою, яка є необхідною для забезпечення такого захисту.

Частина IV ДОТРИМАННЯ НА НАЦІОНАЛЬНОМУ РІВНІ

19. При дотриманні на національному рівні принципів, викладених у частинах II і III цих Основних положень, країнам-членам варто вводити в дію юридичні, адміністративні чи інші процедури та заходи захисту недоторканності приватного життя й індивідуальних свобод, що стосуються персональних даних. Зокрема, країнам-членам слід:

- а) прийняти належні внутрішні закони;
- б) заохочувати і підтримувати саморегулювання шляхом прийняття кодексів поведінки чи інших правил;
- в) забезпечити наявність розумних механізмів реалізації індивідуальних прав;
- г) передбачити необхідні санкції й інші заходи захисту прав на випадок невиконання заходів, що забезпечують дотримання принципів, перелічених у частинах II і III;
- д) забезпечити недискримінаційне ставлення до суб'єктів даних.

Частина V МІЖНАРОДНЕ СПІВРОБІТНИЦТВО

20. Країнам-членам варто надавати іншим країнам-членам на їхнє прохання детальну інформацію про дотримання принципів, перелічених у цих Основних положеннях. Країнам-членам також варто вживати заходів для того, щоб процедури міжнародних обмінів персональних даними і захисту недоторканності приватного життя й індивідуальних свобод були простими і сумісними з процедурами, прийнятими в інших країнах-членах, що дотримуються цих Основних положень.

21. Країнам-членам варто ввести в дію процедури, що сприяють: — обмінам інформацією, що стосується до цих Основних положень; — взаємодопомоги в здійсненні процедур і проведенні розслідувань з питань, що представляють двосторонній інтерес.

22. Країнам-членам варто розробляти принципи — внутрішні і міжнародні, — на яких будуть базуватися прийняті закони про міжнародні обміни персональними даними.

ОКІНАВСЬКА ХАРТЯ ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

(Прийнята 22 липня 2000 року лідерами країн G8, Окінава)

Інформаційно-телекомунікаційні технології (ІТ) є одним із найбільш важливих факторів, котрі впливають на формування суспільства XXI століття. Їхній революційний вплив стосується способу життя людей, їхньої освіти й роботи, а також взаємодії уряду та громадянського суспільства. ІТ швидко стають життєво важливим стимулом розвитку світової економіки. Вони також надають можливість багатом ініціативним індивідуумам, фірмам та спільнотам у всіх частинах земної кулі більш ефективно і творчо вирішувати економічні та соціальні проблеми. Величезні можливості ІТ мають бути розділені всіма нами.

Сутність стимульованих ІТ економічних та соціальних трансформацій полягає в їхній здатності сприяти людям і суспільству у використанні знань та ідей. Інформаційне суспільство, як ми його уявляємо, є таким, що дозволяє людям краще розвинути свій потенціал та реалізовувати свої прагнення. Для цього ми повинні гарантувати, що ІТ слугуватимуть досягненню взаємодоповнюваних цілей: забезпеченню сталою економічного зростання, підвищенню суспільного добробуту і створення соціальної злагоди. Разом з тим ми маємо докласти всіх зусиль, аби якнайповніше реалізувати потенціал ІТ у сфері укріплення демократії, більш прозорого та відкритого управління, у захисті прав людини і сприянні збереженню культурного розмаїття, а також у збереженні миру та стабільності у всьому світі. Узгодження цих цілей і вирішення проблем, що виникають, вимагає розробки ефективних національних та міжнародних стратегій.

У прагненні досягти цих цілей ми знову підтверджуємо наші зобов'язання стосовно принципів включення до глобальної інформатизації: кожному і будь-де має бути забезпечена можливість участі, ніхто не має бути обійдений перевагами глобального інформаційного суспільства. Стабільність цього суспільства залежить від демократичних цінностей, що сприяють розвитку людини, таких як вільний обмін інформацією й знаннями, взаємна терпимість та повага до особливостей інших людей.

Ми здійснюватимемо керівництво подальшими зусиллями урядів, аби сприяти встановленню кращої політики та регулюючих норм, які б стимулювали конкуренцію й новаторство, гарантуватимемо економічну та фінансову стабільність, поглибимо співпрацю учасників щодо оптимізації Глобальної мережі та боротьби зі зловживаннями, котрі підривають цільність Мережі, а також щодо скорочення розриву в цифрових технологіях, інвестування в людей та забезпечення глобального доступу та участі у процесі будівництва інформаційного суспільства.

Ця Хартія є перш за все закликом до всіх, як у державному, так і в приватному секторах, закликом до ліквідації на міжнародному рівні розриву у рівні використання інформації і знань. Тверда основа політики й дій у сфері ІТ може змінити шляхи нашої взаємодії стосовно поширення економічних і

соціальних можливостей ІТ у всьому світі. Ефективне партнерство учасників, включаючи об'єднані політичні зусилля, також є ключовим елементом праймального розвитку глобального інформаційного суспільства.

Використання можливостей цифрових технологій

Потенційні вигоди ІТ, що полягають у стимулюванні конкуренції, сприянні розширенню виробництва, створенні й підтримці економічного зростання та збільшення зайнятості, відкривають значні перспективи. Наше завдання — не лише заохочувати перехід до інформаційного суспільства та полегшувати цей процес, але також і якомога повніше реалізувати його економічні, соціальні та культурні переваги. Для досягнення цих цілей важливо будувати роботу на таких ключових моментах:

проведення економічних і структурних реформ з метою створення умов відкритості, ефективності, конкуренції та новаторства, котрі доповнювалися би заходами щодо адаптації ринків праці, розвитку людських ресурсів та забезпечення соціальної загоди;

управління макроекономікою, яке допоможе підприємствам та споживачам складати більш точні плани, бути випередішими у майбутньому, ефективніше використовувати переваги нових інформаційних технологій; розробка інформаційних мереж, що забезпечуватимуть швидкий, надійний, безпечний та економічний доступ за допомогою конкурентоспроможного ринку, відповідних нововведень у мережевих технологіях, сервісі та застосуваннях;

розвиток людських ресурсів, спроможних відповідати вимогам інформаційної епохи, готових до навчання протягом усього життя та здатних задовольняти зростаючий попит на фахівців з ІТ у багатьох секторах нашої економіки.

активне використання ІТ державним сектором, сприяння настанню в режимі реального часу послуг, необхідних для гарантування підвищення рівня доступності влади для всіх громадян.

Приватний сектор відіграє провідну роль у розвитку інформаційно-комунікаційних систем в інформаційному суспільстві. Однак завдання створення передбачуваної, прозорої і невідкриміальної політики та нормативної бази, необхідних для інформаційного суспільства, лежить на урядових руках. Важливо уникнути неадекватних регулюючих втручань, котрі заважатимуть виявленню ініціатив приватного сектора щодо створення умов, сприятливих для запровадження ІТ. Ми повинні гарантувати, що правила й процедури стосовно ІТ відповідатимуть революційним змінам в економічній діяльності, враховуватимуть принципи ефективного партнерства між державним і приватним секторами, а також будуть прозорими та технологічно нейтральними.

Аби максимізувати соціальні й економічні вигоди інформаційного суспільства, ми домовляємось про такі ключові принципи й підходи і рекомандуємо їх іншим:

продовжувати сприяти розвитку конкуренції на відкритих ринках у галузі інформаційних технологій та телекомунікаційної продукції і послуг,

включаючи недискримінаційне й орієнтоване лише на вартість підключення до основних телекомунікацій;

захист прав інтелектуальної власності у сфері інформаційних технологій життєво важливий для запровадження ІТ-інновацій, розвитку конкуренції та поширення нових технологій; ми вітаємо спільну роботу, що вже реалізується представниками органів влади щодо захисту прав інтелектуальної власності й нададі заохочуватимемо наших експертів обговорювати напрямки майбутньої роботи в цій сфері;

важливо також відновити зобов'язання урядів щодо використання програмного забезпечення повністю відповідно до принципів захисту інтелектуальної власності;

багато з послуг, серед них і телекомунікації, транспорт та пошта, є виключно важливими для економіки інформаційного суспільства — підвищення саме їхньої ефективності здатне максимізувати вигоди ІТ; митні та інші процедури, пов'язані з торгівлею, так само важливі для створення умов, сприятливих для ІТ;

спростити міжнародну е-торгівлю шляхом подальшої лібералізації та вдосконалення мереж, відповідних послуг і процедур у контексті жорстких рамок Світової організації торгівлі (СОТ), проловоження роботи у сфері е-торгівлі у СОТ та на інших міжнародних форумах, зокрема застосування існуючих торговельних правил СОТ до е-торгівлі;

здійснювати послідовний підхід до оподаткування е-торгівлі, що ґрунтується на звичайних принципах, включаючи нейтралітет, дівість і простоту, інші ключові елементи, укладжені в роботі Організації економічної співпраці та розвитку (ОЕСР);

продовжити практику збільшення електронних переказів від митних зборів чи мінімізації їх до того часу, коли це питання буде знову розглянуто на наступній міністерській конференції СОТ;

сприяти ринковим стандартам, включаючи, наприклад, технічні стандарти функціональної сполучності;

підвищувати довіру споживачів до електронних ринків відповідно до керівних принципів ОЕСР і забезпечувати захист споживача в Мережі, еквівалентний його захисту в звичайних обставинах, серед іншого і за допомогою ефективних ініціатив саморегулювання, таких як кодекси мережевої поведінки, довіра до торгової марки та інші програми підтвердження надійності, а також шляхом вивчення варіантів усунення ускладнень, що з ними стикаються споживачі в міжнародних спорах, включаючи використання альтернативних механізмів розв'язання спорів;

розвивати ефективні та дієві механізми захисту секретності споживачів, а також захисту таємниці обробки персональних даних за збереження вільного інформаційного потоку, а також

надалі розвивати й забезпечувати ефективне функціонування електронної ідентифікації, електронного підпису, криптографії та інших засобів безпеки та надійності операцій.

Зусилля міжнародного співтовариства, спрямовані на розвиток Глобального інформаційного суспільства, мають бути скоординованими, аби

забезпечити безпечний та вільний від злочинності кіберпростір. Ми маємо гарантувати, що буде вжито ефективних заходів — як це вказано у Керівних принципах безпеки інформаційних систем ОЕСР — у боротьбі зі злочинністю в комп'ютерному середовищі. Буде розширено співпрацю країн Вісімки в рамках Ліонської групи з транснаціональної організованої злочинності. Ми будемо й надалі підтримувати діалог з представниками промисловості, розвиваючи, таким чином, успіх, досягнутий на нещодавній Паризькій конференції Вісімки «Діалог уряду та промисловості щодо безпеки та довіри у кіберпросторі». Такі нагальні проблеми безпеки, як хакерство та комп'ютерні віруси, також потребують ефективних політичних рішень. Ми продовжуватимемо залучати промисловість та інших учасників для захисту найважливіших інформаційних інфраструктур.

Подолання електронно-цифрового розриву

Питання подолання електронно-цифрового розриву всередині держав та між ними набуло надзвичайної ваги на національному порядку денному наших країн. Кожен повинен мати можливість доступу до інформації та систем телекомунікації. Ми знову підтверджуємо наші зобов'язання щодо тих зусиль, які зараз вживаються у розробленні та здійсненні дослідовної стратегії, спрямованої на вирішення даного питання. Ми також вітаємо те, що і промисловість, і громадське суспільство дедалі більшою мірою визнають необхідність подолання цього розриву. Мобілізація знань і ресурсів у цій галузі є необхідною умовою для врегулювання даної проблеми. Ми й надалі прагнутимемо до ефективної співпраці між урядами та громадськими суспільствами, яка має чутливо реагувати на високі темпи розвитку технологічних та ринкових подій.

Ключовим компонентом нашої стратегії має бути безперервний рух до рівного доступу для всіх. Ми будемо й надалі: заохочувати встановлення сприятливих ринкових умов для безперешкодного надання населенню всіх можливих послуг телекомунікації; вишукувати додаткові можливості, включаючи доступ через засоби, відкриті для широкої публіки;

надавати пріоритет покращенню доступу до Мережі, особливо у відсталих міських, сільських та віддалених районах; приділяти особливу увагу потребам і обмеженням найменш соціально захищених людей, інвалідів і літніх людей та активно вживати заходів для полегшення їм доступу до мережевих ресурсів та користування ними; сприяти подальшому розвитку «дружніх», «вільних від перешкод» технологій, включаючи мобільний доступ до Інтернету, а також ширшому використанню безкоштовного загальнодоступного інформаційного наповнення та відкритих для всіх користувачів програмних засобів, дотримуючись при цьому прав інтелектуальної власності.

Стратегія розвитку інформаційного суспільства має бути підкріплена розвитком людських ресурсів, здатних відповісти на вимоги інформаційної доби. Ми досягнемо того, що всі наші громадяни матимуть можливість набувати й удосконалювати IT-грамотність та навички шляхом освіти й

навчання протягом усього життя. Ми продовжуватимемо рух до цієї честогої мети, об'єднуючи комп'ютерами з підключенням до Інтернету школи, класи й бібліотеки, готуючи викладачів з IT та засобів мультимедіа. Ми й надалі вживатимемо заходів для підтримки малого та середнього бізнесу, індивідуальних підприємців і допомоги їм у під'єднанні до Мережі та ефективному використанні Інтернету. Ми також заохочуватимемо використання IT для надання громадянам протягом усього життя можливостей для творчого навчання, особливо тим, хто інакше не мав би доступу до освіти та професійної підготовки.

Сприяння загальній участі

IT відкривають величезні можливості для становлення й розвитку економик. Країни, які досягли успіху у використанні потенціалу IT, можуть сподіватися подолати перепони, що звичайно виникають у процесі розвитку інфраструктури, та рушити назустріч ефективнішій реалізації своїх цілей, наприклад скорочення бідності, охорона здоров'я, покращення санітарних умов, освіти, а також використання переваг швидкого зростання глобальної електронної торгівлі. Деякі країни, що розвиваються, вже досягли значних успіхів у цих сферах.

Однак не слід недооцінювати проблему подолання інформаційного й технологічного розриву між державами з різним рівнем економічного розвитку. Ми відаємо належає зусиллям, яких вживають у цій сфері багато країн, що розвиваються. Справді, ті країни, що розвиваються, які виявляться неспроможними не відставати від дедалі прискорюваних темпів IT-інновацій, не матимуть можливості бути повноцінними учасниками інформаційного суспільства та глобальної цифрової економіки. Це питання особливо гостро стоїть перед тими країнами, де поширення IT стримується значним відставанням у розвитку основних економічних і соціальних інфраструктур, зокрема енергетичного сектора, телекомунікацій та освіти.

Ми визнаємо, що у вирішенні цієї проблеми слід брати до уваги відмінність умов та потреб у різних країнах. Не існує рішення на зразок «один розмір підходить усім». Це надає надзвичайної ваги ролі країн, що розвиваються, прийняття ними послідовних національних стратегій розвитку IT, і ми звертаємося до них: провадьте сприятливий до IT політичний та регуляторний діяльність, яка б заохочувала конкурентоспроможність ваших економік у цій сфері; використовуйте IT для досягнення розвитку та соціальної єдності; розвивайте людські ресурси, поширюйте навички спілкування з IT; заохочуйте громадські ініціативи та активність вітчизняних підприємців.

Подальший розвиток

Успішність зусиль щодо подолання розриву як між нашими державами, так і в наших суспільствах, залежить від ефективної співпраці всіх учасників. У створенні рамок умов для розвитку IT і надалі відіграватимуть значну роль двостороння та багатостороння співпраця. Міжнародні фінансові структури (IFIs), включаючи багатосторонні банки роз-

виту (MDBs), особливо Всесвітній банк, спроможні зробити серйозний внесок у цю справу, формуюючи й здійснюючи програми, які сприятимуть економічному зростанню, будуть корисні для бізнесу, а також розширять можливість зв'язку, доступу до ІТ та навчання. Міжнародна телекомунікаційна спілка (ITU), Конференція ООН з торгівлі та розвитку (UNCTAD), Програма розвитку ООН (UNDP) та інші відповіли міжнародні форуми також відіграють важливу роль. Приватний сектор залишається центральною діювою особою проєкту ІТ у країнах, що розвиваються, та може робити значний внесок у міжнародні зусилля з подолання цифрового розриву між країнами. Неурядові організації, з їхньою унікальною здатністю ефективно діяти на місцевому ринку, можуть робити корисний внесок у розвиток ресурсів людини та спільноти. ІТ глобальні за своєю сутністю, тож потребують глобального підходу.

Ми вітаємо вже реалізовані зусилля з подолання міжнародного цифрового розриву шляхом двосторонньої допомоги розвитку і міжнародних організацій, і приватних груп. Ми також вітаємо вклад приватного сектора в особі таких організацій, як Глобальна ініціатива з подолання цифрового розриву Всесвітнього економічного форуму (WEF), Глобальний діалог бізнесу з питань е-торгівлі (GBDe) та Глобальний форум.

Як зазначено в Міністерській декларації Економічної та соціальної ради ООН (ECOSOC) «Про роль ІТ в контексті глобальної економіки, що ґрунтується на знанні», існує потреба в розширенні міжнародного діалогу та співпраці для збільшення ефективності програм і проєктів у сфері ІТ для країн, що розвиваються, об'єднання «найкращих методів» та мобілізації ресурсів всіх учасників для подолання цифрового розриву. Велика вісімка й надалі сприятиме зміцненню партнерства між розвиненими країнами та країнами, що розвиваються, між громадським суспільством, включаючи приватні фірми, неурядові організації, фонди та навчальні заклади, і міжнародними організаціями. Ми також працюватимемо над тим, аби країни, що розвиваються, у партнерстві з іншими учасниками могли отримувати фінансове, технічне та політичне забезпечення з метою створення кращих умов для використання ІТ.

Ми погоджуємося заснувати Групу з цифрових можливостей з метою об'єднання наших зусиль у більш широкому міжнародному підході. Ця Група буде скликана у найкоротші строки для дослідження найкращих можливостей гарантування піклуючості до роботи всіх учасників. Ця Група високого рівня в режимі тісного консультування з іншими партнерами і, орієнтуючись на потреби країн, що розвиваються, буде:

активно сприяти діалогу між країнами, що розвиваються, міжнародними організаціями та іншими учасниками для покращення міжнародної співпраці з метою формування політичного, нормативного та мережевого забезпечення, підвищення якості зв'язку, розширення доступу та зменшення його вартості, зміцнення людського потенціалу і заохочення глобальної е-торгівлі в Мережі;

заохочувати власні зусилля Великої вісімки в напрямку співпраці щодо експериментальних програм та проєктів у сфері ІТ;

сприяти більш тісному політичному діалогу між партнерами та працювати над тим, аби збільшити розуміння світової громадою проблем та можливостей;

вивчати вклад приватного сектора та інших зацікавлених груп, таких як Глобальна ініціатива з подолання цифрового розриву;

готувати доповідь за результатами роботи для вручення нашим особистим представникам до наступної зустрічі в Генуї.

На виконання цих завдань Група шукатиме шляхи до вжиття конкретних заходів у пріоритетних сферах, що вказані нижче:

створення політичного, нормативного та мережевого забезпечення:

підтримка політичного консультування та зміцнення місцевого потенціалу, аби сприяти провадженню спрямованої на створення конкуренції, гнучкої та соціально орієнтованої політики та нормативного забезпечення;

сприяння обміну досвідом між розвиненими країнами та іншими партнерами;

сприяння ефективнішому та ширшому використанню ІТ у сфері розвитку, включаючи такі широкі напрямки, як скорочення бідності, освіта, охорона здоров'я і культура;

вдосконалення системи управління, включаючи дослідження нових методів комплексної розробки політики;

підтримка зусиль МБР (MDBs) та інших міжнародних організацій з метою об'єднання інтелектуальних та фінансових ресурсів у контексті програм співробітництва, таких як «InfoDev»;

покращення зв'язку, розширення доступу та зменшення його вартості:

мобілізація ресурсів з метою покращення інформаційної та телекомунікаційної інфраструктури, окремо акцентуючи увагу на утвердженні підходу «партнерства» з боку урядів, міжнародних організацій, приватного сектора та неурядових організацій;

пошук шляхів до зменшення вартості зв'язку для країн, що розвиваються;

підтримка програм доступу на місцевому рівні;

заохочення технологічних досліджень і прикладних розробок, що відповідатимуть потребам країн, що розвиваються;

покращення здатності до взаємодії мереж, послуг та прикладних систем;

заохочення виробництва на місцевому рівні інформаційного контенту, включаючи розвиток контенту рідними мовами учасників;

зміцнення людського потенціалу:

концентрування уваги на базовій освіті, так само як і на збільшенні можливостей для навчання протягом усього життя, з особливим акцентом на розвиткові навичок користування ІТ;

сприяння розвиткові об'єднань освічених фахівців з ІТ та інших пов'язаних галузей в політиці та нормативній сфері;

розвиток творчих підходів з метою розширення традиційної технічної допомоги, включаючи дистанційне навчання та підготовку на місцях; створення мережі громадських закладів та інститутів, включаючи школи, дослідницькі центри та університети;

заохочення глобальної е-торгівлі в Мережі:

оцінка і розширення можливостей використання е-торгівлі шляхом консультування щодо відкриття бізнесу у країнах, що розвиваються, а також шляхом мобілізації ресурсів для допомоги підприємцям у використанні IT для збільшення їхньої ефективності та розширення доступу на нові ринки;

забезпечення відповідності «правил гри», що виникатимуть, зусиллям у сфері розвитку, а також зміцнення здатності країн, що розвиваються, відігравати конструктивну роль у визначенні цих прав.

**ДИРЕКТИВА 95/46/ЄС
ПРО ЗАХИСТ ФІЗИЧНИХ ОСІБ ПРИ ОБРОБЦІ ПЕРСОНАЛЬНИХ
ДАНИХ ТА ПРО ВІЛЬНЕ ПЕРЕМІЩЕННЯ ТАКИХ ДАНИХ**
*(Прийнято Європейським парламентом та Радою ЄС
24 жовтня 1995 року)*

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ і РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

беручи до уваги Договір про заснування Європейського Співтовариства (994_017) і, зокрема, його статтю 100а;

беручи до уваги пропозицію Комісії¹;

беручи до уваги висновок Економічного і Соціального Комітету²; діючи відповідно до процедури, викладеної в статті 189б Договору (994_017)³,

1. Враховуючи, що цілі Співтовариства, викладені в Договорі (994_017), з поправками, внесеними Договором про Європейський Союз (994_029), 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 основних правах, визнаних конституціями і законами держав-членів та Європейською конвенцією про захист прав людини і основних свобод (995_004);

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 7а Договору (994_017) гарантується вільне пересування товарів, осіб, послуг і капіталів, вимагає не тільки можливості вільного переміщення персональних даних з однієї держави-члена в іншу, а й захисту основних 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;

¹ ОІ N С 277, 5. 1990, р. 3 і ОІ N 311, 27.11.1992, р. 30.
² ОІ N 159, 17.06.1991, р. 38.

³ Висновок Європейського Парламенту від 11 березня 1992 р. (ОІ N С 94, 13.04.1992, р. 198), ратифікований 2 грудня 1993 р. (ОІ N С 342, 20.12.1993, р. 30); Загальна позиція Ради від 20 лютого 1995 р. (ОІ N С 93, 13. 4. 1995 р., р. 1) і Рішення Європейського Парламенту від 15 червня 1995 р. (ОІ N С 166, 3.7.1995).

5. Враховуючи, що економічна і соціальна інтеграція, досягнута в результаті створення і функціонування внутрішнього ринку в розумінні статті 7а Договору (994_017), 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 й обмінюватися персональними даними для того, щоб мотти 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 й 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, зокрема 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 поодиночі, особливо з урахуванням ступеня існуючих у даний час розбіжностей 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 7а Договору (994_017); враховуючи, що у зв'язку з цим необхідні дії Співтовариства, спрямовані на зближення такого законодавства;

9. Враховуючи, що при рівному рівні захисту внаслідок зближення національних законодавств держави-члени більше не зможуть перешкоджати вільному пересуванню персональних даних між собою, посиляючись 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 у контексті виконання Директиви може також використовуватися діловими і соціальними партнерами; враховуючи, що дер-

жави-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 системному 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 основних прав і свобод, а особливо права на невтручання в особисте життя, що визнається як статтею 8 Європейської конвенції про захист прав людини й основних свобод (995_004), 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 даній Директиві, уточнюються і посилюються принципами, викладені в Конвенції Ради Європи від 28 січня 1981 року про захист фізичних осіб при автоматизованій обробці персональних даних (994_326);

12. Враховуючи, що принципи захисту повинні застосовуватися до всіх 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 винятково 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 (994_029), 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 (994_017);

враховуючи, що обробка персональних даних, необхідна для захисту економічного добробуту держави, не входить до сфери дії даної 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, рестрації, збереження чи повідомлення звукових і візуальних даних, які стосуються фізичних осіб, який відбувається в інформаційному суспільстві, дана Директива повинна застосовуватися до обробки, що використовує такі дані;

15. Враховуючи, що обробка таких даних підпадає під дію даної 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 даної 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 проводиться з метою журналістики чи з метою літературної або художньої творчості, зокрема, в аудіовізуальному секторі, принципи Директиви повинні застосовуватися з обмеженнями відповідно до положень, викладених у статті 9;

18. Враховуючи, що для того, аби уникнути втрати фізичною особою захисту, на який вона має право згідно з даною Директивою, будь-яка обробка персональних даних у Співтоваристві повинна відбуватися відповідно до законодавства однієї з держав-членів;

враховуючи, що у 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, що той факт, що обробка даних проводиться особою, яка перебуває в третій країні, не повинен перешкоджати захисту фізичних осіб, передбаченому даною 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 даною Директивою;

21. Враховуючи, що дана 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 даної Директиви, загальні умови, при яких обробка даних є законною; враховуючи, що, зокрема, стаття 5 разом 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, які їх стосуються, не зачіпається даною 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 наглядних органів, і обставин, при яких може проводитися обробка, та, з іншого боку, у праві, яким наділені фізичні особи, чий дані підлягають обробці, знати, що обробка справді проводиться, звертатися до даних, вимагати внесення змін і навіть заперечувати проти обробки за певних обставин;

26. Враховуючи, що принципи захисту повинні застосовуватися до будь-якої інформації, яка 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 імовірно очікувати для встановлення вищезгаданої особи; враховуючи, що принципи захисту не застосовуються до даних, які 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 анонімно надання даних і збереження їх 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 такого захисту не повинні залежати від використовуваних методів, бо інакше це створить серйозну загрозу обходу закону; враховуючи, що, незважаючи на це, у тому що стосується ручної обробки, дана Директива охоплює тільки картотеки даних, але не неструктуровані справи; враховуючи, що, зокрема, вміст картотеки даних 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 (с), 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 типові архуші, що не розроблені відповідно до визначених критеріїв, за жодних обставин не входять до сфери дії даної Директиви;

28. Враховуючи, що будь-яка обробка персональних даних повинна бути законною і справедливою щодо 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 стосовно 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 як правова вимога, 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 враховується інтереси чи права і свободи суб'єкта даних; враховуючи, що, зокрема, для того щоб зберегти рівновагу між інтересами, які зачіпаються, водночас гарантуючи ефективну конкуренцію, держави-члени можуть визначити обставини, за яких персональні дані можуть використовуватися чи надаватися третій стороні в контексті законної звичайної ділової діяльності компаній та 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'єктові даних безкоштовно і без зазначення причин заперечувати проти обробки даних, які його стосуються;

31. Враховуючи, що обробка персональних даних повинна розглядатися також як законна, якщо вона проводиться 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 законами-давствами;

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 зі здоров'ям, особами, які зв'язані правовим зобов'язанням зберігати професійну таємницю;

що, або під час законної діяльності певних асоціацій чи фондів, метою яких є дозволити здійснення основних 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 основних 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 гарантії;

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 даної Директиви, у тій мірі, у якій це необхідно для узгодження основних прав людини зі свободою інформації і особливо з правом одержувати і передавати інформацію, яке гарантується, передусім, статтею 10 Європейської конвенції про захист прав людини й основних свобод (95_004); враховуючи, що, виходячи з цього, держави-члени повинні визначити винятки і відступи, необхідні для досягнення балансу між основними 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 щодо заходів із забезпечення безпеки обробки; враховуючи, що принаймні наглядовий орган, відповідальний за цю галузь, повинен також бути наділений певними апостеріорними повноваженнями, наприклад видавати ретельний звіт чи передавати справи судовим органам;

38. Враховуючи, що для того, аби обробка даних була справедливою, суб'єкт даних повинен мати 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 шля-

хом третій стороні, навіть якщо це не було передбачено під час збору даних у суб'єкта даних; враховуючи, що у всіх цих випадках суб'єкт даних повинен бути поінформований про це тоді, коли дані записуються, чи пізніше, коли вони вперше розкриваються третій стороні;

40. Враховуючи, однак, що дане зобов'язання не обов'язково накладалося на суб'єкт даних уже 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'єктові даних виявиться неможливим чи зажадає непропорційних зусиль, що може відбутися у випадку, коли обробка даних проводиться 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 її і перебувають в обробці, з метою їхньої перевірки, особливо перевірки точності її 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 йдеться в пункті 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'єктові 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 та інформування й обмеження деяких інших зобов'язань контролера можуть подібним чином бути встановлені державами-членами тією мірою, якою вони необхідні для захисту, наприклад, національної безпеки, оборони, суспільної безпеки чи важливих економічних і фінансових інтересів держави-члена чи Союзу, а також у карних розслідуваннях, переслідуваннях і діях у зв'язку з порушенням етики встановлених професій; враховуючи, що перелік винятків і обмежень повинен включати завдання моніторингу, інспекції чи регулювання, що необхідні в трьох останніх зі згаданих сфер стосовно суспільної безпеки, економічних чи фінансових інтересів і попередження злочинності; враховуючи, що перелічування завдань 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 даної Директиви в тому, що стосується права доступу, зобов'язання інформувати фізичних осіб, якості даних; з метою виконання деяких із 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 існуючий стан справ і вартість їхньої реалізації з урахуванням пов'язаного з обробкою ризику і характеру даних, що підлягають захисту;

47. Враховуючи, що, коли повідомлення, яке містить персональні дані, передається за допомогою телекомунікацій чи електронної пошти, єдиною метою яких є передача таких повідомлень, контролером щодо персональних даних, які містяться в повідомленні, буде вважатися особа, від якої виходить це повідомлення, а не особа, яка надає послуги з передачі повідомлень; враховуючи, що, незважаючи на це, особи, які надають ці послуги, будуть, як правило, вважатися контролерами стосовно обробки додаткових персональних даних, необхідних для надання цієї послуги;

48. Враховуючи, що процедури повідомлення наглядового органу покликані забезпечити розкриття цілей і основних принципів будь-якого процесу обробки для перевірки того, що процес здійснюється відповідно до національних заходів, прийнятих відповідно до даної Директиви;

49. Враховуючи, що для того, щоб уникнути непотрібних адміністративних формальностей, звільнення від зобов'язання повідомити і сповіщення 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 прийнятого державою-членом заходу, що визначає її рамки; враховуючи, що звільнення чи сповіщення 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 функції абсолютно незалежно;

50. Враховуючи, що звільнення чи сповіщення може бути передбачене у випадках із процесами обробки, єдиною метою яких є ведення реєстру, який, відповідно до національного законодавства, призначений для надання інформації населенню і є відкритим для звернень 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 даної 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 імовірність певних ризиків для прав і свобод суб'єктів даних через їхню природу, їхній обсяг чи їхні цілі, 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, які 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 відповідно до свого національного законодавства дає свій висновок чи дозвол на здійснення обробки; враховуючи, що така перевірка може однаковою мірою 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 в разі 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 даної Директиви;

56. Враховуючи, що транскордонні потоки персональних даних необхідні для розширення міжнародної торгівлі; враховуючи, що захист фізичних осіб, гарантований у Співтоваристві даною Директивою, не перешкоджає передачі персональних даних третім країнам, що забезпечують адекватний рівень захисту; враховуючи, що адекватність рівня захисту, наданого третіми країнами, повинна оцінюватись 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, які 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 звернення осіб, які мають законний інтерес, передача даних повинна здійснюватись 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 щодо порядку переговорів між Співтовариством і такими третіми країнами;

60. Враховуючи, що, в будь-якому випадку, передача даних третій країні може здійснюватись тільки в повній відповідності до положень, прийнятих державами-членами відповідно до даної Директиви, зокрема її статті 8;

61. Враховуючи, що держави-члени і Комісія в межах своїх повноважень повинні заохочувати професійкові об'єднання та інші зацікавлені представницькі організації до складання кодексів поведінки для того, щоб сприяти в застосуванні даної Директиви, беручи до уваги особливі характеристики обробки даних, що проводиться у визначених галузях, і дотримуючись національних положень, прийнятих з метою виконання даної Директиви;

62. Враховуючи, що створення в державах-членах наглядових органів, які 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 з 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 один одному 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, з огляду на її особливий характер вона повинна консультувати Комісію і, зокрема, сприяти однаковому застосуванню національних правил, прийнятих відповідно до даної 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/ЄС⁴;

67. Враховуючи, що 20 грудня 1994 року було досягнуто тимчасової згоди між Європейським Парламентом, Радою та Комісією про заходи з виконання актів, прийнятих відповідно до процедури, викладеної в статті 189б Договору ЄС (994_029);

68. Враховуючи, що викладені в даній 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 законами, що впроваджують дану Директиву, для послідовного застосування таких нових національних правил до всіх процесів обробки, що вже ведуться; враховуючи, що для полегшення їх рентабельної реалізації державам-членам надаватиметься подальший період, що закінчується через 12 років з дати прийняття даної Директиви, для забезпечення відповідності існуючих неавтоматизованих картотек до деяких положень Директиви;

враховуючи, що, коли дані, які містяться в таких картотеках, обробляються вручну в період цього подовженого перехідного періоду, ці картотеки повинні привводитись у відповідність до цих положень під час такої обробки;

70. Враховуючи, що суб'єктові даних не потрібно повторно давати свою згоду для того, щоб дозволити контролерові після набуття чинності національними положеннями, прийнятими відповідно до даної 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 дана Директива не перешкоджає державам-членам у регулюванні маркетингової діяльності, орієнтованої на споживачів, що проживають на їхній території, тією мірою, якою таке регулювання не стосується захисту фізичних осіб при обробці персональних даних;

72. Враховуючи, що дана Директива дозволяє враховувати принципи громадського доступу до офіційних документів при здійсненні принципів, викладених у цій Директиві, **ПРИЙНЯЛИ ЦЮ ДИРЕКТИВУ:**

Глава 1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Ціль Директиви

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.

