ПРАВОВА ІНФОРМАТИКА

№ 1 (9) / 2006

У номері:

НАУКОВИЙ ЖУРНАЛ
З ПИТАНЬ ПРАВОВОЇ ІНФОРМАТИКИ,
ІНФОРМАЦІЙНОГО ПРАВА
ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

До відома авторів

Постановою Президії ВАК України від 08.06.2005 р. № 2-05/5 журнал “Правова інформатика” включено до переліку наукових фахових видань з юридичних наук.

Редакційна колегія журналу звертає увагу авторів статей, які подаються на розгляд та відбір для друку, на необхідність дотримання правил, встановлених Постановою Президії Вищої атестаційної комісії України від 15.01.2003 р. № 7-05/1 *“Про підвищення вимог до фахових видань, внесених до переліків ВАК України”.*

У зв’язку із зазначеним необхідно:

1) подавати статтю, виготовлену у друкарський спосіб, та її електронний варіант (структура та зміст якого повністю відповідає друкованому варіанту) у вигляді файла:

– у текстовому редакторі – Word, шрифт – Times New Roman, з розширенням – .doc, кегль – 12;
– відстань між рядками – 1 інтервал;
– параметри сторінки: формат А4, розташування тексту (таблиці) книжне, береги поля (верхній, нижній, лівий і правий краї) – 20 мм.

Стаття повинна передбачати наявність таких структурних елементів:

- *УДК;*
- *ім’я та прізвище, науковий ступінь, вчене звання автора;*
- *назва статті;*
- *анотація (2-3 речення);*
- *розв’язання проблеми:*
  - *постановка проблеми в загальному вигляді та її зв’язок із важливими науковими чи практичними завданнями;*
  - *аналіз останніх досліджень, в яких започатковано розв’язання даної проблеми і на які спирається автор, виділення не вирішених раніше частин загальної проблеми, котрим присвячується стаття;*
  - *формування цілей статті (постановка завдання);*
  - *виклад основного матеріалу з обґрунтуванням отриманих результатів;*
  - *висновки з даного дослідження і перспективи подальших розвідок;*
- *використана література (за умов додержання державних стандартів);*
- *підпис, адреса, телефон автора;*

2) подавати письмовий експертний висновок на статтю, підписану особою, яка має науковий ступінь. Висновок повинен висвітлювати такі питання:

- *актуальність теми;*
- *новизна та обґрунтованість одержаних висновків;*
- *наукова (практична) цінність результатів.*

НАУКОВО-ДОСЛІДНИЙ ЦЕНТР ПРАВОВОЇ ІНФОРМАТИКИ
АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ

ІНСТИТУТ ЗАКОНОДАВСТВА ВЕРХОВНОЇ РАДИ УКРАЇНИ

ПРАВОВА ІНФОРМАТИКА

ЗАСНОВАНИЙ У ГРУДНІ 2003 РОКУ | НАУКОВИЙ ЖУРНАЛ З ПИТАНЬ ПРАВОВОЇ ІНФОРМАТИКИ, ІНФОРМАЦІЙНОГО ПРАВА ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ | ВИХОДИТЬ ЩОКВАРТАЛЬНО

№ 1 (9)

січень – березень
2006

Засновники:

Науково-дослідний центр правової інформатики Академії правових наук України,

Інститут законодавства Верховної Ради України

Редакція:

01032, м. Київ-32,
вул. Саксаганського, 110-В

Тел.: 234-94-56, 246-48-58
Факс: 234-55-60
e-mail: *bib_rada@i.kiev.ua*

Виготовлено:

Київська філія державного підприємства Науково-дослідного економічного інституту Міністерства економіки України

З М І С Т

==========

Рекомендовано до друку Вченою радою НДЦПІ АПрН України, протокол № 12 від 19 грудня 2005 р.

==========

Створення оригінал-макета – В. Брижко. Редактор – А. Москаленко.
Формат 70 х 108/16. Папір офсетний. Гарнітура Times.
Офсетний друк. Ум. друк арк. 8,6. Обл. вид. арк. 8,6.
Тираж: 100 прим. – паперовий варіант, 5000 прим. – електронний варіант на CD-ROM.

==========

УДК 004:34(075)

М. ШВЕЦЬ, *доктор економічних наук, професор,*
член-кореспондент Академії правових наук України,
О. ГЛАДКІВСЬКА, *кандидат фізико-математичних наук,*
В. ЦИМБАЛЮК, *кандидат юридичних наук*

ПРОБЛЕМИ ВЗАЄМОВІДНОШЕННЯ ПРАВОВОЇ ІНФОРМАТИКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

***Анотація**: У роботі висвітлюються окремі питання сутності і змісту правової інформатики та інформаційної безпеки в контексті їх взаємозв’язку.*

Питання взаємозв’язку правової інформатики та інформаційної безпеки представляє інтерес з огляду на те, що інформаційна безпека як наукове явище формується сьогодні на рівні міжгалузевого комплексного інституту (комплексної наукової дисципліни), який утворився на межі поєднання технічних і гуманітарних наук: правової інформатики, інформаційного права та тектології (теорії організації соціальних систем) [1].