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 даної Директиви:

- (а) «**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 встановленого прямо чи непрямо, зокрема за допомогою ідентифікаційного коду або одного чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості;
- (б) «**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;
- (с) «**картотека персональних даних**» («**картотека**») означає будь-який структурований масив персональних даних, що є доступним за визначеними критеріями, незалежно від того, чи є такий масив централізованим, децентралізованим або розділеним на функціональних чи географічних засадах;
- (д) «**контролер**» означає фізичну чи юридичну особу, державний орган, агентство або будь-який інший орган, що, окремо чи разом з іншими, визначає цілі й засоби обробки персональних даних; якщо цілі й засоби обробки визначені законодавчими або нормативними положеннями держави чи Співтовариства, контролер або особливий критерій його призначення можуть визначатися правом держави чи Співтовариства;
- (е) «**оператор обробки даних**» означає фізичну чи юридичну особу, державний орган, агентство чи будь-який інший орган, що обробляє персональні дані від імені контролера;
- (ф) «**третья сторона**» означає будь-яку фізичну чи юридичну особу, державний орган, агентство чи будь-який інший орган, крім суб'єкта даних, контролера, оператора обробки даних і осіб, які,

⁴ ОJ N L 197, 18.07.1987, р. 33.

будучи безпосередньо підпорядкованими контролерові чи операторові обробки даних, уповноважені обробляти дані;

(г) «**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;

(н) «**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. Дана Директива застосовується до обробки персональних даних за допомогою повного або часткового використання автоматизованих засобів, а також до обробки неавтоматичними засобами персональних даних, що є частиною картотеки чи призначені для внесення в картотеку.

2. Дана 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 (994_029) 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 у 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 відповідно до даної Директиви, до обробки персональних даних, якщо:

- (а) 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 ужити всіх необхідних заходів для забезпечення того, що кожна з цих установ дотримується зобов'язань, передбачених відповідним національним законодавством;
- (б) контролер заснований не на території держави-члена, а в місці, де його національне законодавство застосовується відповідно до міжнародного публічного права;
- (с) 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 виключно з метою транзиту через територію Співтовариства.

2. За обставин, передбачених у підпункті (с) пункту 1, контролер повинен призначити представника на території цієї держави-члена, без шкоди для судових позовів, що можуть бути подані проти самого контролера.

Глава II ЗАГАЛЬНІ ПРАВИЛА ЗАКОННОСТІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Стаття 5

Держави-члени в рамках положень цієї глави більш точно визначають умови, за яких обробка персональних даних є законною.

Розділ I ПРИНЦИПИ, ЯКІ СТОСУЮТЬСЯ ЯКОСТІ ДАНИХ

Стаття 6

1. Держави-члени передбачають, що персональні дані повинні:

- (а) оброблятися чесно і законно;
- (б) 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;
- (с) бути достовірними, відповідними і не надлишковими стосовно цілей, заради яких вони збираються і/або надалі обробляються;
- (д) бути точними і, якщо необхідно, оновлюватися; 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;
- (е) 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.

Розділ II

КРИТЕРІЙ ЗАКОННОСТІ ОБРОБКИ ДАНИХ

Стаття 7

1. Держави-члени передбачають, що персональні дані можуть оброблятися тільки за умови, що:

- (а) суб'єкт даних недовозначно дав свою згоду; чи
- (б) обробка необхідна для виконання контракту, стороною якого є суб'єкт даних, чи для вживання заходів на прохання суб'єкта даних до підписання контракту; чи
- (с) обробка необхідна для дотримання правового зобов'язання, яким зв'язаний контролер; чи
- (д) обробка необхідна для захисту життєво важливих інтересів суб'єкта даних; чи
- (е) обробка необхідна для виконання завдання, здійснюваного в суспільних інтересах, чи при виконанні офіційних повноважень, якими наділений контролер або третя сторона, якій надаються дані; чи
- (ф) обробка необхідна в цілях законних інтересів, переслідуваних контролером чи третьою стороною або сторонами, для яких надаються дані, крім випадків, коли над такими інтересами переважать інтереси основних прав і свобод суб'єкта даних, що вимагають захисту згідно з пунктом 1 статті 1.

Розділ III
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:

- (а) суб'єкт даних дав свою недовозначну 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
- (б) обробка необхідна з метою виконання зобов'язань і особливих прав контролера в галузі законодавства про протиправне втручання, певною мірою, якою це дозволено національним законодавством, що передбачає адекватні гарантії; чи
- (с) обробка необхідна для захисту життєво важливих інтересів суб'єкта даних чи іншої особи, якщо суб'єкт даних не може дати свою згоду через свою недієздатність або неправадіздатність;

чи

- (д) 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 виключно 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'єкта даних; чи

- (е) обробка стосується даних, що явно оприлюднені суб'єктами даних, або необхідна для порушення, виконання чи захисту судових позовів.

3. Пункт 1 не застосовується, якщо обробка даних необхідна з метою профілактичної медицини, медичної діагностики, надання медичних послуг чи лікування або для управління службами охорони здоров'я, і якщо ці дані обробляються медичним 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 збереження таємниці.

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 або 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, які 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 загальноного застосування.

Стаття 9. Обробка персональних даних і свобода самовираження

Держави-члени передбачають винятки чи відступи від положень цієї Глави, Глави IV і Глави VI, у тому, що стосується обробки персональних даних, що проводиться виключно для цілей журналістики або художньої чи літературної творчості, за умови, що вони необхідні, для узгодження прав на невтручання в особисте життя з нормами, що регулюють свободу самовираження.

Розділ IV

ІНФОРМАЦІЯ, ЩО НАДАЄТЬСЯ СУБ'ЄКТОВІ ДАНИХ

Стаття 10. Інформація у разі збору даних від суб'єкта даних

Державні члени передбачають, що контролер чи його представник повинні надати суб'єктові даних, у якого збираються дані щодо нього самого, найнаймні таку інформацію, крім тих випадків, коли в нього вже є ця інформація:

- (а) особа контролера і його представника, якщо такий є;
- (б) ціні обробки, для якої призначені дані;
- (в) будь-яка додаткова інформація, як наприклад:
 - одержувачі чи категорії одержувачів даних;
 - обов'язковість чи добровільність відповіді на запитання, а також можливі наслідки за ненадання відповіді;
 - існування права доступу і права на виправлення даних, які його стосуються, тією мірою, якою така додаткова інформація необхідна, з огляду на особливі обставини, за яких дані збираються, для гарантії справедливої обробки стосовно 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, державні члени передавають, що контролер чи його представник повинні під час рестрації персональних даних чи, якщо передачене розголошення даних третій особі, не пізніше того часу, коли дані вперше розголошуються, надати суб'єктові дані таку 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;
 - існуючі права доступу і права на випадження даних, які його стосуються, тією мірою, якою така додаткова інформація необхідна, з огляду на особливі обставини, за яких дані обробляються, для гарантії справедливої обробки стосовно суб'єкта даних обробки.

3. 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.

Розділ V

ПРАВО СУБ'ЄКТА ДАНИХ НА ДОСТУП ДО ДАНИХ

Стаття 12. Право доступу

Держави-члени гарантують кожному суб'єктові даних право отримувати від контролера:

- (а) без обмежень через розумні інтервали часу і без надмірної загрози ризиків або витрат: — підтвердження того, обробляються чи ні дані, які його стосуються, і інформацію про наявність про цілі обробки, категорії розглянутих даних і про одержувачів чи категорії одержувачів, яким надаються дані; — повідомлення йому в зрозумілій формі про те, що дані перебувають у процесі обробки, і будь-яку іншу доступну інформацію щодо їхнього джерела, — інформацію про логіку, використовувану під час автоматизованої обробки даних, що його стосуються, принаймні у випадку автоматизованих рішень, згаданих у статті 15 (1);
- (б) залежно від випадку, виправлення, стирання чи блокування даних, обробка яких не відповідає положенням даної Директиви, зокрема через неповноту чи неточність даних;
- (с) повідомлення третім сторонам, яким були надані дані, про будь-яке виправлення, стирання чи блокування, виконане відповідно до підпункту (б), якщо це можливо чи не вимагає непропорційних зусиль.

Розділ 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);

(e) захист суб'єкта даних чи прав і свобод інших осіб.

2. За умови виконання відповідних правових гарантій, зокрема того, що дані не використовуються для вжиття 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.

Розділ VII ПРАВО СУБ'ЄКТА ДАНИХ НА ЗАПЕРЕЧЕННЯ

Стаття 14. Право суб'єкта даних на заперечення

Держави-члени надають суб'єктові 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 її і 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 даної Директиви, держави-члени передбачають, що стосовно особи може бути прийняте рішення, про яке йдеться в пункті 1, якщо це рішення:

- (a) прийняте в ході укладення чи виконання контракту, за умови, що прохання про укладення 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.

Розділ VIII КОНФІДЕНЦІЙНІСТЬ І БЕЗПЕКА ОБРОБКИ

Стаття 16. Конфіденційність обробки

Будь-яка особа, яка діє у підпорядкуванні контролерові чи операторові 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 врахуванням нинішнього стану речей і вартості їх 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 контролерові і який передбачає, зокрема, таке: — оператор обробки даних повинен діяти тільки за вказівками контолера;

— 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 акта про захист даних і вимоги про заходи, згадані у пункті 1, повинні бути викладені в письмовій формі чи в іншій рівносильній формі.

Розділ 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 таких випадках і за таких умов:

— якщо для категорії операцій з обробки, які, враховуючи дані, що будуть оброблятися, наведуть 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 таке:

— 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, у такий спосіб забезпечуючи те, що операції з обробки наведуть чи завдадуть шкоди правам і свободам суб'єктів даних.

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 передбачити повідомлення про деякі чи всі неавтоматизовані операції з персональними даними або передбачити спрощений порядок повідомлення про ці операції з обробки.

Стаття 19. Зміст повідомлення

1. Держави-члени визначають інформацію, що повинна міститися в повідомленні. Вона має включати принаймні таке:

- (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 з обробки, що можуть мати певний ризик для прав і свобод суб'єктів даних, і перевіряють, щоб ці операції з обробки вивчалися до початку обробки.

2. Такі попередні перевірки здійснюються наглядовим органом після одержання повідомлення від контролера чи посадової особи з питань захисту даних, що при виникненні сумнівів повинні ріднитися 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 того, що операції з обробки оголошуються.

2. Держави-члени передбачають, що наглядовий орган повинен вести реєстр операцій із обробки, повідомлення про які відбувається згідно зі статтею 18.

Реєстр повинен містити принаймні інформацію, перелічену в підпунктах (a) — (e) пункту 1 статті 19. Будь-яка особа може перевірити такий реєстр.

3. Держави-члени передбачають щодо операцій із обробки, повідомлення про які не передбачаються, що контролери чи інші органи, призначені державами-членами, надають після запиту будь-якої особи у відповідній формі принаймні інформацію, перелічену 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, який 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.

Глава 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, згіданому в статті 28, до звертання в судовий орган, держави-члени передачають 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 передачають, що будь-яка особа, якій завдано шкоди в результаті незаконної операції з обробки чи будь-якої дії, несутімної з 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 даної Директиви і, зокрема, встановлюють санкції, що повинні накладатися у випадку порушення положень, прийнятих відповідно до даної Директиви.

Глава IV ПЕРЕДАЧА ПЕРСОНАЛЬНИХ ДАНИХ ТРЕТІМ КРАЇНАМ

Стаття 25. Принципи

1. Держави-члени передачають, 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 даної 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 і 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. Комісія може дійти висновку, згідно з процедурою, згіданною в пункті 2 статті 31, що третя країна забезпечує адекватний рівень захисту, передбаченого пунктом 2 даної 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 основних свобод і прав фізичних осіб. Держави-члени вживають заходів, необхідних для виконання рішень Комісії.

Стаття 26. Виступи

1. Шляхом виступу від статті 25 і крім випадків, коли інше передбачено національним законодавством, що регулює особливі випадки, держави-члени передачають, що передача чи сукупність передач персональних даних третій країні, яка не забезпечує адекватний рівень захисту, згіданий у пункті 2 статті 25, може відбуватися за умови, що:

- (а) суб'єкт даних дав свою недвозначну згоду на пропоновану передачу даних; або
- (б) передача даних необхідна для виконання контракту між суб'єктом даних і контролером чи для виконання заходів, що передують договору і прийнятті у відповідь на прохання суб'єкта даних; або
- (в) передача даних необхідна для укладення чи виконання контракту, укладеного в інтересах суб'єкта даних між контролером і третьою стороною; або
- (д) передача даних необхідна чи юридично обов'язкова на важливих підставах суспільних інтересів або для встановлення, виконання чи захисту правових вимог; або
- (е) передача даних необхідна для захисту життєво важливих інтересів суб'єкта даних; або
- (ф) 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 основних прав і свобод фізичних осіб і в тому, що стосується здійснення відповідних прав; такі гарантії можуть, зокрема, стати результатом відповідей умов договору.

3. Держава-член повідомляє Комісію й 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 й основних прав і свобод фізичних осіб, 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.

Глава 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 даної Директиви, з урахуванням характерних особливостей різних галузей.

2. Держави-члени передбачають, щоб професійки 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 даної 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 у статті 29. Ця Робоча група визначає, серед іншого, чи відповідають надані проекти національним положенням, прийнятим відповідно до даної 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.

Глава 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, прийнятих державами-членами відповідно до даної Директиви.

Ці органи повністю незалежні при здійсненні функцій, якими вони наділені.

2. 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 зі 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 контролерові, або повноваження звертатися до національних парламентів чи інших політичних інститутів;

— право брати участь у судочинстві, якщо були порушені національні положення, прийняті відповідно до даної Директиви, чи довести ці порушення до відомої 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 перевірку законності обробки даних, зроблені будь-якою особою, у випадках, коли застосовуються національні положення, прийняті відповідно до статті 13 даної 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 оприлюднюватися.

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 тією мірою, шляхом обміну всією корисною інформацією.

7. Держави-члени передають, 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. Робоча група складається з представника наглядового органу чи органів, призначеного кожного державою-членом, і представника від органу чи органів, створених для установ і органів Співтовариства, а також представника Комісії.

2. 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 становить 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

Робоча група:

(а) розглядає будь-яке питання, що стосується життя національних заходів, прийнятих відповідно до даної Директиви, з метою сприяння загальному вжиттю таких заходів;

(б) представляє Комісії висновки щодо рівня захисту в Співтоваристві та в третіх країнах;

(с) повідомляє Комісію про будь-яку запропоновану поправку до даної 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;

(д) вносить висновки про кодекси, складені на рівні Співтовариства.

2. Якщо Робоча група виявляє, що між законами чи практикою держав-членів виникають розбіжності, що 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 щодо 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.

Глава VII

ІМПЛЕМЕНТАЦІЙНІ ЗАХОДИ СПІВТОВАРИСТВА

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 (994_029). Голоси представників держав-членів у комітеті піраховуються відповідно до процедури, встановленої даною статтею. Голова не голосує.

Комісія визначає заходи, що повинні вживатися негайно. Однак, якщо ці заходи не збігаються з висновком Комітету, Комісія негайно повідомляє про це Раду.

У такому випадку:

— Комісія відкладає вжиття визначених 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 даної 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 даної Директиви, уже 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 даної Директиви протягом 12 років з дня її прийняття. Однак держави-члени надають суб'єктові 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, переслідуючи контрольером.

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 даної Директиви.

4. Держави-члени повинні представити Комісії текст положень внутрішнього законодавства, які вони приймають у сфері, що підпадає під дію даної Директиви.

Стаття 33

Комісія регулярно доповідає Раді і Європейському Парламенту, починаючи не пізніше ніж через три роки від дати, зазначеної в пункті 1 статті 32, про виконання даної Директиви, при необхідності додаючи до своєї доповіді відповідні пропозиції про поправки. Доповідь підлягає оприлюдненню.

Комісія вивчає, серед іншого, застосування даної Директиви до обробки звукових і візуальних даних, що стосуються фізичних осіб, і подає будь-які відповідні пропозиції, що є необхідними з погляду досяг-

нень в інформаційних технологіях і у світі рівня прогресу в інформаційному суспільстві.

Стаття 34

Дана Директива адресована державам-членам.

Вчинено в Люксембурзі 24 жовтня 1995 року.
За Європейський Парламент Президент К. Хенш
За Раду Президент Л. Аьенца Сера

Офіційний журнал L 281, 23/11/1995, р. 0031—0050

Переклад здійснено Центром перекладів актів європейського права при Міністерстві юстиції України.

ДИРЕКТИВА 96/9/ЄС ПРО ПРАВОВИЙ ЗАХИСТ БАЗ ДАНИХ

(Прийнято Європейським парламентом та Радою ЄС 11 березня 1996 р.)

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ І РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

Беручи до уваги Договір про створення Європейського Співтовариства і, зокрема, статтю 57(2), 66 і 100 а Договору,

Беручи до уваги пропозицію Комісії¹,

Беручи до уваги висновок Економічного і Соціального Комітету², Діючи відповідно до процедури, викладеної в статті 189б Договору³,

(1) Враховуючи, що наразі бази даних не є достатньо захищеними в усіх державах-членах чинним законодавством; враховуючи, що такий захист, де він існує, має різні характеристики;

(2) Враховуючи, що такі відмінності в правовому захисті баз даних, який надається законодавством держав-членів безпосередньо негативно впливають на функціонування внутрішнього ринку в тому, що стосується баз даних, і, зокрема, на свободу фізичних та юридичних осіб надавати товари та послуги інтерактивних баз даних відповідно до гармонізованих правових домовленостей у межах Співтовариства; враховуючи, що такі відмінності цілком можуть стати ще більш вираженими після запровадження державами-членами нового законодавства в цій сфері, що зараз дедалі більше набирає міжнародного виміру;

(3) Враховуючи, що існуючі відмінності, які порушують функціонування внутрішнього ринку, повинні бути усунуті, а появи нових слід запобігти, у той час як відмінності, які не впливають негативно на функціонування внутрішнього ринку, не повинні усуватися, і їхній появи не потрібно перешкоджати;

(4) Враховуючи, що захист авторських прав на бази даних існує в різних формах у державах-членах відповідно до законодавства чи прецедентом практики, а також враховуючи, що коли між державами-членами залишаються відмінності в законодавстві щодо масштабів та умов захисту, такі неузгоджені права на інтелектуальну власність можуть призвести до перешкоджання вільному руху товарів чи послуг у межах Співтовариства;

(5) Враховуючи, що авторське право залишається належною формою виключного права авторів, які створили бази даних;

(6) Враховуючи, що, однак, за відсутності гармонізованої системи законодавства про нечесну конкуренцію чи прецедентного права з цього

Директива 96/9/ЄС Європейського парламенту та Ради ЄС «Про правовий...

питання необхідні інші додаткові заходи для запобігання несанкціонованому витягненню та/чи повторному використанню вмісту бази даних;

(7) Враховуючи, що створення баз даних вимагає вкладання значних людських, технічних та фінансових ресурсів, тоді як такі бази даних можуть бути скопійовані або ж до них може бути отримано доступ за частку тієї вартості, яка потрібна для їхньої незалежної розробки;

(8) Враховуючи, що несанкціоноване витягнення та/чи повторне використання вмісту бази даних є діями, що можуть призвести до серйозних економічних та технічних наслідків;

(9) Враховуючи, що бази даних є важливим знаряддям розвитку інформаційного ринку в рамках Співтовариства; враховуючи, що це знаряддя також буде корисним у багатьох інших сферах;

(10) Враховуючи, що експонентне зростання, як у Співтоваристві, так і в світі в цілому, обсягів інформації, які створюються та обробляються щорічно в усіх секторах торгівлі та промисловості, вимагає інвестування в передові системи обробки інформації в усіх державах-членах;

(11) Враховуючи, що в даний час існує значний дисбаланс у рівнях інвестування в сектор баз даних як між державами-членами, так і між Співтовариством і третіми країнами, що є найбільшими виробниками баз даних у світі;

(12) Враховуючи, що таке інвестування в сучасні системи зберігання та обробки інформації в Співтоваристві не відбуватиметься, якщо для захисту прав розробників баз даних не буде запроваджено стабільного і єдиного режиму правового захисту;

(13) Враховуючи, що ця Директива захищає збирання, що іноді називаються «копіліціями», робіт, даних чи інших матеріалів, які упорядковуються, зберігаються і до яких отримується доступ за допомогою засобів, що включають електронні, електромagnetні та електрооптичні процеси або аналогові процеси;

(14) Враховуючи, що захист відповідно до цієї Директиви повинен поширюватися на неелектронні бази даних;

(15) Враховуючи, що потрібно встановити критерії, які використовуються для визначення того, чи має захищатися база даних авторським правом, виходячи з того, що підбір чи упорядкування вмісту бази даних є власним інтелектуальним творінням автора; враховуючи, що такий захист повинен охоплювати структуру бази даних;

(16) Враховуючи, що для визначення того, чи підпадає база даних під захист авторського права, не повинен використовуватись жодний інший критерій, окрім оригінальності в сенсі інтелектуального творіння автора і, зокрема, не повинні застосовуватись ніякі естетичні чи якісні критерії;

(17) Враховуючи, що поняття «база даних» слід розуміти як таке, що включає літературні, художні, музичні чи інші збирання творів або збирання інших матеріалів, таких як тексти, звуки, образи, цифри, факти та дані; враховуючи, що воно повинно охоплювати збирання незалежних робіт, даних чи інших матеріалів, які систематично або методично упорядковані і до яких може бути отримано окремий доступ; враховуючи, що це

¹ О Ж № С 156, 23. 6. 1992, стор. 4 та О Ж № С 308, 15. 11. 1993, стор. 1.

² О Ж № С 19, 25. 1. 1993, стор. 3.

³ Позиція Європейського Парламенту від 23 червня 1993 р. (О Ж № С 194, 19. 7. 1993, стор. 144), спільна позиція Ради від 10 липня 1995 р. (О Ж № С 288, 30. 10. 1995, стор. 14), Рішення Європейського парламенту від 14 грудня 1995 (О Ж № С 17, 22. 1. 1996) та Рішення Ради від 26 лютого 1996 р.

означає, що записи або аудіовізуальні, кінематографічні чи музичні твори як такі не входять до сфери дії цієї Директиви;

(18) Враховуючи, що ця Директива не перешкоджає свободі авторів вирішувати, чи дозволяти включати їхні твори в базу даних та в який спосіб це робити і, зокрема, чи є дозвіл, який надається, виключним; враховуючи, що захист баз даних особливим правом не заважає шкоди існуючим правам стосовно вмісту цих баз, і враховуючи, зокрема, що коли автор чи власник суміжного права дозволяє включити деякі з його творів чи тем у базу даних відповідно до невиключного договору, третя сторона може використати ці твори чи теми, за умови отримання необхідної згоди автора чи власника суміжного права без посилення на особливе право розробника бази даних для запобігання цим її діям, за умови, що ці твори чи тема не витягуються із бази даних і повторно не використовуються на її основі;

(19) Враховуючи, що, як правило, збірка кількох записів музичних виконань на компакт-диску не входить до сфери застосування цієї Директиви, тому що як компіляція вона не відповідає умовам захисту авторського права і тому що вона не є достатньо значним вкладенням, щоб підлягати особливому праву;

(20) Враховуючи, що захист відповідно до цієї Директиви може також застосовуватися до матеріалів, які необхідні для функціонування певних баз даних чи консультування з ними, наприклад тезауруса чи систем індексації;

(21) Враховуючи, що передбачений у цій Директиві захист стосується баз даних, у яких твори, дані та інші матеріали систематично або методично впорядковано; враховуючи, що фізичне зберігання цих матеріалів в організованому порядку не є обов'язковим;

(22) Враховуючи, що електронні бази даних в розумінні цієї Директиви можуть також включати пристрої, такі як CD-ROM та CD-i;

(23) Враховуючи, що термін «база даних» не повинен вживатися у спосіб, що поширював би його застосування на комп'ютерні програми, які використовуються при створенні чи функціонуванні бази даних і які захищаються Директивою Ради 91/250/ЄС від 14 травня 1991 року про правовий захист комп'ютерних програм⁴;

(24) Враховуючи, що задоволення в найм та в прокат баз даних у сфері авторського права та суміжних прав регулюється виключно Директивою Ради 92/100/ЄС від 19 листопада 1992 року про право задоволення в найм і право задоволення в прокат, а також певні права, пов'язані з авторським правом у сфері інтелектуальної власності⁵;

(25) Враховуючи, що строки авторського права вже врегульовано Директивою Ради 93/98/ЄС від 29 жовтня 1993 року, якою гармонізуються строки авторського права і певних суміжних прав⁶;

⁴ О Ж № L 122, 17. 5. 1991 р., стор. 42. Директива із змінами, внесеними Директивою 93/98/ЄС С (О Ж № L 290, 24. 11. 1993, стор. 9.)

⁵ О Ж № L 346, 27. 11. 1992, стор. 61.

⁶ О Ж № L 290, 24. 11. 1993, стор. 9. (7) О Ж № L 281, 23. 11. 1995, стор. 31.