Питання дослідження сутності та змісту правової інформатики є актуальними і розглядаються в роботах [2-5] українських і [6, 7] російських учених.

Одним з перших вважається визначення, запропоноване професором Н.С. Польовим [6] і підтримане іншим ученим – доктором юридичних наук, професором О.О. Гавриловим [7]. Воно сформульоване, виходячи зі змісту провідних інститутів та завдань, які ставляться перед інформатикою щодо правової сфери (юридичної діяльності). ***Правова інформатика** – це міждисциплінарна галузь знання про закономірності й особливості інформаційних процесів у сфері юридичної діяльності, про їх автоматизацію, про принципи побудови і методики використання автоматизованих інформаційних систем, які створюються для удосконалення і підвищення ефективності юридичної діяльності й вирішення правових задач на базі комплексного використання теорії та методології правових наук, засобів і методів математики, інформатики і логіки.*

Основними інститутами правової інформатики (за ознаками предметів дослідження) є: дослідження юридичної діяльності з метою автоматизації її через впровадження та використанням сучасних інформаційних технологій; принципи побудови і методики використання автоматизованих інформаційних систем у галузі держави і права, створюваних для удосконалення і підвищення ефективності управлінської діяльності, рішення інших правових завдань на базі засобів і методів кібернетики та інших наук, використання досягнень яких дає можливість розв’язувати проблемні питання в галузі держави і права.

Згідно з даним визначенням, завдання правової інформатики можна подати таким чином:

- активна участь у забезпеченні формування правової держави, реалізації принципів гласності, доступу кожного члена суспільства до всієї сукупності нормативних правових актів, вільного одержання правової інформації в потрібний час, у потрібному місці й у потрібній, особливо в електронній (комп’ютерній, електронно-цифровій), формі;
- розробка наукових і практичних основ впровадження автоматизованих робочих місць юристів, інтелектуальних і консультаційних систем юридичної спрямованості на

основі комп’ютерних інформаційних ресурсів, засобів, систем, сховищ даних;

- суспільна інтелектуалізація юридичної роботи установ і органів, підвищення продуктивності індивідуальної та колективної праці та інформаційної культури правотворчості, правозастосування та правоосвітньої діяльності.

В аспекті організації правоосвітньої діяльності можна виділити такі завдання правової інформатики:

- подання системи знань щодо сутності та змісту правової інформатики як науки та практики інформатизації юридичної сфери;
- створення та розвиток автоматизованих навчальних систем для підготовки юристів на основі комп’ютерних засобів;
- розробка теоретичних і методичних проблем підготовки та перепідготовки юридичних кадрів з використанням комп’ютерних систем та мереж, у тому числі на основі комп’ютерних технологій дистанційного навчання.

На наш погляд, сучасну практичну сутність правової інформатики найбільш точно відображає таке формулювання: *“Правова інформатика – це наукова галузь, що вивчає закономірності інформаційних процесів, проблеми створення, впровадження й ефективного функціонування комп’ютеризованих систем правової інформації і вироблення рішень. Інакше кажучи – це галузь дослідження проблем системної інформатизації законотворчої, нормотворчої, правозастосовної, правоохоронної, судової та правоосвітньої діяльності”* [5].

Виходячи із зазначених міркувань та з позицій функціонального підходу визначення правової інформатики можна подати так: ***Правова інформатика – це комплексна (соціотехнічна) наукова галузь у складі правознавства, що вивчає закономірності суспільних інформаційних процесів для вирішення проблем створення, впровадження, ефективного функціонування та розвитку комп’ютерних систем правової інформації з метою забезпечення прискореного вироблення і прийняття ефективних та правомірних рішень.***

З точки зору системно-функціонально-прикладного підходу визначення правової інформатики можна трактувати ширше, з прив’язкою до напряму досліджень прикладної інформатики: ***Правова інформатика – це галузь прикладної інформатики: прикладних досліджень та системи передачі знань щодо проблем системної інформатизації правотворчості, правозастосування та правоосвітньої діяльності.***

В останньому формулюванні ознака правової інформатики – соціотехнічність (що вжита у попередньому формулюванні) – трансформована в ширше означений термін щодо об‘єкта дослідження – інформатизацію.

На рівні методології можна зазначити, що, як і деякі інші комплексні галузі соціотехнічних знань, правова інформатика умовно ділиться на загальну і особливу частини.