(26) Враховуючи, що захищені авторським правом твори і захищені суміжними правами теми, які включено до бази даних, однак, продовжують захищатися відповідними виключними правами і не можуть включатися до бази даних чи витягуватися з неї без дозволу власника прав чи його правонаступників;

(27) Враховуючи, що на авторське право на такі товари чи суміжні права на теми, включені таким чином до бази даних, жодним чином не впливає існування окремого права на підбір чи упорядкування цих творів і тем в базі даних;

(28) Враховуючи, що моральні права фізичної особи, яка створила базу даних, належать авторів і здійснюються відповідно до законодавства держав-членів та положень Бернської конвенції про охорону літературних і художніх творів; враховуючи, що такі моральні права виходять за межі дії цієї Директиви;

(29) Враховуючи, що механізми, що застосовуються до баз даних, створених працівниками, залишено на розсуд держав-членів; враховуючи, що, таким чином, ніщо в цій Директиві не перешкоджає державам-членам передбачити у своєму законодавстві, що у разі створення бази даних працівником при виконанні своїх службових обов'язків чи згідно зі вказівками, які йому дав його працевлавець, лише працевлавець має право на здійснення всіх економічних прав на створену базу даних, якщо іншого не передбачено контрактом;

(30) Враховуючи, що виключні права автора повинні включати право визначати те, у який спосіб і ким має використовуватися його твір, і, зокрема, контролювати розповсюдження його твору серед осіб, що не мають дозволу;

(31) Враховуючи, що захист авторського права на бази даних включає надання доступу до баз даних у інший спосіб, ніж розповсюдження копій;

(32) Враховуючи, що держави-члени зобов'язані забезпечувати, щоб їхні національні положення були, принаймні в матеріальному аспекті, еквівалентними у разі, якщо такі дії підлягають обмеженням, передбаченим цією Директивою;

(33) Враховуючи, що питання вичерпання права на розповсюдження не виникає у разі інтерактивних баз даних, які входять до сфери надання послуг;

враховуючи, що це ж стосується і випадку, коли користувач такої послуги робить матеріальну копію такої бази даних за згодою власника прав; враховуючи, що, на відміну від CD-ROM і CD-i, де інтелектуальна власність є частиною матеріального носія інформації, а саме товару, кожна інтерактивна послуга є насправді дією, яка повинна підлягати отриманню дозволу, якщо це передбачається авторським правом;

(34) Враховуючи, однак, що коли власник прав вирішив надати копію бази даних користувачеві чи то за допомогою інтерактивної послуги, чи то з використанням іншого способу розповсюдження, законний користувач

повинен мати доступ до бази даних і могли використовувати її для цілей і в спосіб, визначений у договорі з власником прав, навіть якщо такий доступ і використання зумовлюються необхідність виконання інших дій, що за інших умов є обмеженими;

(35) Враховуючи, що потрібно скласти список винятків з обмежених дій, враховуючи той факт, що авторське право, яке регулюється цією Директивою, застосовується тільки до підбору та впорядкування вмісту бази даних; враховуючи, що держави-члени повинні могли передавати такі винятки в деяких випадках; враховуючи, що, така можливість, однак, має реалізовуватись відповідно до Бернської конвенції і тією мірою, якою ці винятки пов'язані зі структурою бази даних; враховуючи, що слід розрізнати винятки для особистого користування і винятки для відтворення для особистих цілей, що стосується положень відповідно до національного законодавства деяких держав-членів про збори на пусті носії інформації та записуюче обладнання;

(36) Враховуючи, що термін «наукове дослідження» в розумінні цієї Директиви охоплює як природні, так і гуманітарні науки;

(37) Враховуючи, що стаття 10 (1) Бернської конвенції не зачіпається цією Директивою;

(38) Враховуючи, що делаті частіше використання цифрових записуючих технологій наражає розробника баз даних на ризик копіювання та електронного перегрупування вмісту бази даних без його дозволу, щоб створити базу даних з того ж вмістом, що, однак, не порушує авторського права на впорядкування його бази даних;

(39) Враховуючи, що окрім намагаючи захистити авторське право на оригінальний підбір та впорядкування вмісту бази даних, ця Директива має на меті захистити становище розробників баз даних від незаконного присвоєння результатів фінансового та професійного інвестування в отримання та збирання вмісту шляхом захисту всієї бази даних чи її значущих частин від певних дій користувача та конкурента;

(40) Враховуючи, що метою цього особливого права є забезпечення захисту будь-якої інвестиції в отримання, перевірку чи представлення вмісту бази даних на обмежений час дії цього права; враховуючи, що така інвестиція може полягати у використанні фінансових ресурсів та/чи витратний часу, зусиль і енергії;

(41) Враховуючи, що метою особливого права є надання можливості розробникові бази даних перешкоджати несанкціонованому витягненню чи повторному використанню всього вмісту такої бази даних або його значної частини; враховуючи, що розробник бази даних є особою, яка провадить ініціативу і йде на ризик, здійснюючи інвестиції; враховуючи, що це виключає, зокрема, сублідрядників з визначення розробника;

(42) Враховуючи, що спеціальне право на перешкоджання несанкціонованому витягненню та/чи повторному використанню стосується дій користувача, які виходять за межі його законних прав і тим шкодять інвестуванню; враховуючи, що право забороняти витягнення чи повторне використання всього вмісту або його значної частини стосується не тільки

витовтворювання паразитичної конкурентної продукції, а й будь-якого користувача, який своїми діями завдає значної шкоди інвестуванню у якісному чи кількісному вимірі;

(43) Враховуючи, що у разі передачі в оперативному режимі право на заборону повторного використання не вичерпується як стосовно бази даних, так і стосовно матеріальної копії бази даних чи її частини, зробленої адресатом передачі за згодою власника прав;

(44) Враховуючи, що коли відображення вмісту бази даних на екрані зумовлює необхідність постійної чи тимчасової передачі такого змісту в цілому або його значної частини на інший носій інформації, така дія повинна підлягати отриманню дозволу власника прав;

(45) Враховуючи, що право перешкоджати несанкціонованому витягненню чи повторному використанню ніяким чином не становить поширення захисту авторського права на самі фати чи дані;

(46) Враховуючи, що існування права на перешкоджання несанкціонованому витягненню чи повторному використанню творів, даних або матеріалів з бази даних в цілому чи їхніх значущих частин не повинно призводити до появи нового права на самі твори, дані або матеріали;

(47) Враховуючи, що в інтересах конкуренції між постачальниками інформаційних продуктів та послуг захист особливим правом не повинен надаватися у спосіб, що полегшував би зловживання домінуючим становищем, зокрема, в тому, що стосується створення і поширення нових продуктів і послуг, які мають інтелектуальну, документальну, технічну, економічну і комерційну вартість, додану обробкою; враховуючи, що, таким чином, положення цієї Директиви не перешкоджають застосуванню правил конкуренції Співтовариства чи держав-членів;

(48) Враховуючи, що мета цієї Директиви, якою є надання належного і рівномірного рівня захисту баз даних як способу забезпечення винагороди розробникові бази даних, є відмінною від мети Директиви 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних⁷, яка має гарантувати вільний обіг персональних даних відповідно до гармонізованих правил, призначених захистити ключові права і, насамперед, право на повагу до приватного життя, визнане в статті 8 Європейської конвенції про захист прав людини і основних свобод;

враховуючи, що положення цієї Директиви не завдають шкоди законодавству про захист даних;

(49) Враховуючи, що, незважаючи на право перешкоджати несанкціонованому витягненню чи повторному використанню всієї бази даних або її значної частини, слід встановити, що розробник бази даних чи власник прав не можуть перешкоджати законному користувачеві бази даних витягувати чи повторно використовувати її незначні частини; враховуючи, однак, що користувач не може безпідставно завдавати шкоди як законним інтересам власника особливого права, так і суб'єкта авторського права чи суміжного права щодо творів або теми, які містяться в базі даних;

(50) Враховуючи, що державам-членам повинна бути надана можливість передавання винятків з права перешкоджати несанкціонованому витягненню чи повторному використанню всього вмісту бази даних або його значної частини у разі витягнення для особистих цілей, для цілей ілюстрування навчання чи наукового дослідження або тоді, коли витягнення та/чи повторне використання здійснюються в інтересах державної безпеки чи для цілей адміністративного провадження чи судочинства, враховуючи, що такі дії не повинні завдавати шкоди виключним правам розробника на експлуатацію бази даних, а їхня ціль не повинна бути комерційною;

(51) Враховуючи, що державам-члени, користуючись можливістю дозволити законному користувачеві бази даних витягати значну частину вмісту для цілей ілюстрування навчання чи наукового дослідження, можуть обмежити такий дозвіл певними категоріями навчальних чи науково-дослідних установ;

(52) Враховуючи, що тим державам-членам, які мають певні норми, що передбачають права, подібні до особливого права, передбаченого цією Директивою, потрібно дозволити зберігати в тому, що стосується нового права, ті винятки, які традиційно визначалися такими нормами;

(53) Враховуючи, що титар доведення щодо дати завершення створення бази даних лежить на розробникові бази даних;

(54) Враховуючи, що титар доведення того, що існують чинники, які дозволяють зробити висновок, що значна зміна у вмісті бази даних має розглядатися як значне нове інвестування, лежить на розробникові бази даних, що є результатом такого інвестування;

(55) Враховуючи, що значне нове інвестування, яке тягне за собою новий строк захисту, може включати перевірку вмісту бази даних щодо її суті;

(56) Враховуючи, що право на перешкоджання несанкціонованому витягненню чи повторному використанню стосовно бази даних повинно застосовуватись до баз даних, розробники яких є громадянами третіх країн або постійно в них проживають, або ж тих баз даних, які виготовлені юридичними особами, які не створені в державі-члені в розумінні Договору, тільки тоді, коли такі треті країни надають подібний захист базам даних, виготовлених громадянами держав-членів або особами, які постійно проживають на території Співтовариства;

(57) Враховуючи, що, окрім засобів правового захисту, передбачених згідно із законодавством держав-членів щодо порушень авторського права та інших прав, держави-члени повинні передбачати відповідні засоби правового захисту від несанкціонованого витягнення чи повторного використання вмісту бази даних;

(58) Враховуючи, що, окрім захисту, який надається відповідно до цієї Директиви стосовно структури бази даних авторським правом і стосовно її вмісту від несанкціонованого витягнення чи повторного використання згідно з особливим правом, продовжують застосовуватися інші правові

Директива 96/9/ЄС Європейського парламенту та Ради ЄС «Про правовий...
положення держав-членів, що стосуються постачання товар і послуг баз даних;

(59) Враховуючи, що ця Директива не перешкоджає застосуванню до баз даних, що складаються з аудіовізуальних творів, жодних правил, визначених законодавством держави-члена щодо трансмісії аудіовізуальних програм;

(60) Враховуючи, що деякі держави-члени наразі захищають, відповідно до домовленостей про авторське право, бази даних, які не відповідають критеріям підлягання захисту авторського права, викладеним у цій Директиві;

враховуючи, що навіть якщо такі бази даних підлягати захисту відповідно до їхнього права, викладеного в цій Директиві, для запобігання несанкціонованому витягненню чи повторному використанню їхнього вмісту, строк захисту відповідно до такого права є значно коротшим, ніж той, який їм надається згідно з діючими зараз національними схемами; враховуючи, що гармонізація критеріїв визначення того, чи має база даних захищатися авторським правом, не повинна призводити до скорочення строків захисту, який зараз надається відповідним власникам прав; враховуючи, що з цією метою слід встановити відступ; враховуючи, що для такого відступу повинна обмежуватися територією відповідних держав-членів,
ПРИЙНЯЛА ТАКУ ДИРЕКТИВУ:

Глава I СФЕРА ДІЇ

Стаття 1. Сфера дії

1. Ця Директива стосується правового захисту баз даних у будь-якій формі.

2. Для цілей цієї Директиви «**база даних**» означає збирання незалежних творів, даних чи інших матеріалів, які систематично чи методично упорядковані і доступні індивідуально за допомогою електронних та інших засобів.

3. Захист за цією Директивою не застосовується до комп'ютерних програм, які використовуються при створенні чи використанні баз даних, доступних за допомогою електронних засобів.

Стаття 2. Обмеження сфери дії

Ця Директива застосовується без шкоди для положень Співтовариства, пов'язаних з:

- (а) правовим захистом комп'ютерних програм;
- (б) правом на здавання в найм, правом на здавання в прокат і певними правами, пов'язаними з авторським правом у сфері інтелектуальної власності;
- (с) строком захисту авторського права та певних суміжних прав.

Глава II АВТОРСЬКЕ ПРАВО

Стаття 3. Об'єкт захисту

1. Відповідно до цієї Директиви, бази даних, які через пібір чи упорядкування їхнього вмісту є власним інтелектуальним творінням автора, захищаються як такі авторським правом. Ніжі інші критерії для визначення того, чи підлягають вони такому захисту, не застосовуються.

2. Захист авторського права на бази даних, який передбачається цією Директивою, не поширюється на їхній вміст і не перешкоджає жодним правам, які існують стосовно самого вмісту.

Стаття 4. Авторство баз даних

1. Автором бази даних є фізична особа чи група фізичних осіб, яка створила цю базу, чи, якщо це дозволяється законодавством держав-членів, юридична особа, визначена власником прав за цим законодавством.

2. Якщо законодавством держави-члена визначається колективні твори, економічні права належать тій особі, яка має авторське право.

3. Щодо бази даних, створених спільно групою фізичних осіб, володіння виключними правами є спільним.

Стаття 5. Обмежені дії

Щодо вираження бази даних, яка підлягає захисту авторським правом, автор бази даних має виключне право на здійснення чи надання дозволу на здійснення:

- (a) тимчасового або постійного відтворення будь-якими засобами і в будь-якій формі, повністю чи частково;
- (b) переказу, адаптації, переробки та будь-якої іншої зміни;
- (c) будь-якої форми публічного розповсюдження бази даних чи її копій. Перший продаж у Співтоваристві копії бази даних власником прав чи за його згодою вичерпує право на контроль перепродажу цієї копії в межах Співтовариства;
- (d) будь-якого повідомлення, демонстрації чи публічного виконання;
- (e) будь-якого відтворення, розповсюдження, повідомлення, демонстрації чи публічного виконання результатів дій, про які йдеться в пункті (b).

Стаття 6. Винятки з обмежень дії

1. Виконання законним користувачем бази даних чи її копії дій, передбачених у статті 5, що є необхідним для цілей доступу до вмісту бази даних та нормального використання цього вмісту, не вимагає дозволу автора бази даних. Якщо законний користувач отримав дозвіл на використання тільки частини бази даних, це положення застосовується тільки до цієї частини.

2. Держави-члени повинні мати можливість передбачити обмеження прав, встановлених в статті 5, у таких випадках:

- (a) у разі відтворення неелектронної бази даних для особистих цілей;
- (b) якщо використання відбувається виключно для цілей ілюстрування навчання чи наукового дослідження, за умови вказування дже-

рета і якщо це виправдано необхідністю досягнення некомерційних цілей;

(c) якщо використання відбувається для цілей державної безпеки чи для цілей адміністративного провадження чи судочинства;

(d) якщо це пов'язано з іншими винятками з авторського права, які традиційно надаються відповідно до національного законодавства, без шкоди для пунктів (a), (b) і (c).

3. Відповідно до Бернської конвенції про охорону літературних і художніх творів, ця стаття не може тлумачитися як така, що дозволяє її застосовувати у спосіб, що безпідставно перешкоджає законним інтересам власника прав чи суперечить нормальному експлуатуванню бази даних.

Глава III ОСОБЛИВІ ПРАВА

Стаття 7. Об'єкт захисту

1. Держава-член передбачає право для розробника бази даних, який продемонструє, що було зроблено якісно та/чи кількісно значні інвестиції в отримання, перевірку чи представлення вмісту, запобігати витягненню та/чи повторному використанню всього вмісту бази даних чи значної її частини у якісному чи кількісному вимірі.

2. Для цілей цієї глави:

(a) «**витягнення**» означає постійну чи тимчасову передачу всього вмісту бази даних чи значної її частини іншому носію інформації в будь-який спосіб та в будь-якій формі;

(b) «**повторне використання**» означає будь-яку форму оприлюднення всього вмісту бази даних чи значної її частини шляхом розповсюдження копій, здачі в найм, шляхом передачі в оперативному режимі чи іншої форми передачі.

Перший продаж копії бази даних у межах Співтовариства власником прав чи з його згоди вичерпує право на контроль за перепродажем цієї копії в межах Співтовариства;

Публічний прокат не є актом витягнення чи повторного використання.

3. Право, про яке йдеться в параграфі 1, може передаватися, приналежати чи надаватися відповідно до договірної ліцензії.

4. Право, передбачене в параграфі 1, застосовується незалежно від того, чи підлягає відповідна база даних захисту авторським правом чи іншими правами. Крім того, воно застосовується незалежно від того, чи підлягає вміст відповідної бази даних захисту авторським правом чи іншими правами.

Захист баз даних відповідно до права, передбаченого в параграфі 1, не перешкоджає правам, які існують щодо їхнього вмісту.

5. Не дозволяється багаторазове та систематичне витягнення і повторне використання незначних частин вмісту бази даних, що включає дії, які суперечать нормальному експлуатуванню бази даних чи які не виправдано завдають шкоди законним інтересам розробника бази даних.

Стаття 8. Права і обов'язки законних користувачів

1. Розробник бази даних, яка оприлюднюється у будь-який спосіб, не може перешкоджати законному користувачеві бази даних витягати та/чи повторно використовувати для будь-яких цілей незначні частини її вмісту у якісному чи кількісному вимірі. Якщо законний користувач має дозвіл на витягнення чи повторне використання тільки частини бази даних, цей параграф застосовується тільки до цієї частини.

2. Законний користувач бази даних, яка оприлюднюється у будь-який спосіб, не може виконувати такі дії, які суперечать нормальному експлуатуванню бази даних чи не виправдано завдають шкоди законним інтересам розробника бази даних.

3. Законний користувач бази даних, яка оприлюднюється у будь-який спосіб, не може надавати шкоди суб'єктові авторського чи суміжного права щодо творів чи тем, які містяться в базі даних.

Стаття 9. Винятки з особливого права

Держави-члени можуть передбачити, що законні користувачі баз даних, які оприлюднюються у будь-який спосіб, можуть без дозволу її розробника витягати чи повторно використовувати значну частину її вмісту:

- (а) у разі витягнення для особистих цілей вмісту неелектронної бази даних;
- (б) у разі витягнення для цілей ілюстрування навчання чи наукового дослідження, за умови вказування джерела і якщо це виправдано необхідністю досягнення некомерційних цілей;
- (с) у разі витягнення та повторного використання для цілей державної безпеки чи для цілей адміністративного провадження або судочинства.

Стаття 10. Строк захисту

1. Право, передбачене в статті 7, починається з дня завершення створення бази даних. Воно закінчується через п'ятнадцять років з першого січня року, який наступає після дня завершення.

2. У разі бази даних, яка оприлюднюється у будь-який спосіб до завершення періоду, передбаченого в параграфі 1, строк захисту цього права закінчується через п'ятнадцять років з першого січня року, який наступає після першого оприлюднення бази даних.

3. Будь-яка значна зміна вмісту бази даних у якісному чи кількісному вимірі, включаючи будь-яку значну зміну внаслідок накопичення послдовних доповнень, вилучень чи змін, що призводить до того, що база даних розглядається як значне нове інвестування у якісному чи кількісному вимірі, надає базі даних, яка є результатом такого інвестування, право на окремий строк захисту.

Стаття 11. Особи, які користуються захистом відповідно до особливого права

1. Право, передбачене в статті 7, застосовується до бази даних, розробники якої чи власники прав на яку є громадянами держави-члена чи постійно проживають на території Співтовариства.

2. Параграф 1 також застосовується до компаній та фірм, які утворені відповідно до законодавства держави-члена і мають свої зареєстровані ус-

танови, центральне управління або основне місце ведення діяльності в Співтоваристві; однак, якщо така компанія чи фірма має на території Співтовариства тільки свою зареєстровану установу, її діяльність повинна бути справедливо пов'язана у даний час із економікою держави-члена.

3. Угоди щодо поширення права, передбаченого в статті 7, на бази даних, які створені в третій країнах і виходять за межі положень параграфів 1 і 2, укладаються Радою, яка діє відповідно до пропозицій Комісії. Строк такого захисту, який поширюється на бази даних згідно з цією процедурою, не перевищує той, який надається відповідно до статті 10.

Глава IV ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 12. Засоби правового захисту

Держави-члени забезпечують належні засоби правового захисту стосовно порушень прав, передбачених цією Директивою.

Стаття 13. Продовження застосування інших правових положень

Ця Директива не перешкоджає положенням, що стосуються, зокрема, авторського права, прав, пов'язаних з авторським чи іншими правами та обов'язками, що існують щодо даних, творів чи інших матеріалів, які входять до бази даних, патентних прав, торгових марок, прав на промислові зразки, захисту національних надбань, законодавства про обмежуючі дії та несправедливу конкуренцію, торгових таємниць, безпеки, конфіденційності, захисту даних і невтручання в приватне життя, доступу до офіційних документів, а також договірних правах.

Стаття 14. Застосування в часі

1. Захист відповідно до цієї Директиви стосовно авторського права також надається щодо баз даних, які створені до дня, про який йдеться в статті 16 (1), і які на цю дату відповідають вимогам, встановленим цією Директивою щодо захисту авторського права на бази даних.

2. Незважаючи на параграф 1, якщо база даних, що захищається відповідно до домовленостей про авторське право в державі-члені, на день публікації цієї Директиви не відповідає критеріям підлягання захисту авторського права, викладеним у статті 3 (1), ця Директива не призводить до скасування в цій державі-члені решти строку захисту, що надається відповідно до цих домовленостей.

3. Захист відповідно до положень цієї Директиви стосовно права, передбаченого в статті 7, також надається стосовно баз даних, створення яких було завершено не пізніше п'ятнадцяти років до дня, вказаного в статті 16 (1), і які на цей день відповідали вимогам, встановленим у статті 7.

4. Захист, передбачений у параграфах 1 і 3, не перешкоджає жодним актам, укладеним, і жодним правам, набутим до дня, про який йдеться в цих параграфах.

5. У разі бази даних, створення якої було завершено не пізніше, як за п'ятнадцять років до дня, вказаного в статті 16 (1), строк захисту, передбачений у статті 7, закінчується через п'ятнадцять років з першого січня, яке наступає після цього дня.

Стаття 15. **Обов'язковість деяких положень**

Будь-яке договірне положення, що суперечить статтям 6 (1) і 8, є недійсним.

Стаття 16. **Заключені положення**

1. Держави-члени приймають закони, постанови та адміністративні положення, необхідні для виконання цієї Директиви не пізніше 1 січня 1998 року.

Коли держави-члени приймають такі положення, останні повинні містити посилення на цю Директиву чи супроводжуватися таким посиленням у разі їх офіційної публікації. Методи, за якими робиться таке посилення, встановлюються державами-членами.

2. Держави-члени передають Комісії текст основних положень національного законодавства, які вони прийняли у сфері, що регулюється цією Директивою.

3. Не пізніше як наприкінці третього року з дати, про яку йдеться в параграфі, та кожні три роки після цього Комісія подає Європейському Парламенту, Раді та і Комітету з економічних і соціальних питань доповідь про застосування цієї Директиви, у якій вона, серед іншого, на основі спеціальної інформації, яку подають держави-члени, розглядає застосування особливого права, включаючи статті 8 і 9, а також особливо перевіряє, чи застосування цього права призвело до зловживання домінуючим становищем або іншого втручання у вільну конкуренцію, яке б випрадалало життя відповідних заходів, включаючи створення недобровільних механізмів ліцензування.

Якщо необхідно, вона передає пропозиції для коригування цієї Директиви відповідно до перетворень, які відбулись у сфері баз даних.

Стаття 17

Цю Директиву адресовано державам-членам. Вчинено в Страсбурзі 11 березня 1996 року.

За Європейський Парламент
Президент К. ХЕНШ
За Раду Президент Л. ДІНІ

Офіційний журнал L 077, 27/03/1996 с. 0020—0028

ДИРЕКТИВА 97/66/ЄС СТОСОВНО ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ І ЗАХИСТУ ПРАВА НА НЕВТРУЧАННЯ В ОСОБИСТЕ ЖИТТЯ В ТЕЛЕКОМУНІКАЦІЙНОМУ СЕКТОРІ

(Прийнято Європейським парламентом та Радою ЄС 15 грудня 1997 р.)

Офіційний переклад

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ і РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

Беручи до уваги Договір про заснування Європейського Співтовариства (94_017)¹ і, зокрема, його статтю 100 а,

Беручи до уваги пропозицію Комісії²,

Беручи до уваги висновок Економічного і соціального комітету³,

Діючи відповідно до процедури, викладеної в статті 189б Договору (94_017)³, в світлі спільного тексту, затвердженого Угодувальним комітетом 6 листопада 1997 року,

(1) Враховуючи, що Директива 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних (94_242)⁴ вимагає, щоб держави-члени забезпечували права та свободи фізичних осіб при обробці персональних даних і, зокрема, їхнє право на невтручання в особисте життя, з метою забезпечення вільного потоку персональних даних в Співтоваристві;

(2) Враховуючи, що конфіденційність зв'язку гарантується відповідно до міжнародних документів, що стосуються прав людини (зокрема, Європейської конвенції про захист прав людини і основних свобод (95_004), а також конституцій держав-членів;

(3) Враховуючи, що зараз в Співтоваристві в телекомунікаційних мережах загального користування запроваджуються нові передові цифрові технології, які зумовлюють певні вимоги щодо захисту персональних даних та невтручання в особисте життя користувачів; враховуючи, що розвиток інформаційного суспільства характеризується запровадженням нових телекомунікаційних послуг;

враховуючи, що успішний транскордонний розвиток таких послуг, як, наприклад, відео на вимогу, інтерактивного телебачення, частково зале-

¹ ОJ C 200, 22.7.1994, р. 4.

² ОJ C 159, 17.6.1991, р. 38.

³ Висновок Європейського Парламенту від 11 березня 1992 року (ОJ C 94, 13.4.1992, р. 198), Спільна позиція Ради від 12 вересня 1996 року (ОJ C 315, 24.10.1996, р. 30) і Рішення Європейського Парламенту від 16 січня 1997 року (ОJ C 33, 3.2.1997, р. 78). Рішення Європейського Парламенту від 20 листопада 1997 року (ОJ C 371, 8.12.1997). Рішення Ради від 1 грудня 1997 року.

⁴ ОJ L 281, 23.11.1995, р. 31.

жити від віри користувачів в те, що загрози втручання в їхнє особисте життя немає;

(4) Враховуючи, що це стосується, зокрема, випадку із запровадженням цифрової мережі зв'язку з комплексними послугами (ISDN) та цифрових мобільних мереж;

(5) Враховуючи, що Рада у своїй Резолюції від 30 червня 1988 року про розвиток спільного ринку телекомунікаційних послуг і обладнання до 1992 року⁵ закликає вжити кроків для захисту персональних даних з метою створення належного середовища для майбутнього розвитку телекомунікацій в Співтоваристві; враховуючи, що Рада ще раз наголосила на важливості захисту персональних даних та невтручання в особисте життя в своїй Резолюції від 18 липня 1989 року про посилення координації для запровадження цифрової мережі зв'язку з комплексними послугами (ISDN) в Європейському Співтоваристві до 1992 року⁶;

(6) Враховуючи, що Європейський Парламент підкреслив важливість захисту персональних даних та невтручання в особисте життя в телекомунікаційних мережах, зокрема, з огляду на запровадження цифрової мережі зв'язку з комплексними послугами (ISDN);

(7) Враховуючи, що у випадку телекомунікаційних мереж загального користування слід розробити спеціальні правові, регулятивні та технічні положення з метою захисту основних прав і свобод фізичних осіб та законних інтересів юридичних осіб, зокрема, з огляду на зростання ризику, пов'язаного з автоматичним зберіганням та обробкою даних, що стосуються абонентів і користувачів;

(8) Враховуючи, що правові, регулятивні та технічні положення, прийняті державами-членами стосовно захисту персональних даних, невтручання в особисте життя та законних інтересів юридичних осіб у телекомунікаційному секторі, повинні бути гармонізовані для того, щоб уникнути перешкод на внутрішньому ринку телекомунікацій, відповідно до мети, встановленої в статті 7а Договору (94_017); враховуючи, що така гармонізація обмежується вимогами, які необхідні для гарантування того, що не буде створено перешкод на шляху сприяння поширенню і розвитку нових телекомунікаційних послуг і мереж між державами-членами;

(9) Враховуючи, що держави-члени, відповідні поставальники та користувачі, разом з компетентними органами Співтовариства, повинні співпрацювати у запровадженні і розробці відповідних технологій, якщо це необхідно для застосування гарантій, передбачених положеннями цієї Директиви;

(10) Враховуючи, що такі нові послуги включають інтерактивне телебачення та відео на вимогу;

(11) Враховуючи, що в телекомунікаційному секторі, зокрема, в усіх питаннях, що стосуються захисту основних прав і свобод, які окремо не

охоплюються положеннями цієї Директиви, включаючи зобов'язання, які покладаються на контролерів, і права осіб, застосовується Директива 95/46/ЄС (994_242); враховуючи, що Директива 95/46/ЄС застосовується до телекомунікаційних послуг, які не є загальнодоступними;

(12) Враховуючи, що ця Директива, подібно до того, що передбачається в статті 3 Директиви 95/46/ЄС (994_242), не розглядає питань захисту основних прав і свобод, пов'язаних із діяльністю, що не регулюється правом Співтовариства; враховуючи, що держави-члени самі мають вживати заходів, які вони вважатимуть необхідними для захисту громадського порядку, оборони, державної безпеки (включаючи економічний добробут держави, коли діяльність стосується питань безпеки держави), а також застосування кримінального права; враховуючи, що ця Директива не впливає на здатність держав-членів здійснювати законне перехоплення телекомунікацій для будь-яких із перелічених цілей;

(13) Враховуючи, що абоненти загальнодоступної телекомунікаційної послуги можуть бути фізичними чи юридичними особами; враховуючи, що положення цієї Директиви спрямовані на захист, шляхом доповнення Директиви 95/46/ЄС (994_242), основних прав фізичних осіб і, зокрема, їхнього права на невтручання в особисте життя, а також законних інтересів юридичних осіб;

враховуючи, що ці положення в жодному разі не можуть накласти на держав-членів зобов'язання поширювати застосування Директиви 95/46/ЄС на захист законних інтересів юридичних осіб; враховуючи, що такий захист забезпечується в рамках відповідного законодавства Співтовариства і держав-членів;

(14) Враховуючи, що застосування певних вимог, пов'язаних з показуванням та обмеженням визначення лінії, з якої робиться з'єднання і з якою з'єднуються, та з автоматичного передавцяцією дзвінка на лінії або-абонентів, підключених до аналогового АТС, не повинне бути обов'язковим в окремих випадках, коли таке застосування виявилось б технічно неможливим чи вимагало б непропорційних економічних зусиль; враховуючи, що для зацікавлених сторін важливо бути поінформованими про такі випадки і що тому держави-члени повинні доводити їх до відома Комісії;

(15) Враховуючи, що поставальники послуг повинні вживати необхідних заходів для гарантування безпеки своїх послуг, якщо необхідно — спільно з оператором мережі, а також інформувати абонентів про особливі загрози порушення безпеки мережі;

враховуючи, що безпека оцінюється в світлі положення статті 17 Директиви 95/46/ЄС (994_242);

(16) Враховуючи, що слід вжити заходів для запобігання несанкціонованому доступу до зв'язку, щоб захистити конфіденційність зв'язку через телекомунікаційні мережі загального користування та за допомогою загальнодоступних телекомунікаційних послуг; враховуючи, що національне законодавство в деяких державах-членах забороняє навмисний несанкціонований доступ до зв'язку;

⁵ ОІ С 257, 4.10.1988, р. 1.

⁶ ОІ С 196, 10.8.1989, р. 4.

(17) Враховуючи, що дані, які стосуються абонентів і які обробляються для встановлення дзвінків, містять інформацію про особисте життя фізичних осіб і пов'язані з правом на поважання таємниці їхнього листування чи пов'язані із законними інтересами юридичних осіб; враховуючи, що такі дані можуть зберігатися тільки тоді, коли це необхідно при наданні послуги для цілей виставляння рахунків чи розрахунків за споживання, і тільки протягом обмеженого часу; враховуючи, що будь-яка подальша обробка, яку може заохотити здійснити постачальник загальнодоступних телекомунікаційних послуг для цілей просування на ринку власних телекомунікаційних послуг, може дозволитися лише у разі, коли абонент надає на це згоду відповідно до точної та повної інформації, наданої постачальником загальнодоступних телекомунікаційних послуг щодо видів подальшої обробки, яку він має намір здійснити;

(18) Враховуючи, що запровадження деталізованих рахунків покращило можливість перевірки абонентом правильності платежів, які стягуються постачальником послуг; враховуючи, що, в той же час, воно може загрозувати таємниці особистого життя користувачів загальнодоступних телекомунікаційних послуг; враховуючи, що, таким чином, для збереження таємниці особистого життя користувача держави-члени повинні заохочувати розвиток таких варіантів телекомунікаційних послуг, як альтернативні механізми платежів, що уможливають анонімний та цілком конфіденційний доступ до загальнодоступних телекомунікаційних послуг, наприклад, телефонні картки чи механізми оплати кредитною карткою; враховуючи, що в якості альтернативи держави-члени можуть з тією ж метою вимагати вилучення певної кількості цифр з номерів, на які здійснюється дзвінок і які вказуються в деталізованих рахунках;

(19) Враховуючи, що в тому, що стосується визначення лінії, з якої здійснюється дзвінок, необхідно захистити право сторони, яка здійснює дзвінок, приховувати показування визначення лінії, з якої робиться дзвінок, і права сторони, якій дзвонять, відхилити дзвінки з невизначених ліній; враховуючи, що справедливо відхилити показування визначення лінії, з якої робиться дзвінок, в окремих випадках; враховуючи, що деякі абоненти, зокрема лінії допомоги і такі інші організації, зацікавлені в збереженні анонімності осіб, які їм дзвонять; враховуючи, що в тому, що стосується визначення лінії, необхідно захистити право і законний інтерес сторони, якій дзвонять, приховувати показування визначення лінії, до якої сторона, якій дзвонять, підключена, зокрема, у разі передресованих дзвінків; враховуючи, що постачальники загальнодоступних телекомунікаційних послуг повинні інформувати своїх абонентів про існування визначення ліній, з яких і на які робляться дзвінки в мережі, а також про всі послуги, які пропонуються на базі визначення ліній, з яких і на які робляться дзвінки, і про наявні варіанти таємності; враховуючи, що це дозволяє абонентам зробити поінформований вибір про механізми таємності, які вони хочуть використовувати; враховуючи, що варіанти таємності, які надаються окремо по кожній лінії, не обов'язково повинні існувати у вигляді автоматичної мережевої послуги, а можуть бути доступними також і

на просте прохання до постачальника загальнодоступної телекомунікаційної послуги;

(20) Враховуючи, що слід передбачити захист абонентів від незручностей, які може створити автоматична передресация дзвінків іншими особами; враховуючи, що в таких випадках повинна існувати можливість для абонентів припинити перекладення передресованих дзвінків на їхні термінали шляхом простого звертання з проханням про це до постачальника загальнодоступної телекомунікаційної послуги;

(21) Враховуючи, що телефонні довідники широко розповсюджуються і є загальнодоступними; враховуючи, що право на невтручання в особисте життя фізичних осіб та законні інтереси юридичних осіб вимагають, щоб абоненти мали змогу визначати те, якою мірою їхні персональні дані публікуватимуться в телефонному довіднику; враховуючи, що держави-члени можуть обмежувати цю можливість для абонентів, які є фізичними особами;

(22) Враховуючи, що слід передбачити заходи охорони абонентів від втручання в їхнє особисте життя через незахищені дзвінки чи телефакси; враховуючи, що держави-члени можуть обмежити такі заходи для абонентів, які є фізичними особами;

(23) Враховуючи, що необхідно забезпечити гармонізацію введення технічних характеристик телекомунікаційного обладнання для цілей захисту даних, з метою забезпечення відповідності реалізації внутрішнього ринку;

(24) Враховуючи, що, зокрема, аналогічно до того, що передбачено в статті 13 Директиви 95/46/ЄС (994_242), держави-члени можуть обмежити за певних обставин обсяги прав і обов'язків абонентів, наприклад, шляхом забезпечення можливості постачальника загальнодоступної телекомунікаційної послуги не брати до уваги скасування показування визначення лінії, з якої робиться дзвінок, відповідно до національного законодавства для цілей запобігання і виявлення кримінальних злочинів чи державної безпеки;

(25) Враховуючи, що у разі недотримання прав користувачів та абонентів, національне законодавство має передбачати засіб судового захисту; враховуючи, що санкції повинні накладатися на будь-яку особу, яка не дотримується національних заходів, вжитих відповідно до цієї Директиви, незалежно від того, є така особа суб'єктом приватного чи публічного права;

(26) Враховуючи, що в сфері застосування цієї Директиви корисно враховувати досвід Робочої групи з питань захисту осіб при обробці персональних даних, до якої входять представники наглядових органів держав-членів і яка встановлена відповідно до статті 29 Директиви 95/46/ЄС (994_242);

(27) Враховуючи, що, виходячи з технологічного розвитку та очікуючи на еволюцію послуг, які пропонуються, буде необхідно уточнити в технічному аспекті категорії даних, перелічені в Додатку до цієї Директиви, для застосування статті 6 цієї Директиви з допомогою Комітету у складі

представників держав-членів, створеному відповідно до статті 31 Директиви 95/46/ЄС (994_242), з метою забезпечення узгодженого застосування вимог, встановлених у цій Директиві, незважаючи на зміни в технологіях; враховуючи, що ця процедура застосовується тільки до специфікацій, необхідних для модифікації додатка з врахуванням змін на ринку та в споживачському попиті; враховуючи, що Комісія повинна належним чином інформувати Європейський Парламент про свій намір застосувати цю процедуру, і враховуючи, що в протилежному випадку повинна застосовуватися процедура, встановлена в статті 100а Договору;

(28) Враховуючи, що для сприяння дотриманню положень цієї Директиви потрібні певні спеціальні домовленості щодо обробки даних, яка триває на день набуття чинності національним імплементаційним законодавством відповідно до цієї Директиви,

ПРИЙНЯЛИ ТАКУ ДИРЕКТИВУ:

Стаття 1. Мета та сфера дії

1. Ця Директива передбачає гармонізацію положень держав-членів, необхідну для забезпечення однакового рівня захисту основних прав і свобод, зокрема, в тому, що стосується права на невтручання в особисте життя, при обробці персональних даних в телекомунікаційному секторі та для забезпечення вільного переміщення таких даних, а також телекомунікаційного обладнання і послуг у Співтоваристві.

2. Положення цієї Директиви уточнюють та доповнюють Директиву 95/46/ЄС (994_242) для цієї, вказаних в параграфі 1. Крім того, вони передбачають захист законних інтересів абонентів — юридичних осіб.

3. Ця Директива не застосовується до діяльності, що виходить за межі права Співтовариства, такої як та, що передбачена в розділах V і VI Договору про Європейський Союз (994_029), і, в жодному разі, до діяльності, що стосується громадського порядку, оборони, державної безпеки (включаячи економічний добробут держави, коли діяльність стосується питань безпеки держави), а також діяльності держави в сфері кримінального права.

Стаття 2. Визначення

На додачу до визначень, наведених у Директиві 95/46/ЄС (994_242), для цієї Директиви:

(а) «**абонент**» означає будь-яку фізичну чи юридичну особу, яка є стороною в контракті з постачальником загальнодоступних телекомунікаційних послуг стосовно надання таких послуг;

(б) «**користувач**» означає будь-яку фізичну особу, яка користується загальнодоступною телекомунікаційною послугою для особистих чи ділових цілей, при цьому передплата цієї послуги не є обов'язковою;

(с) «**телекомунікаційна мережа загального користування**» означає системи передавання і, у відповідних випадках, комутаційне обладнання та інші ресурси, що дозволяють передавати сигнали між визначеними кінцевими

пунктами за допомогою телеграфу, радіо, оптичних чи інших електромагнітних засобів, які використовуються, повністю чи частково, для надання загальнодоступних телекомунікаційних послуг;

(д) «**телекомунікаційна послуга**» означає послуги, надання яких повністю чи частково полягає в передачі та маршрутизації сигналів у телекомунікаційних мережах, за винятком радіо- та телевізійного мовлення.

Стаття 3. Послуги, до яких застосовується Директива

1. Ця Директива застосовується до обробки персональних даних у зв'язку з наданням загальнодоступних телекомунікаційних послуг у телекомунікаційних мережах загального користування в Співтоваристві, зокрема, через цифрову мережу зв'язку з комплексними послугами (ISDN) та цифрові мобільні мережі загального користування.

2. Статті 8, 9 і 10 застосовуються до абонентських ліній, підключених до цифрових АТС, і, якщо це технічно можливо і не вимагає несутірних економічних зусиль, — до абонентських ліній, підключених до аналогових АТС.

3. Держави-члени повідомляють Комісію про випадки, коли виконати вимоги статей 8, 9 і 10 технічно неможливо або ж це вимагає несутірних інвестицій.

Стаття 4. Безпека

1. Постачальник загальнодоступної телекомунікаційної послуги повинен вживати відповідних технічних та організаційних заходів для гарантування безпеки своїх послуг, якщо потрібно, спільно з оператором телекомунікаційної мережі загального користування в тому, що стосується безпеки мережі.

3 врахуванням сучасного стану науки і техніки, а також вартості їхньої реалізації, такі заходи забезпечують рівень безпеки, що відповідає передставленому ризику.

2. У разі особливого ризику порушення безпеки мережі постачальник загальнодоступної телекомунікаційної послуги повинен повідомити абонентів про такий ризик та будь-які можливі засоби захисту, включаючи пов'язані з цим витрати.

Стаття 5. Конфіденційність зв'язку

1. Держави-члени забезпечують у національних положеннях конфіденційність зв'язку за допомогою телекомунікаційної мережі загального користування та загальнодоступних телекомунікаційних послуг. Зокрема, вони забороняють прослуховування, перехоплення, зберігання та інші види перехоплювання і наглядів за зв'язком, окрім того, що здійснюється користувачами, без згоди відповідних користувачів, за винятком випадків, коли на це існує законний дозвіл відповідно до статті 14 (1).

2. Параграф 1 не зачіпає жодного законно санкціонованого записування зв'язку в ході законної економічної діяльності з метою надання доказів комерційної транзакції чи будь-якого іншого економічного зв'язку.

Стаття 6. Дані щодо потоку обміну і рахунків

1. Дані щодо потоку обміну, які стосуються абонентів та користувачів і які обробляються для встановлення дзвінка і зберігаються оператором телекомунікаційної мережі загального користування та/чи постачальником загальнодоступної телекомунікаційної послуги, повинні стиратися чи перетворюватися на анонімі після завершення дзвінка без шкоди для положень параграфів 2, 3 і 4.

2. Для цілей виставляння рахунків абонентам і здійснення оплати за сполучення можуть оброблятися вказані в Додатку дані.

Така обробка дозволяється тільки до завершення періоду, протягом якого рахунок може законно бути оспорений чи протигом якого платіж може вимагатися в судовому порядку.

3. Для цілей просування на ринку власних телекомунікаційних послуг постачальник загальнодоступної телекомунікаційної послуги може обробляти дані, про які йдеться в параграфі 2, якщо абонент дав на це свою згоду.

4. Обробка даних щодо потоку обміну та рахунків має обмежуватися особами, які діють у рамках повноважень операторів телекомунікаційних мереж загального користування та/чи постачальників загальнодоступних телекомунікаційних послуг, які займаються виставлянням рахунків чи управлінням потоками обміну, запитами клієнтів, виявленням обману та збутом власних телекомунікаційних послуг постачальника, і ця обробка не повинна виходити за межі того, що необхідно для цілей такої діяльності.

5. Параграфи 1, 2, 3 і 4 застосовуються без шкоди для можливості інформування компетентних органів про дані щодо рахунків та потоків обміну відповідно до застосовуваного законодавства з метою вирішення спорів, зокрема спорів щодо сполучення чи рахунків.

Стаття 7. Деталізовані рахунки

1. Абоненти мають право на отримання деталізованих рахунків.

2. Держави-члени застосовують національні положення для угодження прав абонентів, які отримують деталізовані рахунки, з правом на не-втручання в особисте життя користувачів, які з'єднуються, і абонентів, з якими з'єднуються, наприклад, шляхом забезпечення того, що для таких користувачів і абонентів існують достатні альтернативні модальності.

Стаття 8. Показування і обмеження визначення ліній, з яких і на які здійснюється дзвінок

1. Якщо пропонується показування ліній, з якої робиться дзвінок, користувач, який робить дзвінок, повинен мати можливість за допомогою простих засобів безкоштовно скасовувати показування ліній, з якої робиться дзвінок, окремо для кожного дзвінка.

Абонент, який здійснює дзвінок, повинен мати таку можливість окремо для кожної лінії.

2. Якщо пропонується показування ліній, з якої робиться дзвінок, абонент, якому дзвонять, повинен мати можливість за допомогою простих засобів безкоштовно для розумного користування цією функцією запобігати показуванню визначення лінії, з якої робиться дзвінок, для вхідних дзвінків.

3. Якщо пропонується показування ліній, з якої робиться дзвінок, і якщо лінія, з якої робиться дзвінок, визначається до встановлення дзвінка, абонент, якому дзвонять, повинен мати можливість за допомогою простих засобів відхилити вхідні дзвінки, коли показування визначення лінії, з якої робиться дзвінок, було скасоване користувачем чи абонентом, які дзвонять.

4. Якщо пропонується показування ліній, з якою існує з'єднання, абонент, якому дзвонять, повинен мати можливість за допомогою простих засобів безплатно скасовувати показування визначення лінії, з якою існує з'єднання, для користувача, який дзвонить.

5. Положення, викладені в параграфі 1, також застосовуються щодо дзвінків із Співтовариства в третій країні; положення, встановлені в параграфі 2, 3 і 4, також застосовуються до вхідних дзвінків з третій країни.

6. Держави-члени забезпечують, щоб у разі надання показування ліній, з якої робиться дзвінок чи з якою існує з'єднання, постачальники загальнодоступних телекомунікаційних послуг інформували громадськість про це та про можливість, встановлені в параграфах 1, 2, 3 і 4.

Стаття 9. Винятки

Держави-члени забезпечують існування прозорих процедур, якими б регулювався спосіб, у який оператор телекомунікаційної мережі загального користування та/чи постачальник загальнодоступної телекомунікаційної послуги може відхилити скасування показування визначення лінії, з якої робиться дзвінок:

(а) тимчасово — після подання абонентом заяви з проханням прослідкувати зловмисні дзвінки чи дзвінки, які порушують спокій; у такому разі, відповідно до національного законодавства, дані, які містять визначення абонента, який дзвонить, зберігатимуться і оприлюднюватимуться оператором телекомунікаційної мережі загального користування та/чи постачальником загальнодоступної телекомунікаційної послуги;

(б) окремо для певних ліній — для організацій, які займаються екстреними викликами і визнані такими державою-членом, включаючи правоохоронні органи, службу швидкої допомоги та пожежні бригади, з метою відповіді на такі дзвінки.

Стаття 10. Автоматична передресация дзвінка

Держави-члени забезпечують, щоб будь-якому абоненту надавалася можливість безкоштовно і за допомогою простих засобів припинити автоматичну передресацию дзвінка третьою стороною на термінал абонента.

Стаття 11. Телефонні довідники абонентів

1. Персональні дані, що містяться в друкованих чи електронних телефонних довідниках абонентів, які є загальнодоступними чи надаються через довідкову службу, повинні обмежуватися тим, що необхідно для визначення певного абонента, якщо тільки абонент не надав своєї незвозначної згоди на публікацію додаткових персональних даних.

Абонент має право на безкоштовне випущення його даних з друкованого чи електронного телефонного довідника на його прохання, на вказування, що його особисті дані не можуть використовуватися для цієї прямого маркетингу, часткове випущення його адреси та невключення останніх, що свідчили б про його статів, якщо це можливо з лінгвістичної точки зору.

2. Незважаючи на параграф 1, держави-члени можуть дозволити операторам вимагати оплати від абонентів, які бажають, щоб деталі, які їх стосуються, не включалися в довідник, за умови, що відповідна сума не слугувала перешкодою для здійснення цього права і що, враховуючи вимоги якості, які висуваються до загальнодоступного довідника з огляду на загальне обслуговування, вона не перевищувала дійсних витрат, яких зазнає оператор у разі адаптації і коригування списку абонентів, які не підлягають включенню в загальнодоступний довідник.

3. Права, які надаються параграфом 1, застосовуються до абонентів, які є фізичними особами. Держави-члени також гарантують, у рамках законодавства Співтовариства і застосовуваного національного законодавства, що законні інтереси абонентів, інших ніж фізичні особи, також достатньо захищені в тому, що стосується їхнього включення до загальнодоступних довідників.

Стаття 12. Незапитувані дзвінки

1. Використання автоматичних викличних систем без людського втручання (пристрій автоматичного виклику) чи факсимільних пристроїв (факсу) для цілей прямого маркетингу може дозволитися тільки стосовно абонентів, які дали на це свою попередню згоду.

2. Держави-члени вживають необхідних заходів для забезпечення того, що без стягнення плати за це незапитувані дзвінки для цієї прямого маркетингу за допомогою засобів, інших ніж ті, про які йдеться в параграфі 1, не дозволяються або у разі відсутності згоди відповідних абонентів, або стосовно абонентів, які не бажають отримувати такі дзвінки, при цьому вибір між цими варіантами визначається національним законодавством.

3. Права, які надаються параграфами 1 і 2, застосовуються до абонентів, які є фізичними особами. Держави-члени також гарантують, у рамках законодавства Співтовариства і застосовуваного національного законодавства, що законні інтереси абонентів, інших ніж фізичні особи, також достатньо захищені в тому, що стосується незапитуваних дзвінків.

Стаття 13. Технічні параметри та стандартизація

1. При застосуванні положень цієї Директиви держави-члени забезпечують, за умови виконання параграфів 2 і 3, що стосовно термінального чи іншого телекомунікаційного обладнання не встановлюється жодних обов'язкових вимог щодо технічних параметрів, які могли б перешкодити розміщенню обладнання на ринку та вільному обігу такого обладнання в державах-членах та між ними.

2. Якщо положення цієї Директиви можуть бути виконані тільки шляхом встановлення вимог щодо технічних параметрів, держави-члени інформують Комісію відповідно до порядку, передбаченого Директивою 83/189/ЄС⁷, якою встановлюється порядок надання інформації в сфері технічних стандартів та правил.

3. Якщо необхідно, Комісія забезпечуватиме складання спільних європейських стандартів для запровадження певних технічних параметрів, відносно до законодавства Співтовариства про наближення законів держав-членів щодо телекомунікаційного термінального обладнання, включаючи взаємне визнання їхньої узгодженості, а також Рішення Ради 87/95/ЄС від 22 грудня 1986 року про стандартизацію в сфері інформаційних технологій і телекомунікацій⁸.

Стаття 14. Поширення сфери застосування деяких положень Директиви 95/46/ЄС

1. Держави-члени можуть приймати законодавчі положення для обмеження сфери дії обов'язків та прав, передбачених у статтях 5, 6 і статті 8(1), (2), (3) і (4), коли таке обмеження є необхідним заходом для гарантування національної безпеки, громадського порядку, запобігання, розслідування, розкриття і переслідування кримінальних злочинів чи несанкціонованого використання телекомунікаційної системи, як про це йдеться в статті 13(1) Директиви 95/46/ЄС (994_242).

2. Положення Глави III щодо засобів судового захисту, відповідальності та санкцій Директиви 95/46/ЄС (994_242) застосовуються стосовно національних положень, прийнятих на виконання цієї Директиви, а також стосовно окремих прав, які випливають з цієї Директиви.

3. Робоча група з питань захисту фізичних осіб при обробці персональних даних, створена відповідно до статті 29 Директиви 95/46/ЄС (994_242), виконує завдання, визначені в статті 30 вищезгаданої Директиви, також у тому, що стосується захисту основних прав і свобод та законних інтересів у телекомунікаційному секторі, який є предметом цієї Директиви.

⁷ ОJ L 109, 26.04.1983, р. 8. Директива з поправками, востаннє внесеними Директивою 94/10/ЄС (ОJ L 100, 19.4.1994, р. 30).

⁸ ОJ L 36, 7.02.1987, р. 31. Рішення з поправками, востаннє внесеними Актом про присвоєння 1994 року.

4. Комісія з допомогою Комітету, створеного відповідно до статті 31 Директиви 95/46/ЄС (994_242), технічно визначає Додаток відповідно до процедури, заданої в цій статті.

Вищезгаданий Комітет складається спеціально для розгляду питань, які охоплюються цією Директивою.

Стаття 15. Імплементация цієї Директиви

1. Держави-члени приймають закони, постанови та адміністративні положення, необхідні для виконання цієї Директиви, не пізніше 24 жовтня 1998 року.

Шляхом відступу від першого абзацу держави-члени приймають закони, постанови та адміністративні положення, необхідні для виконання статті 5 цієї Директиви, не пізніше 24 жовтня 2000 року.

Коли держави-члени приймають такі положення, останні повинні містити посилання на цю Директиву чи супроводжуватися таким посиланням у разі їхньої офіційної публікації. Порядок, за яким робиться таке посилання, приймається державами-членами.

2. Шляхом відступу від статті 6(3) згода не вимагається стосовно обробки, яке вже триває на день набуття чинності національними положеннями відповідно до цієї Директиви. У таких випадках абоненти інформуються про цю обробку, і, якщо вони не виражають своєї незгоди протягом періоду, який має визначити держава-член, вони вважаються такими, що надали свою згоду.

3. Стаття 11 не застосовується до видань довідників, які були опубліковані до набуття чинності національними положеннями відповідно до цієї Директиви.

4. Держави-члени передають Комісії текст основних положень національного законодавства, які вони прийняли у сфері, що регулюється цією Директивою.

Стаття 16. Адресати

Ця Директива адресована державам-членам.

Вчинено в Брюсселі, 15 грудня 1997 року.

За Європейський Парламент Президент Ж.М. Жиль-Роблес
За Раду Президент Дж.С. Джанкер

Додаток

ПЕРЕЛІК ДАНИХ

Для цілей, про які йдеться в статті 6(2), можуть оброблятися такі дані:

- Дані, що містять;
- номер чи розпізнавальний знак термінала абонента;
- адресу абонента та тип термінала;

- загальну кількість юнітів, які створюються за звітний період;
- номер абонента, якому дзвонять;
- тип, початковий час та тривалість з'єднань, які було здійснено, і обсяг переданої інформації;

- дату дзвінка/надання послуги;
- іншу інформацію стосовно платежів, наприклад аванс, часткові виплати, від'єднання та залишок.

Офіційний журнал L 024, 30/01/1998 р. 0001—0008

Переклад здійснено Центром перекладів актів Європейського права при Міністерстві юстиції України.

ДИРЕКТИВА 99/93/ЄС ПРО ЕЛЕКТРОННИЙ ПІДПИС

(Прийнято Європейським парламентом та Радою ЄС 13 грудня 1999 р.)

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ ТА РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ, беручи до уваги:

Угоду про утворення Європейського Співтовариства і, зокрема, статті 47 (2), 55 та 95 цієї Угоди,
пропозицію Комісії¹,
висновок Комітету з економічних та соціальних питань²,
та висновок Комітету у справах регіонів³,
діючи відповідно до процедури, визначеної в статті 251 Угоди⁴,
беручи до уваги, що:

16 квітня 1997 року Комісія представила Європейському Парламенту, Раді ЄС, Комітету з економічних та соціальних питань та Комітету у справах регіонів Повідомлення щодо забезпечення захисту та довіри при обміні інформацією в електронній формі — стосовно Європейської мережі цифрових підписів та шифрування;

8 жовтня 1997 року Комісія представила Європейському Парламенту, Раді ЄС, Комітету з економічних та соціальних питань та Комітету у справах регіонів Повідомлення щодо забезпечення захисту та довіри при обміні інформацією в електронній формі — стосовно Європейської мережі цифрових підписів та шифрування;

1 грудня 1997 року Рада ЄС звернулася до Комісії з проханням подати найближчим часом проект Директиви Європейського Парламенту та Ради ЄС щодо цифрових підписів;

Обмін інформацією в електронній формі та електронна торгівля актуалізують необхідність електронних підписів та пов'язаних з ними послуг, які уможливляють засвідчення автентичності даних; різні правила стосовно юридичної сили електронних підписів та акредитації провайдерів послуг із сертифікації в країнах-членах ЄС можуть становити значну перешкоду для використання обміну інформацією в електронній формі та електронної торгівлі; з іншого боку, чітка політика Співтовариства щодо вимог до електронних підписів посилює довіру та загальне визнання нових технологій; законодавство країн-членів ЄС не повинно створювати перешкоди для вільного руху товарів та послуг на внутрішньому ринку;

Сприяння має бути надано взаємодії продуктів із забезпечення електронних підписів; відповідно до статті 14 Угоди, внутрішній ринок є зо-

¹ ОІ С 325, 23.10.1998, ст. 5.

² ОІ С 40, 15.02.1999, ст. 29.

³ ОІ С 93, 6.04.1999, ст. 33.

⁴ Висновок Європейського Парламенту від 13 січня 1999 року (ОІ С 104, 14.04.1999, ст. 49), Спільна Позиція Ради від 28 червня 1999 року (ОІ С 243, 27.08.1999, ст. 33) та Рішення Європейського Парламенту від 27 жовтня 1999 (ше не опубліковане в Офіційному бюлетені). Рішення Ради від 30 листопада 1999 року.

Директива 99/93/ЄС Європейського парламенту та Ради ЄС про електронний...

ною, позбавленою внутрішніх кордонів, у межах якої забезпечується вільний рух товарів та послуг; вимоги, що стосуються продуктів із забезпечення електронних підписів, повинні виконуватися для того, щоб забезпечити вільний рух на внутрішньому ринку та завоювати довіру до електронних підписів, не порушуючи при цьому положень Постанови Ради (ЄС) № 3381/94 від 19 грудня 1994 року, що визначає режим ЄС щодо контролювання експорту товарів подвійного користування⁵ та Рішення Ради №94/942/CSFР від 19 грудня 1994 року стосовно спільних заходів, прийнятих Радою для контролювання експорту товарів подвійного використання⁶,

Ця Директива не гармонізує надання послуг з точки зору конфіденційності інформації там, де це визначається положеннями національного законодавства, що стосуються державної політики або державної безпеки;

Внутрішній ринок забезпечує вільний рух осіб, унаслідок чого громадяни та резиденти Європейського Союзу мають усе більшу потребу взаємодіяти з органами влади країн-членів ЄС, у яких вони не проживають; можливість обміну інформацією в електронній формі в цьому сенсі може бути дуже корисною.

Швидкий технологічний розвиток та глобальна природа Інтернету робить необхідним підхід, відкритий для різноманітних технологій та послуг, які здатні перевіряти автентичність даних електронними засобами;

Електронні підписи використовуватимуться за дуже різноманітних обставин та в різних програмах, це призведе до виникнення великого спектра нових послуг та продуктів, що пов'язані з електронними підписами або використовують їх; визначення таких продуктів та послуг не повинно обмежуватися видачею сертифікатів та управлінням ними, але також має охоплювати будь-які інші послуги або продукти, що використовують електронні підписи або є допоміжними для них, такі як послуги з реструкції, послуги з хронометричного штампування, довідкові та обчислювальні послуги або консультативні послуги, пов'язані з електронними підписами;

Внутрішній ринок надає провайдерам послуг із сертифікації можливість розвивати транскордонну діяльність з метою підвищити їхню конкурентоспроможність та завдяки цьому запропонувати споживачам та підприємствам нові можливості обміну інформацією та здійснення торгівлі в електронній формі у безпечний спосіб та незважаючи на кордони; для того щоб стимулювати надання послуг із сертифікації в усіх країнах Співтовариства через відкриті мережі, провайдери послуг із сертифікації повинні мати змогу вільно надавати послуги без необхідності попереднього отримання дозволу; попереднє отримання дозволу означає не лише будь-який дозвіл, який провайдер послуг має отримати за рішенням національних

⁵ ОІ L 367, 31.12.1994, ст.1. Постанова з внесеними поправками відповідно до Постанови (ЄС) № 837/95 (ОІ L 90, 21.04.1995, ст. 1).

⁶ ОІ L367, 31.12.1994, ст. 9. Рішення в останній редакції з внесеними поправками відповідно до Рішення 99/193/CSFР (ОІ L 73, 19.0.1999, ст. 1).

органів влади до того, як йому буде дозволено надавати ці послуги, а й будь-які інші подібні заходи;

Схеми добровільної акредитації, спрямовані на підвищення рівня надання послуг, можуть пропонувати провайдерам послуг із сертифікації належну структуру для подальшого розвитку їхніх послуг, спрямованого на досягнення такого рівня довіри, захищеності та якості, яких вимагає ринок, що розвивається; такі схеми мають сприяти розробці найкращої практики серед провайдерів послуг із сертифікації;

провайдери послуг із сертифікації повинні бути вільними у виборі та використанні акредитаційних схем;

Послуги з сертифікації можуть бути запропоновані будь-якою державною установою або юридичною чи фізичною особою, якщо вона створена відповідно до національного законодавства; оскільки країни-члени ЄС не повинні забороняти провайдерам послуг із сертифікації діяти поза межами добровільних схем акредитації, слід забезпечити, щоб акредитаційні схеми не стримували конкуренцію щодо надання послуг із сертифікації;

Країни-члени ЄС самі можуть приймати рішення щодо того, як вони забезпечуватимуть нагляд за виконанням положень, викладених у цій Директиві; ця Директива не чинить перешкоди створенню наглядових систем на базі приватного сектора; ця Директива не зобов'язує провайдерів послуг із сертифікації подавати заявку на проведення нагляду за їхньою діяльністю в рамках будь-якої існуючої схеми акредитації;

Важливо збалансувати потреби споживачів та підприємств;

Додаток III містить вимоги до захищених пристроїв для створення підписів з метою забезпечити функціональність електронних підписів у доєднаного типу; він не охоплює все системне середовище, у якому працюють такі пристрої; функціонування внутрішнього ринку вимагає від Комісії та країн-членів ЄС оперативних дій, спрямованих на створення органів, на які буде покладене проведення оцінки відповідності захищених пристроїв для створення підписів вимогам Додатку III; така оцінка відповідності має бути вчасною та продуктивною для того, щоб відповідати ринковим потребам;

Ця Директива сприяє ширшому використанню та юридичному визнанню електронних підписів у межах Співтовариства; електронні підписи, що використовуються виключно в межах систем, заснованих на добровільних угодах у рамках приватного права між визначеним числом учасників, не потребують нормативного забезпечення; свобода сторін домовлятися між собою щодо умов прийняття інформації, підписаної в електронній формі, повинна поважатися тією мірою, якою це дозволяє національне законодавство; має бути визнана юридична сила електронних підписів, що використовуються в таких системах, та їхня прийнятність як доказів при судовому розгляді;

Ця Директива не ставить на меті гармонізацію національних норм довірчого права, зокрема щодо формування та виконання контрактів або інших формальностей недовірчого характеру, що стосуються підписів; з цієї причини положення стосовно юридичної сили електронних підписів

не повинні призводити до порушення вимог національного законодавства стосовно форми укладення контрактів або правил, що визначають місце укладення контракту;

Збереження та копіювання даних щодо створення підписів може стати новити загрозу юридичній силі електронних підписів;

Електронні підписи будуть використовуватись у державному секторі в рамках національних органів управління та органів управління Співтовариства, а також при обміні інформацією між самими цими органами управління та між ними та громадськими або суб'єктами економічної діяльності, наприклад, у сфері державних закупівель, оподаткування, соціального забезпечення, системах охорони здоров'я та правосуддя;

Гармонізовані критерії юридичної сили електронних підписів сприятимуть збереженню узгодженої законодавчої бази в усіх країнах Співтовариства; національне законодавство встановлює різні вимоги щодо юридичної сили рукописних підписів; оскільки для підтвердження особи власника електронного підпису можуть використовуватися сертифікації; електронні підписи у доєднаного типу, що базуються на кваліфікованих сертифікатах, спрямовані на підвищення рівня захищеності; електронні підписи у доєднаного типу, які базуються на кваліфікованих сертифікатах та створені захищеним пристроєм для створення підписів, можуть вважатися юридично еквівалентними рукописним підписам лише за умови, якщо задовольняються вимоги до рукописних підписів;

З метою сприяння загальному визнанню електронних методів засвідчення автентичності необхідно забезпечити можливість використання електронних підписів як доказів при судовому розгляді у всіх країнах-членах ЄС; юридичне визнання електронних підписів повинно базуватися на об'єктивних критеріях і не повинно бути прив'язане до видачі дозволів провайдером послуг із сертифікації; сфери права, у яких можуть використовуватись електронні документи та електронні підписи, регулюються національним законодавством; ця Директива не порушує повноваження національного суду виносити рішення щодо виконання вимог цієї Директиви і не впливає на національні норми стосовно необмеженого судового розгляду доказів;

Діяльність провайдерів послуг із сертифікації, які надають послуги з сертифікації населенню, регулюється національними нормами щодо відповідальності;

Розвиток міжнародної торгівлі в електронній формі вимагає транскордонних домовленостей з участю третіх країн; з метою забезпечення глобальної взаємодії можуть бути корисними багатосторонні угоди, що визначають правила взаємодії з третіми країнами щодо взаємного визнання послуг із сертифікації;

З метою підвищення довіри користувачів до обміну інформацією в електронній формі та електронної торгівлі, провайдери послуг із сертифікації повинні діяти згідно із законодавством щодо захисту даних та конфідентційності приватної інформації;

Положення щодо використання псевдонімів у сертифікатах не повинні ставати на перешкоді країнам-членам ЄС вимагати встановлення особи відповідно до національного законодавства чи законодавства Співтовариства.

Заходи, необхідні для запровадження цієї Директиви, повинні бути прийняті відповідно до Рішення Ради 1999/468/ЄС від 28 червня 1999 року, що визначає процедури реалізації повноважень щодо запровадження, наданих Комісії⁷.