До загальної частини можна віднести такі інститути:

- теоретико-методологічні питання щодо визначення сутності та змісту предмета наукової дисципліни;
- формування правової інформатики як напряму наукових досліджень у складі юридичних наук та її зв‘язок з іншими науками;
- формування власної історії, методології, адаптації методів, засобів, способів, принципів кібернетики та наук кібернетичного циклу до потреб інформатизації різних сфер суспільства;

• визначення задач та шляхів їх вирішення у контексті проблем створення загальнонаціональної комп‘ютерної системи правової інформації;

• питання формування засад організаційно-технічного забезпечення державної політики інформатизації правової, державно-управлінської, політичної систем;

• вирішення проблем формування єдиного інформаційного простору правової сфери;

• класифікація та структуризація різних видів правової інформації для формування різних систем знань тощо.

До особливої частини правової інформатики можна віднести інститути щодо формування системи знань про шляхи і завдання впровадження та розвитку комп'ютерних технологій у різних напрямах державно-правової сфери правотворчості, правозастосування та у правоосвітній діяльності [3]. У даний час уже чітко окреслилися такі особливі інститути правової інформатики:

а) інформатизація правотворчості, що включає дві складові:

- інформатизація законотворчого процесу;
- інформатизація правотворчого процесу в різних органах державного управління (органах державної виконавчої влади та органах місцевого самоврядування);

б) інформатизація правозастосування, яка включає такі умовні складові:

- інформатизація правоохоронної діяльності;
- інформатизація правозахисної діяльності;
- інформатизація судової діяльності (судова інформатика);
- інформатизація виборчих процесів та референдумів в Україні;

в) інформатизація кримінологічного циклу, яка включає:

- інформатизацію кримінологічних досліджень (кримінологічна інформатика);
- інформатизацію у криміналістиці та судовій експертизі (криміналістична інформатика);
- інформатизацію оперативно-розшукової діяльності (оперативно-розшукова інформатика) та інші.

У порядку визначення перспектив подальшого розвитку правової інформатики як наукового напряму можна зазначити, що в кожній галузі юридичної науки має створюватися інформаційна модель відповідного об’єкта пізнання, що припускає активне використання методів і засобів, які розроблені чи розробляються в теоретичній інформатиці та різних її прикладних галузях.

Так, при розробленні автоматизованих інформаційно-пошукових систем стосовно законодавства створюються класифікатори нормативно-правових актів, через які реалізуються ознаки галузевих юридичних наук (цивільне право, адміністративне право та ін.). Як свідчить практика створення комп’ютерних систем правової інформації, правова інформатика поставила перед теорією права завдання щодо напрацювання єдиного стандарту класифікації галузей законодавства з екстраполяцією на галузі правової науки. Нині в різних органах державної влади існує декілька класифікацій які за структуризацією не рідко виключають одна одну. За таких умов говорити про створення єдиної загальнодержавної системи правової інформації складно.

Це далеко не повний перелік уже визначених проблем правової інформатики. Але це свідчить, що незважаючи на відносно короткий термін свого існування, правова інформатика домоглася істотних успіхів у реалізації державної політики інформатизації правової сфери України.

Про розуміння в нашій країні на державному рівні необхідності якісного наукового забезпечення інформатизації правової сфери, а також координації наукових досліджень свідчить і те, що, за ініціативою Академії правових наук України у її складі постановою

Кабінету Міністрів України від 21 червня 2001 року № 671 створено Науково-дослідний центр правової інформатики (НДЦПІ) на правах інституту.

Основні розробки НДЦПІ спрямовані на фундаментальні та прикладні дослідження проблем правової інформатики, реалізацію Національної програми інформатизації в Україні та Національної програми правової освіти в Україні, зокрема, на дослідження, розроблення і розвиток інтегрованої комп’ютерної системи інформаційно-аналітичного забезпечення правотворчості, правозастосування та правоосвітньої діяльності.

Важливим і актуальним напрямом законодавчої роботи у сфері інформації та інформатизації залишається об’єднання державних і недержавних інформаційних ресурсів, мереж і систем у єдину загальнодержавну систему національних інформаційних ресурсів, у тому числі формування державної системи правової інформації як на загальнодержавному, так і на місцевому рівнях. Базовим і найбільш важливим елементом такої державної системи правової інформації могла б стати розроблена Науково-дослідним центром правової інформатики Академії правових наук України і впроваджена в діяльність багатьох державних інституцій електронна “Бібліотека баз даних і знань у галузі держави і права” (див. [8]). Так, створена у її складі інформаційно-пошукова система “Законодавство України”, яка щоденно підтримується в актуальному стані, є єдиною державною системою нормативно-правової інформації й містить понад 170 тисяч документів. Ця система встановлена і постійно функціонує більш як на 2 тисячах комп’ютеризованих робочих місцях у Верховній Раді України та понад 100 робочих місцях в інститутах Академії правових наук України. Крім того, щодоби за допомогою Інтернет системою користуються близько 5 тисяч абонентів в Україні та за її межами. Нею користуються близько 800 обласних, районних та міських рад тощо.