Через два роки після запровадження цієї директиви Комісія зробить її огляд, зокрема з метою гарантування того, що розвиток технологій або зміни у правовому середовищі не створили перешкод для досягнення цілей, поставлених у цій Директиві; цей огляд має дослідити наслідки запровадження цієї Директиви у споріднених технічних секторах та подати звіт про це до Європейського Парламенту та Ради.

Відповідно до принципів субсидіарності та пропорційності, визначених у статті 5 Угоди, мета створення гармонізованої законодавчої бази щодо надання електронних підписів та відповідних послуг найкращим чином може бути досягнута не на рівні окремих країн-членів Співтовариства, а на рівні Співтовариства в цілому; ця Директива не виходить за межі того, що є необхідним для досягнення цієї мети.

ПРИЙНЯЛИ ТАКУ ДИРЕКТИВУ:

Стаття 1. Сфера застосування

Метою цієї директиви є полегшення використання електронних підписів та сприяння їх юридичному визнанню. Ця Директива встановлює законодавчу базу для електронних підписів та певних послуг із сертифікації з метою забезпечення належного функціонування внутрішнього ринку.

Ця Директива не охоплює аспекти, пов'язані з укладенням та чинністю договорів або інших правових зобов'язань, що включають вимоги щодо форми, які регулюються національним законодавством або законодавством Співтовариства. Ця Директива також не впливає на правила та обмеження, що містяться в національному законодавстві або в законодавстві Співтовариства і регулюють використання документів.

Стаття 2. Визначення

Для цієї цієї Директиви:

«**електронний підпис**» означає дані в електронній формі, які додані до або логічно пов'язані з іншою електронною інформацією і є засобом перевірки автентичності;

«**електронний підпис удосконаленого типу**» означає електронний підпис, який відповідає таким вимогам:

- (а) однозначно пов'язаний з власником підпису;
- (б) дає можливість ідентифікувати власника підпису;
- (в) створений з використанням засобів, які власник підпису може тримати під своїм виключним контролем;

(г) пов'язаний з інформацією, якої він стосується таким чином, що будь-які зміни в цій інформації, внесені після внесення підпису, можуть бути виявлені;

«**власник підпису**» означає особу, що володіє пристроєм для створення підпису та діє або від свого імені, або від імені фізичної, або юридичної особи чи установи, представником якої вона виступає;

«**дані щодо створення підпису**» означають унікальні дані, такі як коди або приватні шифрувальні ключі, які використовують власник підпису для створення електронного підпису;

«**пристрій для створення підпису**» означає програмне забезпечення певної конфігурації або апаратний комплекс, що використовується для застосування даних щодо створення підпису;

«**закриплені пристрій для створення підпису**» означає пристрій для створення підпису, який відповідає вимогам, викладеним у Додатку III;

«**дані щодо верифікації підпису**» означають дані, такі, як коди чи державні шифрувальні ключі, які використовуються для верифікації електронного підпису;

«**пристрій для верифікації підпису**» означає програмне забезпечення певної конфігурації або апаратний комплекс, що використовується для застосування даних щодо верифікації підпису;

«**сертифікат**» означає електронне засвідчення, яке встановлює зв'язок між даними щодо верифікації підпису і власником підпису та підтверджує його особу;

«**кваліфіційний сертифікат**» означає сертифікат, що відповідає вимогам, встановленим у Додатку I, і виданий провайдером послуг із сертифікації, що задовольняє вимогам, визначеним у Додатку II;

«**провайдер послуг із сертифікації**» означає установу або юридичну чи фізичну особу, що видає сертифікати або надає інші послуги, пов'язані з електронними підписами;

«**послуг із забезпечення електронного підпису**» означає програмне забезпечення або апаратний комплекс, або їхні відповідні компоненти, які призначені для використання провайдером послуг із сертифікації для надання послуг, пов'язаних з електронними підписами, або для використання при створенні чи верифікації електронних підписів;

«**добровільна акредитація**» означає будь-який дозвіл, що визначає права та обов'язки, пов'язані з наданням послуг із сертифікації, який надається на прохання відповідного провайдера послуг із сертифікації державною або приватною установою, яка відповідає за визначення цих прав та обов'язків і здійснює нагляд за їх виконанням, при цьому провайдер послуг із сертифікації не може здійснювати права, що визначаються таким дозволом, до отримання рішення цього органу.

⁷ ОJ L 184, 17.07.1999, ст. 23.

Стаття 3. Доступ до ринку

Країни-члени ЄС не повинні вимагати попереднього отримання дозволу на надання послуг із сертифікації.

Не порушуючи положення параграфа 1, країни-члени ЄС можуть запроваджувати або підтримувати схеми добровільної акредитації, спрямовані на підвищення рівня надання послуг з акредитації. Всі умови, що стосуються таких схем, повинні бути об'єктивними, прозорими, пропорційними та недискримінаційними. Країни-члени ЄС не можуть обмежувати кількість акредитованих провайдерів послуг із сертифікації з причин, що підпадають під дію цієї Директиви.

Кожна країна-член ЄС повинна забезпечити створення відповідної системи для здійснення нагляду за діяльністю провайдерів послуг із сертифікації, що засновані на території цієї країни та здійснюють видачу кваліфікаційних сертифікатів населенню.

Відповідність захищених пристроїв для створення підпису вимогам, викладеним у Додатку III, повинна бути визначена відповідними державними та приватними органами, призначеними країнами-членами ЄС. Відповідно до процедури, встановленої в статті 9, Комісія має визначити для країн-членів ЄС критерії призначення таких органів.

Встановлення відповідності вимогам, що диктуються Додатком III, яке здійснюватиметься органами, про які йдеться у першому абзаці цього параграфа, повинно бути визнане всіма країнами-членами ЄС.

Відповідно до процедури, визначеної у статті 9, Комісія може визначити та опублікувати в Офіційному бюлетені Європейського Союзуваріанта кодові номери загальноприйнятих стандартів продуктів із забезпечення електронних підписів. Країни-члени ЄС повинні виходити з припущення, що коли продукт із забезпечення електронних підписів відповідає цим стандартам, то він задовольняє вимогам, викладеним у Додатку II, пункт (f) та Додатку III.

Країни-члени ЄС та Комісія мають спільно сприяти розробці та використання пристроїв для створення підписів у світлі рекомендацій щодо пристроїв для створення підписів, викладених у Додатку IV, та в інтересах споживачів.

Використання електронних підписів у державному секторі може регулюватися додатковими вимогами, встановленими країнами-членами ЄС. Такі вимоги повинні бути об'єктивними, прозорими, пропорційними та недискримінаційними і повинні стосуватися лише конкретних характеристик відповідних програм. Такі вимоги не повинні перешкоджати наданням транскордонних послуг промайданам.

Стаття 4. Принципи внутрішнього ринку

Кожна країна-член ЄС повинна застосовувати до провайдерів послуг із сертифікації, створених на її території, та до надаваних ними послуг положення національного законодавства, прийняті відповідно до цієї Директиви. Країни-члени ЄС не повинні обмежувати надання послуг зі створення електронних підписів, що походить з інших країн-членів ЄС, у сферах, на які поширюється дія цієї Директиви.

Країни-члени ЄС повинні забезпечити вільне розповсюдження продуктів із забезпечення електронних підписів, що відповідають вимогам цієї Директиви, на внутрішньому ринку.

Стаття 5. Юридична сила електронних підписів

Країни-члени ЄС повинні забезпечити, щоб електронні підписи удосконаленого типу, які мають кваліфікаційний сертифікат та створені за допомогою пристрою для створення електронних підписів:

(а) відповідали правовим вимогам до підпису, поставленого щодо даних в електронній формі, так само, як і рукописний підпис відповідає цим вимогам щодо даних на папері;

(б) були дозволені для використання як докази при судовому розгляді.

Країни-члени ЄС повинні забезпечити, щоб електронні підписи не були позбавлені юридичної сили та визнання як докази при судовому розгляді лише на тій підставі, що вони:

мають електронну форму; або

не засновані на кваліфікаційному сертифікаті; або

не засновані на кваліфікаційному сертифікаті, виданому акредитованим провайдером послуг із сертифікації; або

не створені за допомогою захищеного пристрою для створення електронних підписів.

Стаття 6. Відповідальність

Країни-члени ЄС повинні забезпечити, як мінімум, що завдяки видачі кваліфікаційних сертифікатів населенню або завдяки гарантуванню таких сертифікатів, виданих населенню, провайдери послуг із сертифікації нести-муть відповідальність за шкоду, заподіяну будь-якій установі або юридичній чи фізичній особі, яка об'єднано покладається на такий сертифікат:

(а) стосовно забезпечення під час видані сертифіката точності всієї інформації, що міститься у кваліфікаційному сертифікаті, а також стосовно того факту, що сертифікат містить усі деталі, передбачені для кваліфікаційного сертифіката;

(б) стосовно забезпечення того, що на момент видачі сертифіката власник підпису, вказаний у кваліфікаційному сертифікаті, володів даними щодо створення підпису, які відповідають даним щодо верифікації підпису, наданим або вказаним у сертифікаті;

(в) стосовно забезпечення того, що дані для створення підпису та дані для верифікації підпису можуть доповнювати одне одного у тих випадках, коли провайдер послуг із сертифікації створює їх обох;

окрім випадків, коли провайдер послуг із сертифікації доведе, що його дії не були недбалими.

Країни-члени ЄС повинні забезпечити, як мінімум, що провайдер послуг із сертифікації, який видав кваліфікаційні сертифікати населенню, нестиме відповідальність за шкоду, завдану будь-якій установі або юридичній чи фізичній особі, яка об'єднано покладається на такий сертифікат, у разі неможливості зареєструвати ануляцію сертифіката, окрім

випадків, коли провайдер послуг із сертифікації доведе, що його дії не були небезпечними.

Країни-члени ЄС повинні забезпечити для провайдера послуг із сертифікації можливість вказувати у кваліфікаційному сертифікаті обмеження щодо застосування цього сертифіката, за умови, що ці обмеження визначаються третіми сторонами. Провайдер послуг із сертифікації не несе відповідальності за шкоду, завдану в результаті використання кваліфікаційного сертифіката з перевищенням зазначених у ньому обмежень.

Країни-члени ЄС повинні забезпечити для провайдера послуг із сертифікації можливість вказувати у кваліфікаційному сертифікаті обмеження щодо вартості операцій, для яких використовуватиметься цей сертифікат, за умови, що це обмеження визнається третіми сторонами.

Провайдер послуг із сертифікації не несе відповідальності за збитки, що виникли в результаті перевищення цього обмеження.

Положення параграфів 1–4 не повинні призводити до порушення положень Директиви Ради ЄС 93/13/ЕЕС від 5 квітня 1993 року щодо несправедливих умов в угодах зі споживачами⁸.

Стаття 7. Міжнародні аспекти

Країни-члени ЄС мають забезпечити визнання кваліфікаційних сертифікатів, виданих населенню провайдерами послуг із сертифікації, створеними на території третіх країн, як юридично еквівалентних сертифікатів, виданим провайдерами послуг із сертифікації, створеним на території Співтовариства, за умови, що:

(а) провайдер послуг із сертифікації виконує вимоги, встановлені цією Директивою, і акредитований відповідно до добровільної акредитаційної схеми, запровадженій у країні-члені ЄС; або

(б) провайдер послуг із сертифікації, створений на території Співтовариства, який відповідає вимогам, встановленим цією Директивою, дає гарантію на сертифікат; або

(в) сертифікат або провайдер послуг із сертифікації визнається відповідно до двосторонньої або багатосторонньої угоди між Співтовариством та третіми країнами або міжнародними організаціями.

З метою сприяння наданню трансграничних послуг із сертифікації третіми країнами та юридичному визнанню електронних підписів удосконаленого типу, що походять із третіх країн, Комісія повинна, де необхідно, розробити пропозиції щодо забезпечення ефективного запровадження стандартів та міжнародних угод, що застосовуються до послуг із сертифікації. Зокрема, там, де необхідно, Комісія повинна подавати пропозиції до Ради ЄС стосовно відповідних повноважень на проведення переговорів щодо двосторонніх та багатосторонніх угод з третіми країнами та міжнародними організаціями. Рада приймає рішення кваліфікованою більшістю голосів.

⁸ ОJ L 95, 21.04.1993, ст. 29.

У будь-який час, коли Комісія отримує інформацію щодо труднощів, з якими стикається Співтовариство у своїй діяльності, пов'язаній з доступом до ринку у третіх країнах, вона може, у разі необхідності, подавати пропозиції до Ради стосовно відповідних повноважень на проведення переговорів щодо порівнянних прав для Співтовариства на ведення діяльності в цих третіх країнах. Рада приймає рішення кваліфікованою більшістю голосів.

Заходи, вжиті відповідно до цього параграфа, не повинні призводити до порушення зобов'язань Співтовариства та країн-членів ЄС в рамках відповідних міжнародних угод.

Стаття 8. Захист даних

Країни-члени ЄС мають забезпечити виконання провайдерами послуг із сертифікації та національними органами, відповідальними за акредитацію або нагляд за виконанням вимог, встановлених у Директиві Європейського Парламенту та Ради ЄС 95/46/ЄС від 24 жовтня 1995 року щодо захисту процесу обробки особистих даних громадян від несанкціонованого доступу та щодо вільного руху таких даних⁹.

Країни-члени ЄС мають забезпечити для провайдера послуг із сертифікації, що видає сертифікати населенню, можливість отримати особисті дані лише безпосередньо від суб'єкта цих даних або після отримання його чітко вираженого дозволу, і тільки якщо це необхідно для цілей видачі та утримання сертифікату. Дані не можуть бути отримані або оброблені для будь-яких інших цілей без чітко вираженого дозволу суб'єкта даних.

Країни-члени ЄС не повинні перешкоджати провайдерам послуг із сертифікації вказувати у сертифікаті псевдонім замість справжнього імені власника підпису; це не повинно призводити до порушення юридичної сили, що надається псевдонімам національним законодавством.

Стаття 9. Комітет

Комісія отримуватиме допомогу від «Комітету у справах електронних підписів» (надалі — «Комітет»).

При посиланні на цей параграф будуть застосовуватися статті 4 та 7 Рішення 1999/468/ЄС, враховуючи положення статті 8 цього Рішення. Період, передбачений у статті 4 (3) Рішення 1999/468/ЄС, повинен дорівнювати трьом місяцям.

Комітет повинен прийняти власні процедурні правила.

Стаття 10. Завдання Комітету

Комітет повинен дати роз'яснення щодо вимог, викладених у Додатках до цієї Директиви, критеріїв, про які йдеться у статті 3 (4), та загальноприйнятих стандартів продуктів із забезпечення електронних підписів, які встановлені та опубліковані відповідно до статті 3 (5) згідно з процедурою, визначеною у статті 9 (2).

⁹ ОJ L 281, 23.11.1995, ст. 31.

Стаття 11. Повідомлення

Країни-члени ЄС повинні сповіщати Комісію та інші країни-члени ЄС про такі дані:

- (а) інформація щодо національних добровільних акредитаційних схем, у тому числі про будь-які додаткові вимоги відповідно до статті 3 (7);
- (б) назви та адреси національних органів, відповідальних за здійснення акредитації та надляду, а також органів, про які йдеться у статті 3 (4);
- (в) назви та адреси всіх національних акредитованих провайдерів послуг із сертифікації.

2. Будь-яка інформація, подана відповідно до параграфа 1, та зміни в ній мають бути повідомлені країнами-членами ЄС у найкоротший термін.

Стаття 12. Огляд

Комісія повинна зробити огляд дії цієї Директиви та звітувати про це перед Європейським Парламентом та Радою не пізніше 19 червня 2003 року.

Зокрема, огляд повинен передбачати проведення оцінки того, чи потребує змін сфера застосування цієї Директиви, враховуючи розвиток у технологій, ринковій та правовій сферах. Звіт повинен містити, зокрема, оцінку аспектів гармонізації, зроблену на основі наявного досвіду. Де необхідно, звіт має супроводжуватися законодавчими пропозиціями.

Стаття 13. Запровадження

Країни-члени ЄС мають ввести в дію закони, нормативні та адміністративні акти, необхідні для виконання цієї Директиви, до 19 липня 2001 року. Вони повинні негайно сповістити про це Комісію.

При прийнятті країнами-членами ЄС таких законів, нормативних та адміністративних актів вони повинні містити посилання на цю Директиву або супроводжуватися таким посиланням при їх офіційному опублікуванні. Способи такого посилання мають бути визначені країнами-членами ЄС. Країни-члени ЄС мають передати Комісії текст основних положень національного права, які будуть прийняті ними у сфері, що регулюється цією Директивою.

Стаття 14. Набуття чинності

Ця Директива набуває чинності в день її опублікування в Офіційному бюлетені Європейського Співтовариства.

Стаття 15. Адресати

Ця Директива адресована всім країнам-членам ЄС.

Укладено в Брюсселі 13 грудня 1999 року.

Європейський Парламент, Президент Н. ФОНТЕЙН
Рада ЄС, Президент С. ХЕССІ

Додаток І

ВИМОГИ ДО КВАЛІФІКАЦІЙНИХ СЕРТИФІКАТІВ

Кваліфікаційні сертифікати повинні містити:

- (а) зазначення того, що цей сертифікат виданий як кваліфікаційний сертифікат;
- (б) визначення провайдера послуг із сертифікації та країни-члена ЄС, на території якої він створений;
- (в) ім'я власника підпису або псевдонім, який повинен бути визначений як такий;
- (г) якщо необхідно, надання власникові підпису спеціального атрибуту, залежно від цілей сертифікату;
- (д) дані щодо верифікації підпису, які відповідають даним щодо створення підпису, що перебувають під контролем власника підпису;
- (е) зазначення початкового та кінцевого терміну дії сертифіката;
- (є) ідентифікаційний код сертифіката;
- (ж) електронний підпис удоконаленого типу, що належить провайдеру послуг із сертифікації, який видав сертифікат;
- (з) у разі потреби, обмеження щодо сфери застосування сертифіката;
- (и) , обмеження щодо вартості операцій, для яких може використовуватися цей сертифікат.

Додаток ІІ

ВИМОГИ ДО ПРОВАЙДЕРІВ ПОСЛУГ ІЗ СЕРТИФІКАЦІЇ, ЩО ВИДАЮТЬ КВАЛІФІКАЦІЙНІ СЕРТИФІКАТИ

Провайдери послуг із сертифікації повинні:

- (а) продемонструвати надійність, необхідну для надання послуг із сертифікації;
- (б) забезпечити функціонування швидкодіючого та захищеного вказівника й захищеної та нетайної послуги з анулювання сертифікатів;
- (в) забезпечити точне визначення дня та часу видачі або анулювання сертифіката;
- (г) перевірити, вдаючись до належних засобів відповідно до національного законодавства, особу власника кваліфікаційного сертифіката та, якщо необхідно, його будь-які особливі атрибути;
- (д) наймати працівників, які володіють експертним знанням, досвідом та кваліфікацією, необхідними для надання таких послуг, зокрема, компетентністю на управлінському рівні, знаннями в галузі технологій електронних підписів, а також озброєні належними процедурами захисту; вони повинні також застосовувати адекватні адміністративні та управлінські процедури, що відповідають прийнятим стандартам;
- (е) використовувати надійні системи та продукти, які захищені проти модифікацій, і забезпечити технічну та шифрувальну захищеність процесу, що ними підтримується;

(є) вжити заходів проти підробки сертифікатів, а також у випадках, коли провайдер послуг із сертифікації створює дані щодо створення підпису, гарантувати конфіденційність упродовж усього процесу створення таких даних;

(ж) підтримувати достатні фінансові ресурси для того, щоб вести діяльність відповідно до вимог, визначених у Директиві, зокрема нести ризик відповідальності за завдану шкоду, наприклад шляхом придбання відповідного страхового полісу;

(з) записувати всю необхідну інформацію стосовно кваліфікаційних сертифікатів протягом належного періоду часу, зокрема для цілей представлення доказів при судовому розгляді. Такий запис може здійснюватися в електронній формі;

(и) не зберігати і не копіювати дані щодо створення підпису, що належать особі, якій провайдер послуг із сертифікації надавав основні послуги з менеджменту;

(і) перед вступом у договірні стосунки з особою, яка бажає мати сертифікат для підтримання її електронного підпису, поінформувати цю особу за допомогою надійних засобів комунікації про точні умови використання сертифіката, включаючи будь-які обмеження в його застосуванні, існування добровільних акредитаційних схем та процедур розгляду скарг та вирішення спорів. Така інформація, що може передаватися в електронному вигляді, повинна бути письмовою та викладеною легко зрозумілою мовою. Відповідні частини цієї інформації повинні також надаватися на прохання третіх сторін, що покладаються на сертифікат;

(к) використовувати надійні системи для зберігання сертифікатів у формі, яка може бути перевірена таким чином, що:

тільки уповноважені особи можуть вносити дані та зміни до них, інформація може бути перевірена на автентичність, сертифікати можуть бути відкритими для публічного пошуку лише в тих випадках, коли на це дав згоду власник сертифіката,

будь-які технічні зміни, що порушують ці вимоги щодо захисту, будуть помітними для оператора.

Додаток III ВИМОГИ ДО ЗАХИЩЕНИХ ПРИСТРОЇВ ДЛЯ СТВОРЕННЯ ПІДПИСІВ

Захищені пристрої для створення підписів повинні за допомогою технологічних та процедурних засобів забезпечити щонайменше таке:

(а) дані щодо створення підпису, які використовуються для поставлення підпису, можуть з'явитися практично лише один раз, і що секретність цих даних забезпечена належною мірою;

(б) дані щодо створення підпису, що використовуються для поставлення підпису, з достатньою певністю не можуть бути здобуті повторно, а підпис є захищеним від підробки з використанням сучасної технології;

(в) дані щодо створення підпису, що використовуються для поставлення підпису, можуть бути надійно захищені законним власником підпису від використання іншими особами.

Захищені пристрої для створення підписів не повинні змінювати дані, які вимагають підпису, або перешкоджати представленню цих даних власникові підпису до процесу поставлення підпису.

Додаток IV РЕКОМЕНДАЦІЇ ЩОДО ЗАХИЩЕНОЇ ВЕРИФІКАЦІЇ ПІДПИСІВ

У процесі верифікації підписів з достатньою надійністю має бути забезпечене таке:

(а) дані, що використовуються для верифікації підпису, відповідають даним, що відображені на екрані монітора для особи, що здійснює верифікацію;

(б) підпис надійно перевіряється, і результат цієї верифікації правильно відображається;

(в) особа, що здійснює верифікацію підпису, може, якщо необхідно, надійно встановити зміст підписаних даних;

(г) справжність та дійсність сертифіката, що вимагається на момент верифікації підпису, надійно перевіряються;

(д) результати верифікації та встановлення особи власника підпису правильно відображаються;

(є) використання псевдоніма чітко зазначається;

(є) будь-які зміни, що стосуються захищеності, можуть бути виявлені.

**ДЕКЛАРАЦІЯ ПРИНЦИПІВ.
ПОБУДОВА ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА —
ГЛОБАЛЬНЕ ЗАВДАННЯ НОВОГО ТИСЯЧОЛІТТЯ**
Документ WSIS-03/GENEVA/DOC/4-R

*(Прийнято на Всесвітній зустрічі на вищому рівні
з питань інформаційного суспільства. Женева, 12 грудня 2003)*

А. Наша загальна концепція інформаційного суспільства

1. Ми, представники народів світу, ті, що зібралися в Женеві 10—12 грудня 2003 року для проведення першого етапу Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства, заявляємо про наше загальне прання і рішучість побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, у якому кожний міг би створювати інформацію і знання, мати до них доступ, користатися й обмінюватися ними, щоб дати окремим особам, громадам і народам можливість повною мірою реалізувати свій потенціал, сприяючи своєму стійкому розвитку і підвищуючи якість свого життя на основі цілей і принципів Статуту Організації Об'єднаних Націй і дотримуючи в повному обсязі та підтримуючи Загальну декларацію прав людини.

2. Наше завдання полягає в тому, щоб використовувати потенціал інформаційних і комунікаційних технологій для досягнення сформульованих у Декларації тисячоріччя цілей розвитку, а саме ліквідації крайньої бідності і голоду, забезпечення загальної початкової освіти, сприяння рівності чоловіків та жінок і розширенню прав і можливостей жінок, скорочення дитячої смертності, поліпшення охорони материнства, боротьби з ВІЛ /СНІДом, малярією та іншими захворюваннями, сприяння екологічній стійкості і формування глобального партнерства з метою розвитку для забезпечення більш мирного, справедливого і процвітаючого світу. Ми також підтверджуємо свою прихильність до досягнення сталою розвитку і угоджених цілей розвитку, викладених у Йоганнесбурзькій декларації і Плані виконання рішень та Монтеррейському консенсусі, а також в інших документах відповідних зустрічей на вищому рівні в рамках Організації Об'єднаних Націй.

3. Ми знову підтверджуємо універсальність, неподільність, взаємозалежність і взаємозв'язок усіх прав людини і основних свобод, включаючи право на розвиток, як це закріплено у Віденській декларації. Ми знову підтверджуємо також, що демократія, сталій розвиток і дотримання прав людини й основних свобод, а також належне державне керування на всіх рівнях є взаємозалежними і взаємозміцнюючим. Ми далі вирішуємо зміцнювати повагу верховенства права в галузі зовнішньої і внутрішньої політики.

4. Ми знову підтверджуємо, що ми визнаємо як необхідний фундамент інформаційного суспільства проголошене в статті 19 Загальної декларації

Декларація принципів. Побудова інформаційного суспільства — глобальне...

прав людини право кожної людини на свободу переконань і на вільне їх вираження; це право включає свободу безперешкодно дотримуватись своїх переконань і вольно шукати, одержувати і розповсюджувати інформацію та ідеї будь-якими засобами незалежно від державних кордонів. Сплікування є однією з основних соціальних процесів, однією з базових людських потреб і фундаментом будь-якої соціальної організації. Воно складає серцевину інформаційного суспільства. Кожний, де б він не перебував, повинний мати можливість брати участь в інформаційному суспільстві, і нікого не можна позбавити пропонованих цим суспільством переваг.

5. Ми знову підтверджуємо свою прихильність до положень статті 29 Загальної декларації прав людини, згідно з якими кожна людина має обов'язки перед суспільством, у якому тільки й можливий вільний і повний розвиток його особистості, і при здійсненні своїх прав і свобод кожна людина має підпадати тільки під такі обмеження, які встановлені законом виключно з метою забезпечити належне визнання та повагу прав і свобод інших та задоволення справедливих вимог моралі, суспільного порядку і загальної доброти в демократичному суспільстві. Здійснення таких прав і свобод ні в жодному разі не повинне вступати в суперечність із цілями і принципами Організації Об'єднаних Націй. Тим самим ми будемо сприяти створенню інформаційного суспільства, у якому поважатиметься достоїнство людської особистості.

6. Відповідно до духу даної Декларації ми знову заявляємо про свою рішучість дотримуватися принципу суверенної рівності всіх держав.

7. Ми усвідомлюємо, що наука відіграє центральну роль у розвитку інформаційного суспільства. Багато компонентів інформаційного суспільства є результатом науково-технічних досягнень, що стали можливими завдяки спільному використанню результатів досліджень.

8. Ми усвідомлюємо, що освіта, знання, інформація і спількування складають основу розвитку, ініціативності і благополуччя людської особистості. Поряд з цим інформаційні і комунікаційні технології (ІКТ) впливають практично на всі аспекти нашого життя. Стрімкий прогрес цих технологій відкриває зовсім нові перспективи досягнення більш високих рівнів розвитку. Здатність цих технологій послабити вплив багатьох традиційних перешкод, особливо пов'язаних із часом та відстанню, уперше в історії дає змогу використовувати потенціал цих технологій на благо мільйонів людей у всіх кутках земної кулі.

9. Ми усвідомлюємо, що ІКТ варто розглядати як інструмент, а не як ціль. За сприятливих умов ці технології здатні стати могутнім інструментом підвищення продуктивності, економічного росту, створення нових робочих місць і розширення можливостей працевлаштування, а також підвищення якості життя для всіх. Вони також можуть сприяти веденню діалогу між народами, країнами і цивілізаціями.

10. Ми також повністю усвідомлюємо, що сьогодні переважає революція в галузі інформаційних технологій нерівномірно розподілені між розвинутими країнами і такими, що розвиваються, а також усереднені країни. Ми повні рішучості перетворити цей розрив у цифрових технологіях на циф-

рові можливості для всіх, насамперед для тих, кому запрокує відставання і подальша маргіналізація.

11. Ми підтримуємо ідею перетворити в життя нашу загальну концепцію інформаційного суспільства на благо нинішнього і майбутнього поколінь. Ми усвідомлюємо, що молодь є майбутнім трудовим ресурсом, вона відіграє провідну роль у створенні ІКТ і швидше за інших освоює ці технології. Тому варто надати їй можливість учитися і брати участь у прийнятті рішень. Особливу увагу ми повинні приділяти тим молодим людям, які поки не мають можливості повною мірою користатися перевагами, що надаються ІКТ. Ми також визнаємо за необхідне забезпечити дотримання прав дитини, зокрема щодо захисту дітей та їхнього благополуччя при розробці додатків і наданні послуг на базі ІКТ.

12. Ми підтверджуємо, що розвиток ІКТ відкриває грандіозні перспективи для жінок, які повинні скласти невід'ємну частину інформаційного суспільства і стати його ключовими учасниками. Ми визнаємо необхідним забезпечити, щоб в інформаційному суспільстві жінкам надавалися всі права і можливості і щоб вони повною мірою брали участь на рівних правах у всіх сферах життя суспільства і в усіх процесах прийняття рішень. Для цього ми повинні включити в основні напрямки нашої діяльності принцип рівноправності жінок і чоловіків і застосовувати ІКТ як інструмент для досягнення цієї мети.

13. При побудові інформаційного суспільства ми повинні приділяти першорядну увагу особливим потребам маргіналізованих і вразливих груп суспільства, у тому числі емігрантів, внутрішньо переміщених осіб і біженців, безробітних і знедолених людей, меншин і кочових народів. Ми повинні також враховувати особливі потреби пристарілих та осіб з обмеженими можливостями.

14. Ми сповнені рішучості розширити можливості незаможних, насамперед тих, які проживають у віддалених, сільських і маргіналізованих міських районах, стосовно доступу до інформації і використання ІКТ як інструменту, що допомагає їм у їхніх зусиллях позбутися злиднів.

15. При становленні інформаційного суспільства увагу насамперед слід приділяти особливому становищу корінних народів, а також збереженню їхньої спадщини і культурного надбання.

16. Ми продовжуємо приділяти особливу увагу специфічним потребам жителів країн, що розвиваються, країн з перехідною економікою, найменш розвинутих країн, малих острівних держав, та країн, які не мають виходу до моря, що розвиваються, бідних країн із великою заборгованістю, окупованих країн і територій, країн, що долають наслідки конфліктів, а також країн і регіонів з особливими потребами, зокрема з обставинами які створюють серйозну загрозу для розвитку, у тому числі стихійні лиха.

17. Ми усвідомлюємо, що для створення відкритого для всіх інформаційного суспільства вимагаються нові форми солідарності, партнерства та співробітництва між органами державного управління та іншими зацікавленими сторонами, тобто приватним сектором, громадянським суспіль-

ством і міжнародними організаціями. Усвідомлюючи, що поставлене в цій Декларації масштабне завдання — подолати розрив у цифрових технологіях і забезпечити гармонійний, справедливий і рівноправний розвиток для всіх — вимагає твердої рішучості всіх зацікавлених сторін, ми закликаємо до цифрової солідарності як на національному, так і на міжнародному рівнях.

18. Ніщо в даній Декларації не повинне тлумачитись як зазіхання на положення Статуту Організації Об'єднаних Націй, Загальної декларації прав людини, будь-які інші міжнародні документи чи національне законодавство, прийняті на підтримку цих документів, як таке, що суперечить, обмежує чи відступає від них.

В. Інформаційне суспільство для всіх: основні принципи

19. Ми сповнені рішучості, будуючи інформаційне суспільство, забезпечити, щоб кожний міг скористатися можливостями, які можуть надати ІКТ. Ми згодні в тим, що для вирішення цих завдань усі зацікавлені сторони повинні працювати спільно над розширенням доступу до інформаційних і комунікаційних інфраструктур і технологій, а також до інформації і знань, нарощувати потенціал, підвищувати довіру і безпеку при використанні ІКТ, створювати на всіх рівнях сприятливе середовище, розробляти додатки ІКТ і розширювати сферу їх застосування, сприяти культурній розмаїтості і поважати її, визнавати роль засобів масової інформації, приділяти увагу етичним аспектам інформаційного суспільства і заохочувати міжнародне і регіональне співробітництво. Ми згодні з тим, що це — ключові принципи побудови відкритого для всіх інформаційного суспільства.

1) Роль органів державного управління і всіх зацікавлених сторін у сприянні застосуванню ІКТ із метою розвитку

20. Органам державного управління, а також приватному секторові, громадянському суспільству, Організації Об'єднаних Націй та іншим міжнародним організаціям слід відіграти важливу роль у розвитку інформаційного суспільства, взяти за це на себе відповідальність, а також у певних випадках брати участь у процесах прийняття рішень. Побудова інформаційного суспільства, орієнтованого на інтереси людей, є загальною справою, що вимагає співробітництва та партнерських відносин між усіма зацікавленими сторонами.

2) Інформаційна і комунікаційна інфраструктура — необхідний фундамент відкритого для всіх інформаційного суспільства

21. Забезпечення підключення є одним із головних чинників побудови інформаційного суспільства. Надання універсального, розповсюдженого, справедливого і прийнятного щодо ціни доступу до інфраструктури ІКТ і послуг на базі ІКТ є одним із завдань інформаційного суспільства і має

стати метою всіх зацікавлених сторін, що беруть участь у його розбудові. Забезпечення підключення також передбачає доступ до послуг енергопостачання і поштового зв'язку, яким слід забезпечувати відповідно до національного законодавства кожної країни.

22. Добре розвинута інфраструктура інформаційних і комунікаційних мереж і додатків, що відповідають регіональним, національним і місцевим умовам, легкодоступні і прийнятні в ціновому плані, що дозволяють більшою мірою використовувати широкосмуговий зв'язок та інші інноваційні технології там, де це можливо, здатна прискорити соціально-економічний прогрес країн і підвищити добробут усіх людей, громад і народів.

23. Політика, що створює на всіх рівнях сприятливі умови для стабільності, передбачуваності і сумлінної конкуренції, повинна розроблятися і здійснюватися так, щоб не тільки у великих масштабах залучати приватні інвестиції в розвиток інфраструктури ІКТ, а й забезпечувати виконання зобов'язань з універсального обслуговування в тих секторах, де не діють традиційні ринкові механізми. У районах, що знаходяться в несприятливих умовах, створення публічних пунктів доступу до ІКТ у таких структурах, як поштові відділення, школи, бібліотеки й архіви, може слугувати ефективним способом забезпечення універсального доступу до інфраструктури і послуг інформаційного суспільства.

3) Доступ до інформації і знань

24. Забезпечення кожному можливості мати доступ до інформації, ідеї і знань та робити в цій галузі свій внесок є необхідним елементом відкритого для всіх інформаційного суспільства.

25. Спільному використанню і розширенню глобальних знань з метою розвитку може сприяти усунення бар'єрів на шляху досягнення рівного правого доступу до інформації для здійснення діяльності в галузі економіки, у соціальній сфері, політиці, охороні здоров'я, культурі, освіті та науці, а також спрощенню доступу до інформації, що є публічним надбанням, у тому числі шляхом забезпечення універсального дизайну і використання асистивних технологій.

26. Наявність великого публічного надбання — найважливіший складник розвитку інформаційного суспільства, що забезпечує такі численні переваги, як одержання населенням освіти, створення нових робочих місць, інноваційна діяльність, відкриття перспектив у господарській сфері і науковий прогрес. Інформація, що відноситься до публічного надбання, має бути легкодоступною в інтересах розвитку інформаційного суспільства і захищеною від незаконного присвоєння. Варто зміцнювати публічні установи, такі як бібліотеки й архіви, музеї, збирання культурних цінностей та інші колективні пункти доступу, для того щоб сприяти збереженню документальних записів і вільному та рівноправному доступу до інформації.

27. Доступу до інформації і знань можна сприяти шляхом підвищення поінформованості всіх зацікавлених сторін про можливості, надані різними

ми моделями програмного забезпечення, у тому числі розробленими окремими компаніями, програмного забезпечення відкритими кодами і вільно розповсюджуваного програмного забезпечення, для того щоб підсилювати конкуренцію, розширювати доступ до них користувачам і діапазон їхнього вибору, а також дати всім користувачам можливість вирішувати, який саме варіант краще задовольняє їхні потреби. Прийнятний у ціновому плані доступ до програмного забезпечення є важливим компонентом справді відкритого для всіх інформаційного суспільства.

28. Ми прагнемо сприяти забезпеченню загальному і рівноправному універсального доступу до наукових знань, створення і поширення наукової інформації, включаючи ініціативи з організації вільного доступу до наукових публікацій.

4) Нарощування потенціалу

29. Кожна людина повинна мати можливість оволодіти навичками і знаннями, необхідними для розуміння суті інформаційного суспільства та економіки, що базується на знаннях, брати активну участь у них і повномасштабно використовувати їхні переваги. Грамотність і загальна початкова освіта є ключовими факторами при побудові відкритого для всіх без винятку інформаційного суспільства, при цьому першорядна увага має приділятися особливим потребам дівчат і жінок. З урахуванням потреби на всіх рівнях для значної кількості фахівців в області ІКТ та інформатики особливої уваги заслуговує нарощування інституціонального потенціалу.

30. Необхідно сприяти застосуванню ІКТ на всіх рівнях освіти, професійної підготовки і розвитку людських ресурсів із врахуванням особливих потреб осіб з обмеженими можливостями, а також таких, які перебувають у несприятливих умовах, і вразливих груп населення.

31. Безперервна освіта та освіта для дорослих, передпідготовка, навчання протягом усього життя та дистанційне навчання та інші спеціальні послуги, такі як телемедицина, можуть зробити вирішальний внесок у розширення можливостей працевлаштування та сприятимуть людям при використанні ними нових перспектив, що відкриваються ІКТ щодо традиційних робочих місць, самозайнятості та освоєння нових професій. Необхідним фундаментом для цього є інформованість та грамотність у галузі ІКТ.

32. Активну роль у формуванні інформаційного суспільства повинні відіграти розробники, видавці і виробники контенту, а також викладачі, інструктори, працівники архівів і бібліотек та учні, особливо в найменш розвинутих країнах.

33. Для забезпечення сталого розвитку інформаційного суспільства варто нарощувати національний потенціал у галузі науково-технічних і дослідно-конструкторських робіт у сфері ІКТ. Поряд з цим партнерські відносини, передусім між розвинутими країнами і країнами, що розвиваються, та всередині груп цих країн, включаючи країни з перехідною економікою, у галузі науково-технічних і дослідницько-конструкторсь-

ких робіт, передачі технологій, виробництва і використання продуктів і послуг на базі ІКТ, є найважливішою умовою сприяння нарощуванню потенціалу і загальній участі в інформаційному суспільстві. Виробництво продукції ІКТ відкриває широкі перспективи для створення матеріального благ.

34. Реалізація наших загальних прагнень, насамперед до того, щоб країни, що розвиваються, і країни з перехідною економікою стали повноправними членами інформаційного суспільства, і позитивний процес їхньої інтеграції в економіку, що базується на знаннях, багато в чому залежать від прискорення нарощування потенціалу в галузі освіти, технологій, наука і доступу до інформації. Ці чинники є вирішальними у визначенні рівня розвитку і конкурентоспроможності.

5) Зміцнення довіри і безпеки при використанні ІКТ

35. Зміцнення основи для довіри, включаючи інформаційну безпеку і безпеку мереж, автентифікацію, захист недоторканності приватного життя і прав споживачів, є передумовою становлення інформаційного суспільства і росту довіри з боку користувачів ІКТ. Необхідно формувати, розвивати і впроваджувати глобальну культуру кібербезпеки в співробітництві з усіма зацікавленими сторонами і компетентними міжнародними організаціями. Дані зусилля повинні спиратися на міжнародне співробітництво, що розширюється. У рамках цієї глобальної культури кібербезпеки важливо підвищувати безпеку і забезпечувати захист даних і недоторканність приватного життя, розширюючи при цьому доступ і масштаб торгових операцій. Крім того, необхідно враховувати рівень соціально-економічного розвитку кожної країни і пов'язані з орієнтацією на розвиток аспекти інформаційного суспільства.

36. Визнаючи принципи універсального і недискримінаційного доступу до ІКТ для всіх країн, ми підтримуємо діяльність Організації Об'єднаних Націй, спрямовану на запобігання можливості використання ІКТ з метою, яка несумісна із завданням забезпечення міжнародної стабільності і безпеки та здатна здійснювати негативний вплив на цілісність державних інфраструктур, завдаючи шкоди їхній безпеці. Варто запобігати використанню інформаційних ресурсів і технологій у злочинних і терористичних цілях, дотримуючись при цьому прав людини.

37. Спам представляє для користувачів, мереж і в цілому для Інтернету серйозну проблему, масштаби якої зростають. Питання, що стосуються спаму і кібербезпеки, варто розглядати на відповідному національному і міжнародному рівнях.

6) Сприятливе середовище

38. Необхідною умовою існування інформаційного суспільства є сприятливе середовище на національному і міжнародному рівнях. ІКТ варто застосовувати, як важливий інструмент належного державного керування.

39. Верховенство права, поряд зі сприятливим, прозорим, сприятливим для конкуренції, заснованим на принципі технологічної нейтральності і передбачуваною політичною і регламентною базою, що враховує національні особливості, необхідне для створення орієнтованого на інтереси людей інформаційного суспільства. Органи державного управління повинні вживати в нагальних випадках заходів для компенсації несприятливості ринкових механізмів, підтримки добросовісної конкуренції, залучення інвестицій, сприяння розвитку інфраструктури ІКТ і додатків на базі ІКТ, максимального використання економічних і соціальних вигод з урахуванням національних пріоритетів.

40. Життєво важливими додатковими компонентами, які стосуються ІКТ, національних зусиль у сфері розвитку є динамічне і сприятливе міжнародне середовище, що сприяє залученню прямих іноземних інвестицій, передачі технологій і міжнародному співробітництву, у першу чергу в галузях фінансів, заборгованості і торгівлі, а також повномасштабна й ефективна участь країн, що розвиваються, у прийнятті рішень на світовому рівні. Розширення прийнятної в ціновому плані можливості глобального підключення може значно сприяти ефективності цих зусиль у сфері розвитку.

41. ІКТ, сприяючи підвищенню ефективності і продуктивності, насамперед підприємств малого і середнього бізнесу (МСП), є могутнім каталізатором економічного росту. У цьому сенсі розвиток інформаційного суспільства важливий для економічного росту на широкій основі як у розвинутих, так і в країнах, що розвиваються. Варто заохочувати обумовлений ІКТ ріст продуктивності і впровадження інновацій у сектори економіки. Справедливий розподіл створених благ сприяє ліквідації бідності і соціальному розвитку. Найбільш сприятливий вплив будуть, імовірно, здійснювати ті політичні стратегії, які сприяють продуктивним інвестиціям і дають можливість підприємствам, передусім МСП, здійснювати зміни, необхідні для отримання вигод із застосування ІКТ.

42. Для заохочення інноваційної діяльності і творчості в інформаційному суспільстві важливо забезпечувати захист інтелектуальної власності; аналогічно широке розповсюдження, популяризація і спільне використання інформації також важливі для заохочення інноваційної діяльності і творчості. Сприяння усвідомленій участі всіх у вирішенні питань інтелектуальної власності і спільному використанні знань за допомогою повномасштабного інформування і нарощування потенціалу є одним з основних елементів відкритого для всіх інформаційного суспільства.

43. В інформаційному суспільстві сталому розвитку може найбільшою мірою сприяти повномасштабна інтеграція заходів і програм, що стосуються ІКТ, у національні і регіональні стратегії розвитку. Ми втеємо Нове партнерство в інтересах розвитку Африки (НЕПАД) і закликаємо міжнародне співтовариство підтримати вжиті в рамках цієї ініціативи заходи, що стосуються ІКТ, а також аналогічні заходи, що здійснюються в інших регіонах. Розподіл вигод від економічного росту, одержуваних завдяки застосуванню ІКТ, сприяє ліквідації злиднів і забезпеченню сталого розвитку.

44. До найважливіших складників побудови інформаційного суспільства відносяться стандартизація. Особливу увагу варто приділити розробці і прийняттю міжнародних стандартів. Розробка і використання відкритих, що забезпечують можливість взаємодії, недискримінаційних і зумовлених попитом стандартів обліком потреб користувачів і споживачів, — одна з основних умов розвитку і розширення розповсюдження ІКТ і забезпечення більш прийняттого в ціновому плані доступу до них, насамперед у країнах, що розвиваються. Міжнародні стандарти мають на меті створення сервюшів, у якому споживачі могли б користатися відповідними послугами в будь-якому місці у світі, незалежно від застосовуваної технології.

45. Управління використанням радіочастотного спектра має здійснюватися в інтересах суспільства згідно із принципом законності, при неухильному дотриманні національних законів і норм, а також відповідних міжнародних угод.

46. Держави наполегливо закликаються вживати при побудові інформаційного суспільства заходів, спрямованих на недопущення і відмову від будь-яких односторонніх дій, що не відповідають міжнародному праву і Статуту Організації Об'єднаних Націй, перешкоджають повномасштабному забезпеченню соціального розвитку країн і торкаються добробуту їхнього населення.

47. Оскільки ІКТ поступово змінюють наші методи роботи, першорядне значення має створення захищених, безпечних і таких, які не заповдіють шкоди здоров'ю, умов праці, що передбачають використання ІКТ, з дотриманням усіх відповідних міжнародних норм.

48. Інтернет перетворився на публічний ресурс глобального масштабу, і управління його використанням має стати одним з основних питань порядку денного інформаційного суспільства. Управління використанням Інтернету на міжнародному рівні необхідно здійснювати на багатобічній, прозорій і демократичній основі за повномасштабної участі органів державного управління, приватного сектора, промислового суспільства і міжнародних організацій. Це управління повинне забезпечувати справедливий розподіл ресурсів, сприяти доступу для всіх, гарантувати стабільне і захищене функціонування Інтернету з урахуванням багатомовності.

49. Управління використанням Інтернету охоплює як технічні питання, так і питання державної політики, і в ньому повинні брати участь усі зацікавлені сторони і відповідні міжурядові і міжнародні організації. У зв'язку з цим визнається, що:

- а) політичні повноваження щодо питань державної політики, пов'язані з Інтернетом, є суверенним правом держав. Держави мають права й обов'язки щодо пов'язаних з Інтернетом питань державної політики міжнародного рівня;
- б) приватний сектор відіграє і повинний продовжувати відігравати важливу роль у розвитку Інтернету, як у технічній, так і в економічній сфері;

- с) промисловне суспільство також відіграє важливу роль у питаннях, які стосуються Інтернету, особливо на рівні промисла, і повинно продовжувати відігравати таку роль;
- д) міжурядові організації відіграють і повинні продовжувати відігравати роль, що сприяє координації питань державної політики, пов'язаних з Інтернетом;
- е) міжнародні організації також відіграють і повинні продовжувати відігравати важливу роль у розробці технічних стандартів і відповідної політики, що стосуються Інтернету.

50. Питання управління використанням Інтернету на міжнародному рівні варто вирішувати шляхом узгодження. Ми звертаємося до Генерального секретаря Організації Об'єднаних Націй з проханням створити робочу групу з управління використанням Інтернету в рамках відкритого і всеосяжного процесу, що забезпечує механізм для повномасштабної й активної участі органів державного управління, приватного сектора і промислового суспільства, як з тих, що розвиваються, так і з розвинутих країн, у тому числі відповідних міжурядових і міжнародних організацій і форумів, з метою вивчення питань про управління використанням Інтернету і надання до 2005 року в належних випадках пропозицій для прийняття рішення стосовно організації управлінням і користуванням Інтернету.

7) Додатки на базі ІКТ: переваги у всіх аспектах життя

51. Використання і розпорядання ІКТ повинні бути спрямовані на створення переваг у всіх аспектах нашого повсякденного життя. Додатки на базі ІКТ потенційно важливі для діяльності органів державного управління і наданих ними послуг охорони здоров'я й інформації про охорону здоров'я, освіти і професійної підготовки, зайнятості, створення робочих місць, підприємництва, сільського господарства, транспорту, охорони навколишнього середовища і раціонального використання природних ресурсів, запобігання катастроф, для розвитку культури, а також для ліквідації бідності і досягнення інших покладених цілей у сфері розвитку. Крім того, ІКТ повинні сприяти стійкості структур виробництва та споживання і подоланню традиційних бар'єрів, даючи тим самим можливість всім одержати доступ на місцеві і глобальні ринки на більш рівноправній основі. Додатки ІКТ повинні бути зручними для користувачів, доступними для всіх, прийнятними в ціновому плані, відповідати місцевим потребам завдяки адаптації до місцевих мов і культури і підтримувати стабільний розвиток. Для цього місцеві органи влади повинні відігравати важливу роль у наданні послуг на базі ІКТ на благо своїх громадян.

8) Культурна різноманітність і культурна самобутність, мовна різноманітність і місцевий контент

52. Культурна різноманітність — це загальна спадщина людства. Інформаційне суспільство повинне ґрунтуватися на повазі до культурної само-

бутності, розмаїтості культур і мов, традицій і релігій, стимулювати повагу і сприяти діалогу між культурами і цивілізаціями. Популяризація, зміцнення і збереження різних культур і мов, що відбито у відповідних документах, прийнятих Організацією Об'єднаних Націй, у тому числі в Загальній декларації ЮНЕСКО про культурну різноманітність, будуть далі збагачувати інформаційне суспільство.

53. При побудові відкритого для всіх інформаційного суспільства пріоритет варто віддавати створенню, поширенню і збереженню контенту на різних мовах і в різних формах, при цьому особливо увагу необхідно приділяти розмаїтості пропозицій творчих здобутків і належному визнанню прав авторів і діячів мистецтв. Необхідно сприяти виробництву і забезпеченню доступності всього контенту — освітнього, наукового, культурного і розважального — різними мовами і в різних формах. Розвиток місцевого контенту, що відповідає національним чи регіональним потребам, буде сприяти соціально-економічному розвитку і стимулюватиме участь усіх зацікавлених сторін, включаючи жителів сільських, віддалених і маргінальних районів.

54. Збереження культурної спадщини є одним із найважливіших елементів самобутності і самосвідомості людей і зв'язує суспільство з його минулим. Інформаційне суспільство повинне усіма відповідними методами, включаючи переказ у цифрову форму, збирати і зберігати культурну спадщину для майбутніх поколінь.

9) Засоби масової інформації

55. Ми знову підтверджуємо нашу прихильність до принципів свободи друку і свободи інформації, а також незалежності, плюралізму і розмаїтості засобів масової інформації, що є основним складником інформаційного суспільства. Свобода шукати, одержувати, передавати і використовувати інформацію для створення, нагромадження і поширення знань має істотне значення для інформаційного суспільства. Ми закликаємо засоби масової інформації відповідально використовувати інформацію і користуватися нею відповідно до найвищих етичних і професійних стандартів. Традиційні засоби масової інформації у всіх їхніх видах відіграють важливу роль в інформаційному суспільстві, тому ІКТ повинні сприяти цьому. Варто заохочувати розвиток засобів масової інформації різноманітних форм власності відповідно до національного законодавства, з огляду на відповідні міжнародні конвенції. Ми знову підтверджуємо необхідність скорочення диспропорцій у засобах масової інформації на міжнародному рівні, особливо в тому, що стосується інфраструктури, технічних ресурсів і розвитку навичок і вмінь.

10) Етичні аспекти інформаційного суспільства

56. В інформаційному суспільстві необхідно поважати світ і відстоювати основні цінності, такі як воля, рівність, солідарність, тер-

пимість, колективна відповідальність і дбайливе ставлення до природи.

57. Ми визнаємо важливість для інформаційного суспільства етичних норм, які повинні сприяти справедливості, а також підтримувати гідність і цінність людської особистості. Максимально надійний захист варто забезпечити родині, для того щоб дати їй можливість відігравати в суспільстві вирішальну роль.

58. При використанні ІКТ і при створенні контенту варто поважати права людини і основні свободи інших людей, включаючи неотчужданість приватного життя і право на свободу думки, совісті і релігії, відповідно до положень відповідних міжнародних документів.

59. Всі учасники інформаційного суспільства повинні здійснювати відповідні дії і вживати встановлених законодавством заходів для запобігання неналежного використання ІКТ, такого як протиправні діяння та інші дії на ґрунті расизму, расової дискримінації, ксенофобії і пов'язані з ними прояви нетерпимості, ненависті, насильства, усі форми жорстокого поводження з дітьми, включаючи педофілію і дитячу порнографію, а також торгівля людьми і їх експлуатація.

11) Міжнародне і регіональне співробітництво

60. Ми маємо намір повною мірою використовувати надані ІКТ можливості в нашому прагненні досягти погоджених на міжнародному рівні цілей у сфері розвитку, у тому числі, що містяться в Декларації тисячоріччя, а також відстоювати ключові принципи, викладені в цій Декларації. Інформаційне суспільство глобальне за своєю суттю, і докладені на національному рівні зусилля необхідно підтримувати за допомогою ефективного міжнародного і регіонального співробітництва між органами державного управління, приватним сектором, громадським суспільством та іншими зацікавленими сторонами, включаючи міжнародні фінансові установи.

61. Для побудови відкритого для всіх глобального інформаційного суспільства ми будемо вишукувати й ефективно застосовувати на міжнародному рівні конкретні підходи і механізми, у тому числі здійснювати фінансову і технічну допомогу. Тому, належно оцінюючи співробітництво у сфері ІКТ, що здійснюється в рамках різних механізмів, ми закликаємо всі зацікавлені сторони зобов'язатися прийняти «Порядок денний цифрової солідарності», що міститься в Плані дій. Ми переконані в тому, що подолання на світовому рівні ціль укладається для сприяння подоланню розриву в цифрових технологіях, розширення доступу до ІКТ, створення цифрових можливостей і використання вкладеного в ІКТ потенціалу в інтересах розвитку. Ми визнаємо бажання деяких зацікавлених сторін створити міжнародний добровільний «Фонд цифрової солідарності» і бажання інших сторін провести дослідження, що стосуються існуючих механізмів, а також ефективності й доцільності створення такого фонду.

62. Регіональна інтеграція сприяє розвитку глобального інформаційного суспільства і робить необхідним тісне співробітництво в рамках регіонів і між ними. Регіональний діалог має сприяти нарощуванню потенціалу на національному рівні і приведенню національних стратегій у відповідність до цілей даної Декларації принципів обліку національних і регіональних особливостей. У зв'язку з цим ми закликаємо міжнародне співтовариство підтримати вжиті в рамках таких ініціатив заходи, що стосуються ІКТ.

63. Ми приймаємо рішення сприяти країнам, що розвиваються, нерозвинутим країнам і країнам з перехідною економікою за допомогою мобілізації засобів із усіх джерел фінансування, надання фінансової і технічної допомоги і шляхом створення середовища, що сприяє передачі технологій, відповідно до цілей даної Декларації і Плану дій.

64. Основні сфери компетенції Міжнародного союзу електрозв'язку (МСЕ) в галузях ІКТ — сприяння в подоланні розриву в цифрових технологіях, міжнародне і регіональне співробітництво, управління використанням радіочастотного спектра, розробка стандартів і поширення інформації — мають вирішальне значення для побудови інформаційного суспільства.

С. До інформаційного суспільства для всіх, заснованого на спільному використанні знань

65. Ми беремо на себе зобов'язання зміцнювати співробітництво, для того щоб спільно знаходити рішення проблем і виконувати План дій, перетворюючи в життя концепцію відкритого для всіх інформаційного суспільства, заснованого на ключових принципах, що містяться в даній Декларації.

66. Ми беремо на себе зобов'язання кількісно оцінювати процес подолання розриву в цифрових технологіях і спостерігати за цим процесом з огляду на розбіжності в рівнях розвитку, з тим щоб досягти погоджених на міжнародному рівні цілей у сфері розвитку, у тому числі тих, що містяться в Декларації тисячоріччя, і визначати ефективність інвестицій і зусиль у сфері міжнародного співробітництва для побудови інформаційного суспільства.

67. Ми твердо переконані, що всі разом ми вступимо в нову еру величезних можливостей — еру інформаційного суспільства і розширення сфери людського спілкування. У цьому суспільстві, що зароджується, інформацію і знання можна виробляти, обмінюватися ними, спільно їх використовувати і передавати по всіх світових мережах. Якщо ми будемо здійснювати необхідні дії, незабаром усі люди зможуть спільно побудувати нове інформаційне суспільство, засноване на спільному використанні знань, на базі глобальної солідарності і більш повного взаєморозуміння між народами і країнами. Ми віримо, що ці заходи відкриють шлях до подальшого розвитку суспільства, справді заснованого на знаннях.

ПЛАН ДІЙ

Документ WSIS-03/GENEVA/DOC/5-R

(Прийнято на Всесвітній зустрічі на вищому рівні з питань інформаційного суспільства. Женева, 12 грудня 2003)

А. Вступ

1. У цьому Плані дій загалом концепція і керівні принципи Декларації знаходять своє втілення в конкретних напрямках діяльності, що спрямовані на досягнення погоджених на міжнародному рівні цілей розвитку, у тому числі тих, що містяться в Декларації тисячоріччя, Монтеррейському консенсусі і Йоганнесбурзькій Декларації і Плані виконання рішень, шляхом сприяння використанню продуктів, мереж, послуг і додатків на базі ІКТ, а також покликані допомогти країнам у подоланні розриву в цифрових технологіях. Інформаційне суспільство, створення якого передбачається в Декларації принципів, буде будуватися в умовах співробітництва і солідарності, органами державного управління і всіма іншими зацікавленими сторонами.

2. Інформаційне суспільство — це еволюціонуюча структура, що, відображаючи різні стадії розвитку, досягла різних рівнів у різних країнах світу. Технологічний прогрес та інші зміни стрімко перетворюють середовище, у якому розвивається інформаційне суспільство. У зв'язку з цим План дій є основою, що еволюціонує, що забезпечує поступ до інформаційного суспільства на національному, регіональному і міжнародному рівнях. Унікальна двоетапна структура Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства (ВЗРІС) дозволяє враховувати подібну еволюцію.

3. Усі зацікавлені сторони відіграють важливу роль в інформаційному суспільстві, насамперед через партнерські відносини:

- а) органам державного управління відведена роль у розробці і здійсненні всеосяжних, перспективних і стійких національних електронних стратегій. Приватний сектор і промисловість суспільства, у діалозі з органами державного управління, повинні відіграти важливу консультативну роль у формуванні національних електронних стратегій;
- б) участь приватного сектора має велике значення для розвитку і поширення інформаційних і комунікаційних технологій (ІКТ), для інфраструктури, контенту і додатків. Приватний сектор не тільки є учасником ринку, а й відіграє певну роль у більш широкому контексті сталого розвитку;
- в) участь і зацікавленість промисловського суспільства настільки ж важливі для створення справделивого інформаційного суспільства і здійснення ініціатив у сфері розвитку, що відносяться до ІКТ.

- d) міжнародні і регіональні установи, у тому числі міжнародні фінансові установи, відіграють ключову роль в інтеграції застосування ІКТ у процес розвитку й у надання необхідних ресурсів для побудови інформаційного суспільства й оцінки досягнутого прогресу в цій сфері.

В. Завдання, цілі і контрольні показники

4. Завдання Плану дій полягають у тому, щоб побудувати відкрите для всіх інформаційне суспільство; поставити потенціал, закладений у знаннях і ІКТ, на служіння розвитку; сприяти використанню інформації і знань для досягнення погоджених на міжнародному рівні цілей розвитку, у тому числі тих, що містяться в Декларації тисячоріччя; і вирішувати нові проблеми інформаційного суспільства на національному, регіональному і міжнародному рівнях. На другому етапі ВЗРІС варто скористатися з можливості для аналізу й оцінки прогресу, досягнутого в ліквідації прогалів у цифрових технологіях.

5. На національному рівні в межах національних електронних стратегій і відповідно до державної політики у сфері розвитку в певних випадках повинні бути встановлені конкретні контрольні показники побудови інформаційного суспільства з урахуванням національних особливостей. Такі контрольні показники можуть слугувати корисними віхами для здійснюваних дій і оцінки прогресу в досягненні загальних цілей інформаційного суспільства.

6. Засновані на потовджених на міжнародному рівні цілях у сфері розвитку, у тому числі тих, що містяться в Декларації тисячоріччя, які базуються на міжнародному співробітництві, орієнтовані контрольні показники можуть слугувати глобальними цільовими показниками росту рівня підключення і доступу при використанні ІКТ у межах виконання завдань Плану дій, що повинні бути реалізовані до 2015 року. Ці контрольні показники можуть враховуватися при встановленні національних контрольних показників з урахуванням національних особливостей.

забезпечити підключенням на базі ІКТ села і створити в них пункти ко-лективного доступу;

забезпечити підключенням на базі ІКТ університети, коледжі, середні і початкові школи;

забезпечити підключенням на базі ІКТ науково-дослідні центри;

забезпечити підключенням на базі ІКТ публічні бібліотеки, культурні центри, музеї, поштові відділення й архіви;

забезпечити підключенням на базі ІКТ центри охорони здоров'я і лікарні; забезпечити підключенням усі місцеві і центральні державні установи і забезпечити наявність у них веб-сайтів і адрес електронної пошти;

внести зміни в програми всіх початкових і середніх шкіл, для того щоб включити в них завдання, висуваючі інформаційним суспільством, з урахуванням національних особливостей;

забезпечити все населення планети доступом до служб теле- і радіомовлення;

заохочувати розвиток контенту і створити технічні умови, що сприяли б представленню і використанню в Інтернеті усіх мов світу;

забезпечити доступ до ІКТ в межах можливого більш ніж для половини населення планети.

7. При вирішенні цих завдань і досягненні цілей і контрольних показників особлива увага повинна приділятися потребам країн, що розвиваються, зокрема країн, народів і груп, що згадуються в пунктах 11—16 Декларації принципів.

С. Напрямок дій

С1. Роль органів державного управління і всіх зацікавлених сторін у сприянні використанню ІКТ із метою розвитку

8. Вирішальне значення для розвитку інформаційного суспільства має дієва участь органів державного управління і всіх зацікавлених сторін, для чого необхідне співробітництво і партнерські відносини між усіма ними.

- a) Усі країни повинні заохочувати розробку до 2005 року національних електронних стратегій, включаючи наروшування необхідного людського потенціалу, з урахуванням національних особливостей.

- b) Приступити на національному рівні до організованого діалогу за участю всіх зацікавлених сторін, у тому числі в рамках партнерських відносин між державним і приватним сектором, щодо розробки електронних стратегій для інформаційного суспільства й обміну зразками найкращої практики.

- c) При розробці і здійсненні національних електронних стратегій зацікавлені сторони повинні враховувати місцеві, регіональні і національні потреби і проблеми. Для одержання максимальних переваг від здійснюваних ініціатив до них необхідно включити принцип стійкості. Приватний сектор має брати участь у конкретних проєктах розвитку інформаційного суспільства на місцевому, регіональному і національному рівнях.

- d) Кожну країну покликано до створення до 2005 року принаймні одного дієвого партнерства між державним і приватним секторами (ПДП) чи партнерства між кількома секторами (ПКС) як зразка для подальшої діяльності.

- e) Визначити на національному, регіональному і міжнародному рівнях механізми, необхідні для встановлення і розвитку партнерських відносин між зацікавленими сторонами в інформаційному суспільстві.

- г) Вивчити доцільність створення на національному рівні порталів для корінних народів за участю різних зацікавлених сторін.
- г) До 2005 року відповідні міжнародні організації і фінансові установи повинні розробити власні стратегії застосування ІКТ з метою сталого розвитку, у тому числі таких, що належать до стійких схем виробництва і споживання; ці стратегії повинні стати також ефективним інструментом сприяння досягненню цілей, встановлених Організацією Об'єднаних Націй у Декларації тисячоріччя.
- г) Міжнародні організації повинні публікувати, у тому числі на своїх веб-сайтах, достовірну інформацію, що відноситься до сфери їхньої компетенції і надану відповідними зацікавленими сторонами, про успішно проведені заходи щодо вклюднення ІКТ в основи напрямки діяльності.
- г) Сприяяти здійсненню ряду пов'язаних з цим заходів, у тому числі створенню схем бізнесів-інкубаторів, надання венчурного капіталу (на національному і міжнародному рівнях), встановленню державних інвестиційних фондів, у тому числі для мікрофінансування малих, середніх і мікропідприємств (МСМП), реалізації стратегії залучення інвестицій, проведення заходів на підтримку експорту програмного забезпечення (торгового консультування), підтримку мереж для проведення науково-дослідницьких і дослідницько-конструкторських робіт і парків програмного забезпечення.

С2. Інформаційна і комунікаційна інфраструктура — необхідний фундамент інформаційного суспільства

- 9. Інфраструктура є основою для досягнення мети з охоплення всіх жителів планети цифровими технологіями, тобто надання універсального, стійкого, поширеного і прийняттого в цілому плану доступу до ІКТ для всіх, з урахуванням відповідних рішень, уже застосовуваних у країнах, що розвиваються, і країнах з перехідною економікою, для забезпечення надійного підключення і доступу до віддалених і маргіналізованих районів на національному і регіональному рівнях.
- а) Органи державного управління в рамках національної політики розвитку повинні приймати рішення, спрямовані на підтримку сприятливого і конкурентного середовища для одержання необхідних інвестицій в інфраструктуру ІКТ і для розвитку нових послуг.
- б) Виробити в межах національних електронних стратегій відповідні політику і стратегію забезпечення універсального доступу і визначити кошти їх реалізації, відповідно до орієнтованих контрольних показників, а також розробити показники доступу до ІКТ.
- с) У межах національних електронних стратегій, відповідно до орієнтованих контрольних показників, забезпечити й удосконалювати

- вати підключення на базі ІКТ усіх шкіл, університетів, установ охорони здоров'я, бібліотек, поштових відділень, обштинних центрів, музеїв та інших доступних для населення установ.
- д) Розвивати і зміцнювати інфраструктуру національних, регіональних і міжнародних мереж широколінійного зв'язку, включаючи супутникові й інші системи, для сприяння забезпеченню пропускної здатності, що відповідає потребам країн і їхніх громадян, а також створює умови для надання нових послуг на базі ІКТ. Надавати підтримку технічним, регламентним і експлуатаційним дослідженням, проведенням Міжнародним союзом електронного зв'язку (МСЕ) і, у належних випадках, іншими відповідними міжнародними організаціями, для того щоб:
- г) розширити доступ до орбітальних ресурсів, забезпечити глобальну гармонізацію використання частот і глобальну стандартизацію систем;
- г) заохочувати партнерські відносини між державним і приватним сектором;
- гг) сприяти наданню глобальних послуг високошвидкісного супутникового зв'язку для районів, що недостатньо обслуговуються, зокрема віддалених і малонаселених районів;
- гг) досліджувати інші системи, здатні забезпечувати високошвидкісні підключення.
- г) У рамках національних електронних стратегій домагатися задоволення особливих потреб старих, осіб з обмеженими можливостями, дітей, насамперед маргіналізованих дітей, а також інших вразливих груп населення, що перебувають у скрутному становищі, за допомогою відповідних заходів освітнього, адміністративного і законодавчого характеру, спрямованих на забезпечення повномасштабного вклюднення зазначених груп в інформаційне суспільство.
- г) Заохочувати розробку і виробництво устаткування і послуг на базі ІКТ, зручних у використанні і прийнятних у цілому плані для всіх, включаючи старих, осіб з обмеженими можливостями, дітей, насамперед маргіналізованих дітей, так само як і інші вразливі групи населення, і тих, що перебувають у скрутному становищі, а також сприяти розвитку технологій, додатків і контенту, відповідно до їхніх потреб, на основі принципів універсального дизайну і при подальшому удосконаленні шляхом використання асистиивних технологій.
- г) З метою пом'якшення проблем, пов'язаних з непрацотнстю, розробити прийнятні щодо ціни технології і безтекстові комп'ютерні інтерфейси, для того щоб полегшити людям доступ до ІКТ.
- г) На міжнародному рівні проводити науково-дослідницькі і дослідницько-конструкторські роботи, спрямовані на створення належного і прийнятного в цілому плану устаткування на базі ІКТ для кінцевих користувачів.

- і) Заохочувати використання у розвинутих країнах і, особливо, у країнах, що розвиваються, невикористовуваних потужностей безпроводного зв'язку, включаючи супутниковий зв'язок, для забезпечення доступу у віддалених районах, насамперед у країнах, що розвиваються, і в країнах з перехідною економікою, а також для більш широкого впровадження низьковартісного підключення в країнах, що розвиваються. Особливу увагу варто приділяти найменш розвинутим країнам (НРК), що прагнуть створити інфраструктуру електрозв'язку.
- і) Оптимізувати з'єднання між основними інформаційними мережами, заохочуючи створення і розвиток регіональних магістральних структур на базі ІКТ і комутаційних станцій Інтернету для зниження вартості міжмережових з'єднань і розширення доступу до мереж.
- к) Розробляти стратегії поширення в глобальному масштабі прийняттого в ціновому плані підключення, сприяючи тим самим удосконалюванню доступу. Визначені на комерційній основі витрати на транзит і міжмережіві з'єднання через Інтернет повинні базуватися на об'єктивних, прозорих і таких, що не допускають дискримінації, параметрах з обліком роботи, що ведеться по цій темі.
- і) Заохочувати і стимулювати спільне використання традиційних коштів масової комунікації і нових технологій.

С3. Доступ до інформації і знань

10. ІКТ дають людям можливість одержувати доступ до інформації і знань практично миттєво в будь-якій точці планети. Можливостями доступу до знань і інформації повинні користуватися приватні особи, організації і громади.

- а) Розробляти політичні керівні принципи для розвитку і популяризації інформації, що є публічним надбанням, як важливий міжнародний інструмент сприяння доступу населення до інформації.
- б) Органи державного управління покликані забезпечити за допомогою різних ресурсів зв'язку, передусім Інтернету, належний доступ до офіційної інформації, що є публічним надбанням. Заохочується розробка законодавства щодо доступу до інформації і збереження даних, що є публічним надбанням, особливо в галузі нових технологій.
- с) Підтримувати науково-дослідницькі і дослідницько-конструкторські роботи, для того щоб сприяти доступності ІКТ для всіх, у тому числі для тих, хто перебуває в несприятливих умовах, маргіналізованих і вразливих груп населення.
- д) Органам державного управління й іншим зацікавленим сторонам варто створювати стабільно функціонуючі багатодієві публічні пункти колективного доступу, що надають для грома-

- дин за прийнятними цінами чи безкоштовно доступ до різних ресурсів зв'язку, передусім до Інтернету. Ці пункти доступу повинні, наскільки можливо, володіти достатньою пропускну здатністю для надання допомоги користувачам у бібліотеках, навчальних закладах, державних структурах, поштових відділеннях та інших громадських місцях, причому особливу увагу варто приділяти сільським районам, і районам, що недостатньо обслуговуються, за отримання прав інтелектуальної власності (ПС) і заохочення використання інформації й обміну знаннями.
- е) Заохочувати дослідження і сприти поінформованості всіх зацікавлених сторін про можливість, надані різними моделями програмного забезпечення, і про кошти його створення, включаючи програмне забезпечення, розроблене окремими компаніями, програмне забезпечення з відкритими кодами, а також вільно поширюване програмне забезпечення, для того щоб розширювати конкуренцію й розмаїтість вибору, підвищувати цінову прийнятність і надавати усім зацікавленим сторонам можливість зрозуміти, який варіант є для них найбільш придатним.
- і) Уряди повинні активно сприяти застосуванню громадянами своїх країн і місцевих органів влади ІКТ як основного робочого інструменту. Для досягнення цієї мети міжнародному співтовариству й іншим зацікавленим сторонам варто підтримувати — як впровадження місцевого управління — наروшування потенціалу місцевих органів влади на основі широкого використання ІКТ.
- е) Заохочувати дослідження з питань інформаційного суспільства, у тому числі з інноваційних форм створення мереж адаптації інфраструктури ІКТ, інструментів і додатків на базі ІКТ, що сприяє доступності ІКТ для всіх, зокрема для груп населення, що перебувають у несприятливих умовах.
- і) Підтримувати створення і розвиток публічної бібліотечної й архівної цифрової служби, адаптованої до інформаційного суспільства, у тому числі шляхом перегляду національних стратегій і законодавства в галузі бібліотечного обслуговування, забезпечення на глобальному рівні розуміння потреби в «гібридних бібліотеках» і сприяючи співробітництву бібліотек на всесвітньому рівні.
- і) Заохочувати ініціативи зі сприяння доступу, у тому числі доступу вільного й прийнятнього за ціною, до журналів, що знаходяться у відкритому доступі, книг і відкритих архівів наукової інформації.
- і) Підтримувати науково-дослідницькі і дослідницько-конструкторські роботи у сфері проектування корисних інструментів для всіх зацікавлених сторін з метою підвищення поінформованості, проведення аналізу й оцінки різних моделей програмного забезпечення і відповідного ліцензування, для того, щоб забезпечити

оптимальний вибір належного програмного забезпечення, яке б шонайкраще сприяло досягненню цілей розвитку в місцевих умовах.

С4. Нарощування потенціалу

II. Кожен повинний мати навички, необхідні для використання повною мірою переваг інформаційного суспільства. Тому варто нарощувати потенціал і підвищувати грамотність у сфері ІКТ. ІКТ можуть сприяти досягненню у всесвітньому масштабі загального навчання шляхом надання коштів для отримання освіти і підготовки викладачів, створення більш досконалих умов для навчання протягом усього життя, що охоплювало б людей, що перебувають поза рамками формальної системи освіти, а також для удосконалення професійних навичок.

- a) Розробляти національні стратегії для забезпечення повномасштабної інтеграції ІКТ у сферу освіти і професійної підготовки на всіх рівнях, у тому числі в розробку навчальних програм, підготовку викладачів, управління і керівництво установами, так само як і підтримку навчання протягом усього життя.
- b) Розробляти програми ліквідації неграмотності за допомогою ІКТ на національному, регіональному і міжнародному рівнях і сприяти їх впровадженню.
- c) Сприяти всім в оволодінні навичками електронної грамотності, наприклад, шляхом розробки й організації курсів для державних службовців, використовуючи для цього такі існуючі структури, як бібліотеки, багатопільові обштинні центри, публічні пункти доступу, а також шляхом створення на місцях центрів професійної підготовки в сфері ІКТ у співробітництві з усіма зацікавленими сторонами. Особливу увагу слід приділяти вразливим групам населення і таким, що перебувають в несприятливому становищі.
- d) У контексті національної політики у сфері освіти і з урахуванням необхідності ліквідації неграмотності серед дорослих забезпечити, щоб молодь була озброєна знаннями і навичками застосування ІКТ, у тому числі мала змогу творчо і по-новому аналізувати й обробляти інформацію, ділитися своїм досвідом і повною мірою брати участь в інформаційному суспільстві.
- e) Організація державного управління, у співробітництві з іншими зацікавленими сторонами, повинні розробляти програми нарощування потенціалу, у яких основна увага приділялася б створенню критичної маси кваліфікованих і досвідчених професіоналів і експертів у галузі ІКТ.
- f) Розробляти експериментальні проекти для демонстрації впливу альтернативних систем освіти на базі ІКТ, насамперед для досягнення цілей освіти для всіх, у тому числі цілей забезпечення базової грамотності.

- g) Працювати над усуненням гендерних бар'єрів для одержання освіти і професійної підготовки у сфері ІКТ і сприяти забезпеченню рівних можливостей професійної підготовки у пов'язаних з ІКТ сферах для жінок і дівчат. Програми, здійснювані в галузі науки і техніки, із самого початку повинні бути орієнтовані на дівчат, щоб збільшити число жінок, зайнятих у сфері ІКТ. Сприяти обміну зразками найкращої практики до включення принципу рівноправності чоловіків і жінок в освіті в галузі ІКТ.
 - h) Давати місцевим громадам, у першу чергу в сільських районах і в районах, що обслуговуються недостатньою мірою, можливість застосовувати ІКТ і забезпечувати виробництво корисної і соціально значимої складової для загального благополуччя.
 - i) Приступити до здійснення програм в галузі освіти і професійної підготовки, використовуючи, де це можливо, інформаційні мережі, споконвіку кочових і корінних народностей, щоб відкрити їм можливість повною мірою брати участь в інформаційному суспільстві.
 - j) Планувати і здійснювати на регіональному і міжнародному рівнях спільні заходи з метою розвитку потенціалу, насамперед керівників і експлуатаційного персоналу в країнах, що розвиваються, і НРК, для ефективного застосування ІКТ на всіх напрямках освітньої діяльності. При цьому варто передбачати і навчання поза рамками освітньої системи, наприклад на робочому місці чи вдома.
- Розробляти спеціальні програми професійної підготовки із застосування ІКТ для задоволення потреб у навчанні фахівців у сфері інформації, таких як архівні, бібліотечні і музейні працівники, вчені, викладачі, журналісти, поштові службовці й інші відповідні професійні групи. При підготовці фахівців у галузі інформації варто спиратися не тільки на нові методи і способи, призначені для розвитку і надання інформаційних і комунікаційних послуг, а й на відповідні навички управління, для того щоб забезпечити оптимальне застосування технологій. При підготовці викладачів основну увагу слід приділяти технічним аспектам ІКТ, розробці контенту і можливостям та перспективам, що відкривають ІКТ.
 - l) Розвивати дистанційне навчання, професійну підготовку й інші форми навчання і професійної підготовки як частину програм нарощування потенціалу. Приділяти особливу увагу країнам, що розвиваються, і насамперед НРК, із різними рівнями розвитку людських ресурсів.
 - m) Сприяти міжнародному і регіональному співробітництву у сфері нарощування потенціалу, у тому числі впровадженню для країн програм, розроблюваних Організацією Об'єднаних Націй і її спеціалізованими установами.
 - n) Здійснювати експериментальні проекти для розробки нових форм роботи мережі на основі ІКТ, що поєднували б педагогічні і про-

фесійно-технічні навчальні заклади і науково-дослідницькі установи в розвинутих країнах і країнах, що розвиваються, а також країнах із перехідною економікою.

о) Рух добровольців, якщо він діє відповідно до національної політики і місцевих культурних традицій, може бути цінним засобом як для підвищення здатності людських ресурсів продуктивно використовувати інструменти на базі ІКТ, так і для побудови більш відкритого для всіх інформаційного суспільства. Організовувати добровільні програми для нарощування потенціалу в галузі ІКТ із метою розвитку, насамперед у країнах, що розвиваються.

р) Розробляти програми для навчання користувачів методів розвитку потенціалу самоосвіти і саморозвитку.

С5. Зміцнення довіри і безпеки при використанні ІКТ

12. Довіра і безпека належать до основного підґрунтя інформаційного суспільства.

а) Сприяти співробітництву між державами в рамках Організації Об'єднаних Націй і з усіма зацікавленими сторонами в межах відповідних форумів з метою зміцнення довіри користувачів, підвищення надійності і захисту цілісності як даних, так і мереж; аналізу існуючої і потенційної небезпеки в галузі ІКТ; а також вирішення інших питань інформаційної безпеки і безпеки мереж.

б) Органам державного управління в співпраці з приватним сектором необхідно попереджати, виявляти прояви кіберзлочинності і неналежного використання ІКТ і реагувати на ці прояви шляхом розробки керівних принципів, що враховували б роботу, яка проводиться в цій сфері; вивчення законодавства, що дає можливість ефективно розслідувати і переслідувати неналежне використання; сприяти ефективним заходам взаємодопомогти; посилити на міжнародному рівні інституційну підтримку профілактики таких інцидентів, їх виявлення і ліквідацію їх наслідків; а також шляхом сприяння освіті і підвищенню поінформованості.

с) Органи державного управління й інших зацікавлених сторін повинні активно заохочувати навчання користувачів і підвищувати їхню поінформованість щодо недоторканності приватного життя при роботі в он-лайнному режимі і способів його захисту.

д) Живити необхідних заходів на національному і міжнародному рівнях для захисту від спаму.

е) Заохочувати проведення на національному рівні оцінки внутрішнього законодавства з метою ліквідації перешкод для ефективного використання документів і здійснення угод в електронній формі, у тому числі використання електронних методів автентифікації.

ф) Продовжувати зміцнення надійності і безпеки за допомогою взаємодоповнюючих і взаємопоглинюючих ініціатив у сфері безпеки при використанні ІКТ та ініціатив чи керівних принципів щодо прав на недоторканність приватного життя, захист даних і прав споживачів.

г) Обмінюватися зразками найкращої практики у сфері інформаційної безпеки і безпеки мереж і заохочувати їх використання всіма зацікавленими сторонами.

и) Запропонувати зацікавленим країнам призначити координаторів для реагування в режимі реального часу на події у сфері безпеки й об'єднати цих координаторів у відкритий спільну мережу для обміну інформацією і технологіями реагування на події.

і) Заохочувати подальший розвиток безпечних і надійних додатків для спрощення здійснення угод в он-лайнному режимі.

ж) Заохочувати активну участь зацікавлених країн у проведенні Організацією Об'єднаних Націй діяльності зі зміцнення довіри і надійності при використанні ІКТ.

С6. Сприятливе середовище

13. Для досягнення максимальних переваг інформаційного суспільства в соціальній, економічній і екологічній сферах органам державного управління необхідно створювати надійне, прозоре, недискримінаційне правове, регуляторне і політичне середовище. Для цього:

а) Органи державного управління повинні сприяти створенню сприятливого, прозорого, сприятливого для розвитку конкуренції середовища і передбачуваних політичних, правових і регуляторних меж, що забезпечували б належні стимули для інвестицій і розвитку проклад в інформаційному суспільстві.

б) Ми звертаємося до Генерального секретаря Організації Об'єднаних Націй із проханням створити робочу групу з управління використанням Інтернету в рамках відкритого і всеосяжного процесу, що забезпечує механізм для повномасштабної й активної участі органів державного управління, приватного сектора і громадського суспільства як з таких, що розвиваються, так і з розвинутих країн, у тому числі певних міждержавних і міжнародних організацій і форумів, з метою вивчення питання про управління використанням Інтернету і надання до 2005 року пропозицій для ухвалення рішень щодо організації управління використанням Інтернету. Зокрема, групи слід:

- i) виробити робоче визначення управління використанням Інтернету;
- ii) вивчити питання державної політики, що відносяться до управління використанням Інтернету;
- iii) сформувати єдине розуміння відповідної ролі і сфери відповідальності органів державного управління, існуючих міжу-

- дових і міжнародних організацій та інших форумів, а також приватного сектора і громадського суспільства як з тих країн, що розвиваються, так і з розвинутих країн;
- iv) підготувати звіт про результати виконаної роботи для подання на розгляд у ході другого етапу ВЗРІС у Тунісі в 2005 році й уведення відповідного рішення.
- с) Органам державного управління пропонується:
- i) сприяти створенню національних і регіональних комунікаційних центрів Інтернету;
 - ii) здійснювати в певних випадках управління своїми доменами вищого рівня, що мають код країни (ccTLD), чи нагляд за ними;
 - iii) підвищувати рівень поінформованості про використання Інтернету.
- d) У співробітництві з відповідними зацікавленими сторонами сприяти створенню регіональних кореневих серверів і використанню інтернаціональних найменувань доменів, для того щоб по-долати бар'єри, що перешкоджають доступу.
- e) Органам державного управління варто продовжувати оновлювати національні закони про захист прав споживачів, приводячи їх у відповідність до нових вимог інформаційного суспільства.
- f) Сприяти ефективній участі країн, що розвиваються, і країн з перехідною економікою в міжнародних форумах з питань ІКТ і створювати можливість для обміну досвідом.
- g) Органам державного управління необхідно розробити національні стратегії, у тому числі стратегії електронного державного управління, для того щоб зробити державне управління більш прозорим, ефективним і демократичним.
- h) Розробити основу для безпечного збереження й архівування документів та інших електронних інформаційних записів.
- i) Органи державного управління і зацікавлені сторони повинні активно сприяти освіті користувачів та інформуванню їх щодо недоторканності приватного життя при роботі в он-лайнному режимі і способів захисту недоторканності приватного життя.
- j) Запропонувати зацікавленим сторонам забезпечити, щоб заходи, розроблені з метою сприяння електронній торгівлі, давали споживачам також можливість вибору: використовувати електронний зв'язок чи відмовитися від нього.
- k) Заохочувати роботу, що ведеться у сфері створення ефективних систем вирішення спорів, зокрема зі введення альтернативних методів вирішення спорів(АМВ), що можуть сприяти вирішенню спорів.
- l) Органам державного управління в співпраці із зацікавленими сторонами пропонується розробити політику в галузі ІКТ, сприятливу для розвитку підприємництва, сприяння інноваціям та інве-

- стиціям, приділяючи при цьому особливу увагу розширенню участі жінок;
- m) З урахуванням економічного значення ІКТ для малих і середніх підприємств (МСП) варто допомагати їм підвищувати свою конкурентоспроможність, спрощуючи адміністративні процедури, забезпечуючи їм доступ до фінансових ресурсів і підвищуючи їхню здатність брати участь у пов'язаних з ІКТ проєктах.
- n) Органам державного управління повинні бути зразковими користувачами і лідерами в переході до електронної торгівлі згідно з рівнем соціально-економічного розвитку своїх країн.
- o) Органи державного управління в співпраці з іншими зацікавленими сторонами повинні підвищувати поінформованість про значення міжнародних стандартів функціональної сумісності для глобальної електронної торгівлі.
- p) Органи державного управління в співпраці з іншими зацікавленими сторонами повинні сприяти розробці і застосуванню відкритих, таких, що забезпечують можливість взаємодії, недискримінаційних і обумовлених попиту стандартів.
- q) МСЕ, використовуючи свій потенціал договірних відносин, координує використання і здійснює розподіл частот в інтересах сприяння загальному і прийнятному у цілому плані доступу.
- r) У рамках МСЕ й інших регіональних організацій варто вживати додаткових заходів для забезпечення раціонального, ефективного й економічного використання всіма країнами радіочастотного спектра, а також справедливого доступу до нього на основі відповідних міжнародних угод.

С7. Додатки на базі ІКТ: переваги у всіх аспектах життя

14. Додатки на базі ІКТ можуть служити опорою для сталого розвитку у сферах державного управління, господарської діяльності, освіти і професійної підготовки, охорони здоров'я, зайнятості, навколишнього середовища, сільського господарства і науки в рамках національних електронних стратегій. Сюди можна віднести діяльність у таких секторах:

15. Електронне державне управління

- a) Здійснювати стратегію електронного державного управління, звертаючи особливу увагу на додатки, спрямовані на забезпечення інноваційної діяльності і прозорості державних установ та демократичних процесів, підвищуючи ефективність і зміцнюючи зв'язок із громадянами.
- b) Розробити на всіх рівнях національні ініціативи і послуги електронного державного управління, що відповідають потребам громадян і ділових кіл, для того, щоб домогтися більш ефективного розподілу ресурсів і публічного надбавня.

- с) Підтримувати ініціативи з міжнародного співробітництва у сфері електронного державного управління з метою підвищення прозорості, підзвітності й ефективності на всіх рівнях державного управління.

16. Електронна комерційна діяльність

- а) Органи державного управління, міжнародні організації і приватний сектор покликані популяризувати переваги міжнародної торгівлі і сприяти веденню електронної комерційної діяльності, а також використанню в країнах, що розвиваються, і країнах з перехідною економікою моделей електронної комерційної діяльності.
- б) Органам державного управління слід шляхом створення сприятливого середовища і на основі загальнопоширеного доступу до Інтернету стимулювати інвестиції з боку приватного сектора, заохочувати створення нових додатків і розробку контенту, а також сприяти співробітництву державного і приватного секторів.
- с) Політика органів державного управління повинна спрямовуватися на підтримку і розвиток МСМП у галузі ІКТ, а також на сприяння їхній участі в електронній комерційній діяльності, для того щоб стимулювати економічний ріст і створення нових робочих місць у рамках стратегії скорочення рівня бідності за допомогою утворення матеріальних благ.

17. Електронне навчання (див. розділ С4)

18. Електронна охорона здоров'я

- а) Заохочувати спільні дії органів державного управління, органів, що займаються плануванням, фахівців у сфері охорони здоров'я, а також інших установ поряд з участю міжнародних організацій у створенні надійних, працюючих без перешкод, високоякісних і доступних у ціновому плані систем охорони здоров'я й інформаційних систем з охорони здоров'я, а також у сприянні постійній професійній підготовці, освіті і дослідженням у галузі медицини за допомогою ІКТ, при цьому дотримуючись і захищаючи право громадян на недоторканність приватного життя.
- б) Сприяти доступу до існуючих у світі медичних знань і актуальних на місцевому рівні інформаційних ресурсів для зміцнення державних дослідницьких і профілактичних програм в галузі охорони здоров'я й охорони здоров'я чоловіків і жінок, зокрема до інформації про сексуальне і репродуктивне здоров'я й інфекції, що передаються статевим шляхом, а також про захворювання, на які звернена увага всього світу, такі як ВІЛ/СНІД, малярія і туберкульоз.
- с) Проводити профілактику, моніторинг і контроль за поширенням інфекційних захворювань, удосконалюючи для цього колективні інформаційні системи.

- д) Сприяти розробці міжнародних стандартів для обміну медичними даними, приділяючи при цьому належну увагу забезпеченню недоторканності приватного життя.
- е) Заохочувати застосування ІКТ для підвищення якості і поширення охорони здоров'я й інформаційних систем охорони здоров'я у віддалених районах і районах, що обслуговуються недовідстатньою мірою, а також в інтересах вразливих груп населення, визнаючи при цьому роль жінок у наданні медичної допомоги в родинних і промадах.
- ф) Зміцнювати і розширювати ініціативи на базі ІКТ з надання медичної і гуманітарної допомоги в надзвичайних ситуаціях.

19. Електронна зайнятість

- а) Заохочувати на національному рівні створення для працівників і роботодавців, що застосовують електронні форми праці, принципи найкращої практики на основі принципів справедливості і рівноправності жінок і чоловіків, дотримуючись при цьому всіх відповідних міжнародних норм.
- б) Популяризувати нові способи організації роботи і комерційної діяльності з метою підвищення продуктивності, сприяння економічному росту і росту добробуту шляхом інвестицій у ІКТ і людські ресурси.
- с) Заохочувати застосування телероботи, що дозволяє громадянам, насамперед у країнах, що розвиваються, НРК і малих країнах жити у своєму суспільстві, працюючи при цьому в будь-якому місці, а також розширювати можливості працевлаштування для жінок і осіб з обмеженими можливостями. Популяризуючи телероботу, особливу увагу варто приділяти стратегіям, що сприяють створенню робочих місць і збереженню кваліфікованої робочої сили.
- д) Сприяти введенню з самого початку орієнтованих на дівчат програм у науково-технічній галузі з метою збільшення числа жінок, що працюють у сфері ІКТ.

20. Електронна охорона навколишнього середовища

- а) Органи державного управління в співпраці з іншими зацікавленими сторонами покликані використовувати і пропагувати ІКТ як інструмент для охорони навколишнього середовища і сталого використання природних ресурсів.
- б) Органи державного управління, промадянське суспільство і приватний сектор покликані виступати ініціаторами заходів і здійснювати проекти і програми сталого виробництва і споживання й екологічно безпечної утилізації і рециркуляції апаратного забезпечення, що вийшло з ужитку, і деталей устаткування на базі ІКТ.
- с) Створювати системи контролю на базі ІКТ для прогнозування і моніторингу впливу на навколишнє середовище стихійних і ан-

тропотенних катестроф, особливо в країнах, що розвиваються, НРК і малих країнах.

21. Електронне сільське господарство

- а) Забезпечувати систематичне поширення на базі ІКТ інформації із сільського господарства, тваринництва, рибної промисловості, лісового господарства і продовольства з метою надання вільного доступу до комплексних, актуальних і детальних знань та інформації, особливо в сільських районах.
- б) У партнерстві державного і приватного секторів варто прагнути максимально розширювати використання ІКТ як інструмента для вдосконалення виробництва (у кількісному і якісному сенсі).

22. Електронна наукова діяльність

- а) Сприяти тому, щоб усі університети і науково-дослідницькі інститути мали прийнятне щодо ціни і надійне високошвидкісне підключення до Інтернету з метою забезпечення їхньої вирішальної ролі у виробництві інформації і знань, освіти й професійній підготовці і сприяти налагодженню партнерських відносин, співробітництву і мережевому зв'язку між цими установами.
- б) Стимулювати ініціативи у сфері електронної видавничої діяльності, диференційованого ціноутворення і відкритого доступу, для того щоб наукова інформація була прийнятною щодо ціни і доступною на справедливій основі у всіх країнах.
- в) Сприяти застосуванню однорангової технології для спільного використання наукових знань, препринтів і передруків праць учених, що відмовилися від свого права на гонорари.
- г) Сприяти в довгостроковій перспективі систематичному й ефективному збору, поширенню і збереженню найважливіших наукових даних у цифровій формі, наприклад демографічних і метеорологічних даних, у всіх країнах.
- е) Популяризувати принципи і стандарти метаданих для сприяння співробітництву й ефективному використанню зібраної наукової інформації і даних, як це потрібно для проведення наукових досліджень.

С8. Культурна різноманітність і культурна самобутність,

мовна різноманітність і місцевий контент

23. Культурна і мовна різноманітність, що стимулює повагу до культурної самобутності, традицій і релігій, є необхідною умовою розвитку інформаційного суспільства на базі діалогу між культурами регіонального і міжнародного співробітництва. Вона є важливим фактором стійкого розвитку.

- а) Розробляти політику, що сприяє повазі, збереженню, розвитку і зміцненню культурної і мовної різноманітності і культурної спадщини в рамках інформаційного суспільства, що відображає-

но у відповідних прийнятих Організацією Об'єднаних Націй документах, у тому числі в Загальній декларації ЮНЕСКО про культурну різноманітність. Зокрема, необхідно спонукати органи державного управління розробляти політику в сфері культури для сприяння виробництву культурного, освітнього і наукового контенту і розвитку на місцевому рівні галузей культури, що відповідають мовним і культурним особливостям користувачів.

- б) Розробляти національні політику і законодавство, завдяки яким бібліотеки, архіви, музеї й інші установи культури в інформаційному суспільстві могли б повною мірою виконувати свою функцію постачальників контенту — у тому числі традиційних знань, — зокрема, забезпечуючи постійний доступ до записаної інформації.
- в) Підтримувати зусилля з розробки і застосуванню ІКТ для збереження природної і культурної спадщини, забезпечувати доступ до них як до живої частини сучасної культури. Для цього необхідно розробляти системи забезпечення постійного доступу до архівованої інформації в цифровій формі і мультимедійного контенту в цифрових сховищах, а також надавати підтримку архівам, зібраним предметів культури і бібліотекам як пам'яті людства.
- г) Розробляти і здійснювати політику, що сприяла б збереженню, зміцненню, повазі і розвитку різноманіття культур, знань і традицій корінних народів за допомогою створення різноманітного інформаційного контенту і застосування різних методів, у тому числі переведення в цифрову форму спадщини в сфері освіти, науки і культури.
- е) Підтримувати діяльність місцевих органів влади з розробки, перекладу й адаптації місцевого контенту, створенню архівів у цифровій формі і забезпеченню різноманітності форм цифрових і традиційних засобів масової інформації. Ці види діяльності можуть також сприяти зміцненню місцевих і корінних промислових і культурних галузей.
- ф) За допомогою доступу до послуг традиційних і цифрових засобів масової інформації забезпечити наявність контенту, актуального в культурному і лінгвістичному аспектах для людей, які складають інформаційне суспільство.
- г) За допомогою встановлення партнерських відносин між державним і приватним сектором прискорювати створення різноманітного місцевого і національного контенту, у тому числі доступного мовами користувачів, а також визнавати і підтримувати роботу на базі ІКТ у всіх сферах мислелства.
- д) Розширювати в системах формальної і неформальної освіти для всіх навчальні програми, що враховують гендерні аспекти, і підвищувати грамотність жінок у галузі зв'язку і ЗМІ, для того, щоб нарощувати потенціал дівчат і жінок стосовно розробки контенту ІКТ.

- і) Розвивати існуючий на місцях потенціал для розробки і поширення програмного забезпечення місцевими мовами, а також контенту, актуального для різних верств населення, у тому числі неписьмених, осіб з обмеженими можливостями, тих, що перебувають у несприятливих умовах, і вразливих груп населення, особливо в країнах, що розвиваються, і країнах з перехідною економікою.
- і) Надавати підтримку засобам масової інформації місцевих громад і підтримувати проекти, у яких поєднуються застосування традиційних ЗМІ і нових технологій в інтересах більш широкого використання місцевих мов, документування і збереження місцевої спадщини, включаючи ландшафтну і біологічну різноманітність, і як засоби, що забезпечують охолодження сільських, ізолюваних і кочових громад.
- к) Зміцнювати потенціал корінних народів з розвитку контенту їхніми рідними мовами.
- л) Співпрацювати з корінними народами і традиційними громадами, для того щоб в інформаційному суспільстві вони могли ефективніше застосовувати свої традиційні знання й одержувати від цього прибутки.
- м) Здійснювати обмін знаннями, досвідом і зразками найкращої практики, що стосуються політики й інструментів, спрямованих на сприяння культурній і мовній різноманітності на регіональному і субрегіональному рівнях. Цього можна домогтися шляхом створення, для сприяння з метою інтеграції зусиль регіональних і субрегіональних робочих груп з конкретних питань даного Плану дій.
- п) Проводити на регіональному рівні оцінку внеску ІКТ у культурний обмін та взаємодію і на підставі результатів цієї оцінки розробляти відповідні програми.
- о) Органи державного управління, у рамках партнерських відносин між державним і приватним секторами, повинні сприяти поширенню технологій і здійсненню програм НЮКР у таких сферах, як письмовий переклад, іконографія і послуги на базі мовного зв'язку, а також розвитку моделей необхідного апаратуного і різноманітного програмного забезпечення, у тому числі програмного забезпечення, розроблюваного окремими компаніями, програмного забезпечення з відкритими кодами і вільно розповсюджуваного програмного забезпечення, такого як стандартні набори символів, мовні коди, електронні словники, термінологічні довідники і тезауруси, багатомовні пошукові машини, інструменти машинного перекладу, інтернаціоналізовані найменування доменів, постачання контенту посиланнями, а також загального і прикладного програмного забезпечення.

С9. Засоби масової інформації

24. Засоби масової інформації — у своїх різних видах і різноманітні форми власності — як дієвий фактор відіграють істотну роль у розвитку інформаційного суспільства і визнані важливим виразником волі слова і плюралізму інформації.

- а) Заохочувати ЗМІ — друковані й електронні, а також нові види ЗМІ — до того, щоб вони і далі відігравали важливу роль в інформаційному суспільстві.
- б) Заохочувати розробку національного законодавства, що гарантує незалежність і плюралізм засобів масової інформації.
- в) Ужити належних заходів — не зазігаючи при цьому на волю слова — для боротьби з незаконним і незбитковим контентом у ЗМІ.
- г) Заохочувати професійних працівників засобів масової інформації в розвинутих країнах до встановлення партнерських відносин і створення мереж із засобами масової інформації в країнах, що розвиваються, особливо у сфері професійної підготовки.
- е) Підтримувати створення гармонійного і багатогранного образу жінки і чоловіка в засобах масової інформації.
- ф) Скорочувати існуючі на міжнародному рівні і ті, які позначаються на ЗМІ диспропорції, особливо щодо інфраструктури, технічних ресурсів і розвитку навичок і вмінь людей, використовуючи для цієї мети всі переваги, що надають для цього інструменти на базі ІКТ.
- г) Заохочувати традиційні засоби масової інформації до подолання розриву в знаннях і сприяння поширенню культурного контенту, особливо в сільських районах.

С10. Етичні аспекти інформаційного суспільства

25. Інформаційне суспільство повинне спиратися на загальновизнані цінності і піклуватися про загальне благо, а також запобігати зловживанням при використанні ІКТ.

- а) Вживати заходів для зміцнення світу і відстоювання таких основних цінностей, як воля, рівність, солідарність, терпимість, колективна відповідальність і дбайливе ставлення до природи.
- б) Усі зацікавлені сторони повинні повніше враховувати етичний аспект при застосуванні ІКТ.
- в) Усі учасники інформаційного суспільства повинні піклуватися про загальне благо, захищати недоторканність приватного життя й особистих даних, виконувати відповідні дії і вживати встановлених заходів для запобігання неналежному використанню ІКТ, такому як протиправні діяння та інші дії на ґрунті расизму, расової дискримінації, ксенофобії і пов'язаних з ними нетерпимості, ненависті, насильства, усіх форм жорстокого поводження з дітьми, включаючи педофілію і дитячу порнографію, а також торгівля людьми і їх експлуатація.

- d) Залучати відповідні зацікавлені сторони, насамперед учених, до продовження дослідження етичних аспектів ІКТ.

С11. Міжнародне і регіональне співробітництво

26. Міжнародне співробітництво всіх зацікавлених сторін має вирішальне значення для здійснення даного Плану дій і повинне зміцнюватися з метою сприяння реалізації універсального доступу і ліквідації розриву в цифрових технологіях, зокрема шляхом забезпечення спосібів реалізації.

- a) Органи державного управління країн, що розвиваються, повинні підвищувати відносний ступінь пріоритетності проєктів в галузі ІКТ у запитах щодо міжнародного співробітництва і надання допомоги по проєктах розвитку інфраструктури з боку розвинутих країн і міжнародних фінансових організацій.
- b) У контексті Глобального договору ООН і з опорою на Декларацію тисячоліття Організації Об'єднаних Націй створювати і розвивати партнерські відносини між державним і приватним секторами, приділяючи особливу увагу використанню ІКТ в інтересах розвитку.
- c) Запропонувати міжнародним і регіональним організаціям включати ІКТ в основні напрямки своїх робочих програм і надавати підтримку країнам, що розвиваються, та тим, що перебувають на різних рівнях розвитку, у складанні і реалізації національних планів дій, спрямованих на досягнення цілей, зазначених у Декларації принципів і даному Плану дій, з огляду при цьому на значимість регіональних ініціатив.

Д. Порядок денний цифрової солідарності

27. Метою Порядку денного цифрової солідарності є створення умов для мобілізації людських, фінансових і технологічних ресурсів, необхідних для включення всіх чоловіків і жінок в інформаційне суспільство, що формується. Життєво важливе значення для виконання цього Порядку денного має тісне співробітництво всіх зацікавлених сторін на національному, регіональному і міжнародному рівнях. Для подолання розриву в цифрових технологіях нам буде потрібно з більшою ефективністю використовувати існуючі підходи і механізми і повною мірою освоїти нові підходи і механізми, для того щоб забезпечувати фінансування розвитку інфраструктури, устаткування, нарощування потенціалу і створення контенту, необхідних для участі в інформаційному суспільстві.

Д1. Пріоритети і стратегії

- a) Національні електронні стратегії повинні складати невід'ємну частину національних планів у сфері розвитку, включаючи стратегії скорочення масштабів бідності.

- b) ІКТ повинні бути цілком включені в основні напрямки стратегій офіційної допомоги з метою розвитку (ОДР) за допомогою більш ефективного обміну інформацією і координації з донорами, а також за допомогою аналізу найкращої практики й уроків, засвоєних з досвіду застосування ІКТ у програмах у сфері розвитку, і обміну ними.

Д2. Мобілізація ресурсів

- a) Усі країни і міжнародні організації повинні працювати над створенням умов, сприятливих підвищенню доступності й ефективної мобілізації ресурсів для фінансового розвитку, як зазначено в Монтеррейському консенсусі.
- b) Розвинуті країни повинні вжити конкретних заходів для виконання своїх міжнародних зобов'язань із фінансування розвитку, включаючи ті, що містяться в Монтеррейському консенсусі, де до тих розвинутих країн, які ще цього не зробили, звернений наполегливий заклик ужити конкретних заходів для досягнення цільового рівня ОДР країнами, що розвиваються, складового 0,7 відсотка від їхнього валового національного продукту (ВНП), а також виділення найменш розвинутим країнам 0,15–0,20 відсотка ВНП розвинутих країн.
- c) Ми вітаємо ініціативи на користь країн, що розвиваються, тих, що страждають від непомірного боргового тягара, спрямовані на зменшення непоташеної заборгованості, і пропонуємо вжити подальших національних і міжнародних заходів у цьому напрямку. У тому числі у відповідних випадках анулювати борги й укладати інші домовленості. Особливу увагу варто приділяти розвитку ініціатив щодо бідних країн з великою заборгованістю. Ці ініціативи дозволять визволити більше ресурсів, що можуть використовуватися для фінансування проєктів у галузі ІКТ із метою розвитку.
- d) З огляду на потенціал ІКТ для цілей розвитку, ми далі закликаємо:
 - i) країни, що розвиваються, — активізувати свої зусилля із залучення великих приватних національних і іноземних інвестицій у ІКТ шляхом створення прозорого, стабільного, передбачуваного і сприятливого інвестиційного клімату;
 - ii) розвинуті країни і міжнародні фінансові організації — належним чином реагувати на стратегії і пріоритети ІКТ з метою розвитку, включаючи ІКТ у свої робочі програми і сприяти країнам, що розвиваються, і країнам з перехідною економікою в розробці і реалізації національних електронних стратегій. На підставі пріоритетів національних планів розвитку і здійснення вищевказаних зобов'язань розвинуті країни повинні збільшити зусилля, що докладаються ними, з надання більшого

обсягу фінансових ресурсів країнам, що розвиваються, для застосування ІКТ з метою розвитку;

iii) приватний сектор — робити свій внесок у реалізацію даного Порядку денного цифрової солідарності.

е) У своїх зусиллях з подолання розриву в цифрових технологіях нам варто сприяти, у межах нашої співпраці у сфері розвитку, надання технічної і фінансової допомоги, спрямованої на на-
рошення національного і регіонального потенціалу, передачі технологій на взаємопогоджуваних умовах, співробітництво за програмами НЮКР і обмінні ноу-хау.

f) Слід повною мірою використовувати всі існуючі фінансові механізми і при цьому завершити до кінця грудня 2004 року детальний аналіз їх відповідності до завдань із застосування ІКТ з метою розвитку. Цей аналіз повинен проводитися певною ціловою групою, що діє під егідою Генерального секретаря Організації Об'єднаних Націй, а його результати повинні бути представлені на розгляд у рамках другого етапу даної Зустрічі на вищому рівні. На основі результатів аналізу варто розглянути питання про вдосконалення і відновлення фінансових механізмів, у тому числі про ефективність, доцільність і створення добровільного фонду цифрової солідарності, згаданого в Декларації принципів.

г) Країнам варто розглянути питання про створення національних механізмів забезпечення універсального доступу в обслуговуваних недостатньою мірою сільських і міських районах з метою подолання розриву в цифрових технологіях.

Е. Подальші заходи і оцінка

28. Варто розробити реалістичну міжнародну систему оцінки і визначення (як якісного, так і кількісного) ефективності, використовуючи порівняльні статистичні показники і результати досліджень, для того щоб вести спостереження за виконанням завдань, досягненням цілей і контр-
рольних показників Плану дій, беручи до уваги національні особливості.

а) У співробітництві з кожною зацікавленою країною розробити і ввести зведений індекс показників розвитку ІКТ (цифрових можливостей). Його можна було б публікувати щорічно чи раз у два роки в Звіті про розвиток ІКТ. В індексі наводилися б статистичні дані, а в звіті представлялися аналітичні дослідження прийняті в них політики і результати її проведення за належно від національних особливостей, у тому числі дані гендерного аналізу.

б) Належні показники й орієнтири, у тому числі показники колективного доступу, повинні відображати величину розриву в цифрових технологіях як у національному, так і в міжнародному масштабі і забезпечувати його регулярну оцінку, для того щоб відслідковувати світові досягнення у використанні ІКТ для вирі-

шення погоджених на міжнародному рівні завдань, включаючи ті, котрі містяться в Декларації тисячоріччя.

с) Міжнародні і регіональні організації повинні проводити оцінку і на регулярній основі представляти доповіді про рівень універсального доступу ІКТ у різних країнах, для того щоб забезпечити створення рівних можливостей для розвитку секторів ІКТ у країнах, що розвиваються.

д) Варто розробити, враховуючи гендерну специфіку, показники із застосування ІКТ і потреби в них, а також визначити показники, що піддаються кількісному виміру, виконання з метою оцінки впливу фінансованих проєктів у сфері ІКТ на життя жінок і дівчат.

е) Підготувати і відкрити заснований на матеріалах, що надійшли як внески від усіх зацікавлених сторін, веб-сайт, присвячений зразкам найкращої практики й успішно проведених заходах, формат якого має бути чітким, доступним і наочним, відповідно до визначених на міжнародному рівні стандартів мережевої доступності. Веб-сайт можна було б періодично оновлювати і перетворювати його на засіб постійного обміну досвідом.

f) Усім країнам і регіонам варто розробити інструменти, необхідні для надання статистичної інформації з питань інформаційного суспільства, що включає базові показники й аналіз динаміки його ключових параметрів. Пріоритет варто надавати створенню погоджених і порівнянних на міжнародному рівні систем показників, враховуючи розбіжності в рівнях розвитку.

Ф. Готуючись до другого етапу ВЗРІС (Туніс)

29. Відповідно до резолюції 56/183 Генеральної Асамблеї і з урахуванням підсумків женецького етапу ВЗРІС варто провести в першій половині 2004 року підготовчі збори з метою аналізу тих віднесених до інформаційного суспільства питань, що будуть фігурувати як основні у рамках туніського етапу ВЗРІС, і ухвалити рішення щодо структури процесу підготовки до другого етапу. Відповідно до рішення, прийнятого даною Зустріччю на вищому рівні щодо її туніського етапу, на другому етапі ВЗРІС необхідно розглянути, зокрема, такі питання:

а) розробка відповідних заключних документів на підставі підсумків женецького етапу ВЗРІС, з метою консолідації процесу побудови глобального інформаційного суспільства, скорочення розриву в цифрових технологіях і перетворення його в цифрові можливості;

б) наступні заходи і реалізація Женецького плану дій на національному, регіональному і міжнародному рівнях, у тому числі в системі Організації Об'єднаних Націй, у рамках цілісного і погодженого підходу, що передбачає участь усіх відповідних зацікавлених сторін. Ці дії повинні проводитися, зокрема, у межах партнерських відносин між зацікавленими сторонами.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Українські джерела

1. Антонов А. В. Інформація: восприяття і помилання. — К.: Наук. думка, 1994. — 184 с.
2. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти. — Х.: УВС, 2000. — 368 с.
3. Баранов А. А., Брыжко В. М., Бзанов Ю. К. Защита персональных данных. — К.: Национальное агентство по вопросам информатизации при Президенте Украины, 1998. — 128 с.
4. Баранов А. А., Брыжко В. М., Бзанов Ю. К. Права человека и защита персональных данных. — К.: Государственный комитет связи и информатизации Украины, 2000. — 280 с.
5. Безяков К. І. Деякі питання щодо формування реформи інформаційного законодавства України // Систематизація законодавства в Україні: проблеми теорії і практики: Матеріали міжнародної науково-практичної конференції. — К.: Інститут законодавства Верховної Ради України, 1999. — С. 253.
6. Бенедисюк И. Использование информации с ограниченным доступом // Бизнес. Бухгалтерия. — 1999. — № 37. — С. 87—89.
7. Бережний Є. О. Законодавчі та нормативні акти, прийняті після проголошення незалежності України, які пов'язані зі створенням, інтеграцією та використанням інформаційних ресурсів // Інформація. Ринок. — 1996. — № 4.
8. Брыжко В. М., Орехов А. А., Гильченко О. Н., Цимбалюк В. С. Е-будущее и информационное право / Под. ред. Р. А. Каложного и Н. Я. Швеца. — К.: Интергал, 2002.
9. Булаков А. С. Правовая информатизация и обеспечение доступа к информации // http://www.rainmedia.ru/conf.asp?db_po=279.
10. Гавловський В. Д. Інформаційне законодавство України: від інкорпорації до кодіфікації // Систематизація законодавства в Україні: проблеми теорії і практики: Матеріали міжнародної науково-практичної конференції. — К.: Інститут законодавства Верховної Ради України, 1999. — С. 289.
11. Гавловський В. Д., Грищенко В. І., Ковпак Р. Д., Цимбалюк В. С. Україна на шляху формування інформаційного суспільства: проблеми щодо формування інформаційного законодавства // Проблеми впровадження інформаційних технологій в економіці та бізнесі: Матеріали другої міжнародної науково-практичної конференції. 3—5 травня 2001 року. — Ірпінь: АПСУ, 2001.
12. Гавловський В. Д., Кашпур В., Цимбалюк В. С. Державно-правове регулювання соціальних інформаційних відносин (укр. і англ. мова) // Українське право. — 1998. — № 1. — С. 173—176.
13. Гавловський В., Швель М., Каложний Р., Цимбалюк В. С. Інформаційне законодавство України: концептуальні основи формування // Право України. — 2001. — № 7. — С. 88—81.
14. Голобуцький О. П., Шевчук О. Б. Електронний уряд. — К.: ЗАТ «Атлант UMS», 2002. — 173 с.
15. Гонимж Я., Гиндюк Н. Свобода інформації та виконавча гілка влади: Правові норми. Інституції. Процедури. — К.: Міленіум, 2002. — 240 с.
16. Демкова М., Колішуко І. Електронне урядування: світовий досвід та українські реалії // Електронне урядування: окремі аспекти становлення. — К., 2003.
17. Закони та практика ЗМІ в Україні / Харківська правозахисна група; худож.-оформлювач І. Гаврилюк. — Харків: Фоліо, 2002. — 128 с.
18. Захаров Є., Рапп І. Аналіз практики доступу до урядової інформації // Додаток до інформаційно-аналітичного бюлетеня «Права Людини». — 2002. — № 1 (13), січень-березень.
19. Захаров Є., Рапп І. Свобода доступу до урядової інформації // Додаток до інформаційно-аналітичного бюлетеня «Права Людини». — 2000. — № 4 (8), жовтень-грудень.
20. Ібраїмова І. М. Інформація та/або комунікація. Обираючи політику. — Командор. — К.: Вид-во УАДУ, 2001.
21. Інформатизація та відкритість влади як засоби демократизації суспільства: Матеріали «Круглого столу». — К.: Альтерпрес, 2003. — 160 с.
22. Інформатизація, право, управління (організаційно-правові питання): Монографія / Каложний Р. А., Кручан О. Д., Гавловський В. Д., Гуцалюк М. В., Швель М. Я., Цимбалюк В. С. / За заг. ред. М. Я. Швеца, О. Д. Кручана. — К.: НДЦ правової інформатики АПРНУ, 2002. — 191 с.
23. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики: Монографія / Каложний Р. А., Шамрай В. О., Гавловський В. Д., Гуцалюк М. В., Швель М. Я., Цимбалюк В. С., Ялишин Ю. В., Ласовський А. С. / За ред. Р. А. Каложного та В. О. Шамрая. — К.: АПСУ України, 2002. — 296 с.
24. Інформаційне право та інформаційна безпека / Сучасний стан, поняття та визначення змістовної частини, інкорпорація нормативних актів з правових питань у сфері інформації та її захисту. Наукове видання / Гавловський В. Д., Коваленко О. І., Гіжевський І. К., Цимбалюк В. С. та ін. / За заг. ред. Р. Каложного та В. Влонова. — Київ: Донецьк: Донецький інститут внутрішніх справ МВС України. Інститут економіки і права «КРОК», 2001. — 230 с.
25. Інформаційне суспільство. Дефініції... / Брыжко В. М., Орехов А. А., Цимбалюк В. С., Кальченко О. Н., Чорнобров А. Н. / За ред. Р. А. Каложного і М. Я. Швеца. — К.: Интергал, 2002. — 220 с.
26. Каложний Р., Гавловський В., Гуцалюк М., Цимбалюк В. Питання концепції реформи інформаційного законодавства України // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — К.: НТУУ «КПІ», 2000. — С. 17—21.
27. Каложний Р., Гавловський В., Гуцалюк М., Цимбалюк В. Інформаційному суспільству України інформаційне законодавство (щодо питань реформування законодавства у сфері суспільних інформаційних відносин) // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — К.: НТУУ «КПІ». — 2001. — № 2. — С. 7—11.
28. Каложний Р., Гавловський В., Цимбалюк В. Питання кодіфікації законодавства України про інформацію з обмеженим доступом // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — К.: НТУУ «КПІ». — 2001. — № 3. — С. 35—38.
29. Концепція реформування законодавства України в сфері інформаційних відносин. Затверджена рішенням Урядової комісії з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади (Протокол № 7 від 6.10.2000, м. Київ).
30. Котляр Д. Правова природа та підходи до регулювання комерційної таємниці // «Часопис ПАРЛАМЕНТУ», — 2004. — № 3. — С. 34—46.
31. Лисинський В., Тацій В. До питання реформування законодавства України у сфері суспільних інформаційних відносин // Вісник Академії правових наук. — 2000. — № 4 (23). — С. 298—302.
32. Литвиненко О. В., Паламарчук В. М., Янішевський С. О., Жигалюк В. В., Сахаренко О. В. Інформаційна відкритість української влади. Аналітична доповідь, Національний інститут стратегічних досліджень. — К., 2002.
33. Міжнародні стандарти забезпечення свободи слова: Збірник публікацій міжнародної організації «Артикль 19». — К.: Міленіум, 2003.
34. Ожєвин М. Інформаційна безпека України // Президентський вісник — 2000. — № 10. — С. 8.

35. Онопчук І. Ю. Окремі проблеми міжнародного та національного інформаційного права // Проблеми гармонізації законодавства України з міжнародним правом. — К., 1998. — С. 312—316.

36. Осауленко О. Г. Інформаційне забезпечення державного управління сталим розвитком. — К., 2001. — 72 с.

37. Пазюк А. В. Захист прав громадян у зв'язку з обробкою персональних даних у правоохоронній діяльності: європейські стандарти і Україна. — К.: МГО Прайвсі Юкрейні, 2001. — 258 с.

38. Пазюк А. В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти. — К.: МГО Прайвсі Юкрейні, 2000. — 88 с.

39. Писемницький А. А. Інформаційне право України (законодавство, коментарі, перспективи). — Х.: АО «Бізнес Інформ», 1996. — 208 с.

40. Питання відкритості влади: Програма співробітництва парламенту України. — К., 2002.

41. Питання концепції реформування інформаційного законодавства України. / Р. Каложний, В. Павловський, В. Цимбалюк, М. Гуцалюк. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — К.: НТУУ «КПІ». Міністерство науки України, СБУ, 2000.

42. Почепцов Г. Г. Інформаційне суспільство, інформаційний простір, інформаційна політика: чи існують вони в Україні? // День. — 2001. — 13 квіт. — С. 6—7.

43. Право на приватність: conditio sine qua non / Харківська правозахисна група; худ.-оформлювач О. Герчук. — Харків: Фолио, 2003. — 216 с.

44. Правовий самозахист журналістів: Практичний посібник з юридичного захисту працівників ЗМІ в Україні. — К.: Геопрінт, 2003. — 106 с.

45. Практика Європейського суду та Європейської комісії з прав людини при застосуванні статті 10 Європейської конвенції з прав людини. Сорок років юриспруденції Суду та Комісії. 1959—1999 // Українська правнича фундація, 1999. — № 6.

46. Романов Р. В. Послужка досконалих моделей правового регулювання доступу до інформації // Свобода висловлювань і приватність (СвП), № 4 (8), жовтень — грудень, Харків.

47. Світова доповідь ООН з питань державного сектора 2003: Е-уряд на перехресті. / Пер. з англ. (неоф.) — К.: СПД Гошка Ніна Іванівна, 2004. — 258 с.

48. Свобода висловлювань в Україні — 2002. Огляд повідомлень про конфлікти в інформаційній сфері України у 2002 році / Харківська правозахисна група, худ.-оформлювач Б. Є. Захаров. — Харків: Фолио, 2003. — 320 с.

49. Свобода інформації, прозорість, електронне врядування: погляд промисловця суспільства (аналітичні доповіді, збірка перекладів документів) / За ред. к.ю.н. А. В. Пазюка. — К.: МГО «Прайвсі Юкрейні», 2004. — 206 с.

50. Суспільство, засоби масової інформації, влада: свобода слова і цензура в Україні. — К.: Парламентське видавництво, 2003.

51. Субота Н. Конфіденційна інформація, що є власністю держави: вид інформації з обмеженням доступу чи засіб обмеження доступу до відкритої інформації? // Юридичний журнал. — 2003. — № 9 (15).

52. Цимбалюк В. С., Павловський В. Д. Інформаційне право: Навчально-методичний комплекс. — К.: Інститут економіки, управління та господарського права. — 1999. — 183 с.

53. Швейц М., Каложний Р., Павловський В., Цимбалюк В. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — Київ: НТУУ «КПІ», — 2002 — № 4. — С. 10—18.

54. Швейц М. Я., Каложний Р. А., Павловський В. Д., Цимбалюк В. М., Цимбалюк В. С. Основи інформаційного права та концепції формування системи інформаційного законодавства України // Наукові записки. Том 19, Частина 1. Спеціальний випуск. — К.: Національний університет «Києво-Могилянська академія», 2001. — С. 168—172.

55. Subota N. M. Access of Printed Mass Media to State Information. // «The Ukrainian journal of business law» No. 7 July 2003.

Зарубіжні джерела

56. Аблеев Р. Ф. Философия информационной цивилизации. — М.: Владос, 1994. — 336 с.

57. Абдуллин А. И. Правовая охрана баз данных в Европейском Союзе // Журнал международного частного права. — 1997. — № 2.

58. Агапов А. Б. Основы федерального информационного права России. — М., 1995.

59. Батурин Ю. М. Проблемы компьютерного права. — М., 1991.

60. Венгеров А. Б. Право и информация в условиях автоматизации управления (теоретические вопросы). — М., 1978.

61. Вихорев С. В. Что есть что в информационном праве // <http://www.infotecs.pl/etc/New-publications/PILOSOF.html>.

62. Волокитин А. В., Копылов В. А. Информационная безопасность и информационное законодательство // Сб. НИИ. Сер. 1. — 1996. — № 7.

63. Волчинская Е. К. Проблемы законодательного регулирования доступа к информации // http://www.rakmedia.ru/conf/ar?ob_lo=303.

64. Ефремов А. А. Понятие и виды конфиденциальной информации // <http://www.russia-law.net/law/doc/a90.html>.

65. Дайсон Естер. Життя за доби Інтернету. — К.: Видавничий дім «Альтернативи», 2002. — 344 с.

66. Кастельс М. Информационная эпоха: экономика, общество и культура. — М.: ГУ ВШЭ, 2000. — 608 с.

67. Кьюндер Міхель, Нойн Андреас. Інформаційне право. — Мюнхен: Бек, 2002.

68. Копылов В. А. Информационное право: Учебник. — 2-е изд., перераб. и доп. — М.: Юристъ, 2002. — 512 с.

69. Копылов В. А. Информация как объект правового регулирования // Сб. НИИ. Сер. 1. — 1996. — № 8.

70. Кузнецов В. К. Информационное право. — Новосибирск: СибАГС, 2001. — 128 с.

71. Кумишский С. П. Основы организации информационной деятельности в сфере управления: Навч. посіб. — К.: МАУП, 2002. — 224 с.

72. Куприянов А. Интернет и право // <http://www.gessialaw.net/law/doc/a72.htm#ONE>.

73. Рассолов М. М. Управление, информация и право. — М., 1983.

74. Рассолов М. М. Информационное право. — М., 1999.

75. Сергиенко Л. А. Правовая защита персональных данных. Цели и принципы правового регулирования // Проблемы информатизации. — 1995. — № 1.

76. Терещенко Л. К. Информация в обществе: правовой аспект // Журнал российского права. — 1998. — № 4/5.

77. Урсел А. Д. Информатизация. Методологические аспекты. — М., 1965.

78. Шиверский А. А. Защита информации: проблемы теории и практики. — М.: Юристъ, 1996.

79. Vanisat, David, Freedom of Information and Access to Government Records Around the World. Privacy International, March 2001.

80. Vege, Achim Improved rules on public access to documents? The discussion on a regulation under Art 255 ECT, Stockholm University, Master of European Law, 2001.

81. Edes, Bart W., Role of Public Administration in Providing Information Offices and Citizens Information Services, presentation at the EIPA Seminar on «An Efficient, Transparent Government and the Rights of Citizens to Information», 29-30 May, 2000, Maastricht.

82. Gotszulska, Teresa, Prawo do informacji I zasady jawności administracyjnej (Право на інформацію і принципи адміністративної відкритості). — Краків, Zakamcze, 1999. — С. 27—28.

83. Information Technology as An Instrument of Public Management Reform: A Study of Five OECD Countries, OECD. — Paris, 1998.

84. Kapitais, Edvins, Public Sector Information in Latvia: Processing, Availability and Use.

Наукове видання

Автори-упорядники: *М. С. Демкова, М. В. Фігель*

**ДОСТУП ДО ІНФОРМАЦІЇ
ТА ЕЛЕКТРОННЕ УРЯДУВАННЯ**

Відповідальний редактор: *І.Б. Коліушко*

Художній редактор: *Т. Мосієнко*
Літературний редактор, коректор *Л. Неділько*
Верстка М.Неділько

Підписано до друку Формат 60х84/16
Папір офсет № 1. Гарнітура Таймс. Друк офсетний.

Видавництво «Факт»
Наклад прим. Зам. №