Для обміну думками, досягненнями в науково-дослідній, дослідно-конструкторській роботі та освітній діяльності з проблем правової інформатики у 2003 році був заснований фаховий журнал під назвою “Правова інформатика”.

У становленні і розвитку теорії та практики правової інформатики в Україні значну роль відіграють вчені, які працюють у Національній академії внутрішніх справ України, у Міжвідомчому науково-дослідному центрі з проблем боротьби з організованою злочинністю, у Науково-дослідному центрі з проблем оподаткування Національної академії державної податкової служби України, фахівці Управління комп’ютеризованих систем Апарату Верховної Ради України, Управління інформаційних технологій Верховного Суду України та ряду інших державних органів, а також ряду недержавних організацій.

Таким чином, правова інформатика тісно пов’язана зі стратегіями інформаційного суспільства.

Нормативно-правовий аспект інформаційної безпеки досліджено, наприклад, в [1, 2]. У роботі [1] на основі проведеного системно-структурного правового аналізу дається узагальнене визначення категорії “інформаційна безпека” як соціального явища та правового чинника суспільних інформаційних відносин. *Інформаційна безпека в умовах інформатизації України (формування інформаційного суспільства)* – це суспільні інформаційні відносини щодо створення і підтримання в належному стані режиму нормального функціонування відповідної автоматизованої (комп’ютеризованої) інформаційної системи, систем телекомунікації; комплекс організаційних, правових та інженерно-технологічних (технічних та програмно-математичних) заходів щодо охорони, захисту, запобігання і подолання природних, техногенних і соціогенних загроз,

реалізація яких може порушити чи припинити життєдіяльність конкретної соціотехнічної інформаційної системи.

Як вказано в аналітичному огляді [9], в українському законодавстві на сьогодні термін “інформаційна безпека” однозначно не визначено (в поданих законопроектах пропонується визначити як цей термін, так і термін “інформаційна безпека телекомунікацій”). Інформаційну безпеку можна розуміти, з одного боку, як безпосередньо захист інформації, і особливо – захист таємної, комерційної інформації, інформації з обмеженим доступом, персональних даних тощо, з іншого – як захист інформаційних систем, які фактично є засобом передачі інформації. У контексті інформаційно-комунікаційних технологій інформаційна безпека має три основні складові: конфіденційність (захист інформації від несанкціонованого доступу), цілісність (захист точності і повноти інформації) і доступність (своєчасне забезпечення доступу до інформації). Згідно з [2] інформаційна безпека – це стан захищеності людини, суспільства і держави, за якого забезпечуються охорона і захист від інформаційних впливів, небажаних наслідків використання інформаційних продуктів за інформаційних технологій. Під інформаційною війною розуміються дії, розпочаті для досягнення інформаційної переваги шляхом завдання збитків інформації, інформаційним процесам і системам супротивника при одночасному захисті власної інформації та інформаційних процесів [10].

За роки незалежності в нашій країні сформовано практично нове законодавство у сфері інформації та інформатизації. Законодавчі норми в цій сфері суттєво впливають на законодавче урегулювання відносин між громадянами і державою, між громадянами і комерційними структурами тощо, тобто інформаційні відносини є, з одного боку, зовнішнім проявом будь-яких відносин у житті країни та її громадян, з іншого – є основою, на якій вибудовується законодавство, що регулює суспільні відносини, в інших сферах. У свою чергу процеси розвитку інформації та процеси розвитку інформатизації настільки тісно пов’язані між собою, що неможливо уявити загальну картину побудови інформаційного суспільства в державі без відповідного рівня розвитку інформатизації. У роботах [2, 3, 9] аналізується законодавство України у сфері інформації та інформатизації, зокрема, те, яке стосується інформаційної безпеки.

Як випливає із аналітичного огляду [9], окремі аспекти формування законодавства України у сфері інформації та інформатизації залишаються неврегульованими на законодавчому рівні, а саме:

- забезпечення права громадян на вільний доступ до інформації;
- забезпечення захисту персональних даних;
- законодавче врегулювання питань інформаційної безпеки;
- законодавче визначення правил і умов функціонування національного ринку інформаційної продукції та інтеграції його у світовий інформаційний ринок;
- визначення правових аспектів регулювання Інтернет.

Говорячи про інформаційну безпеку, не можна не звернути увагу на безпеку персональної інформації кожного суспільства. Питанням забезпечення *захисту персональних даних* присвячені роботи [11,12]. Розвиток міжнародно-правової, економічної, фінансової, банківської, культурної, правоохоронної та інших форм співробітництва, що передбачає вільний рух інформаційних ресурсів щодо товарів, капіталів і послуг за умов використання інформаційно-комп’ютерних технологій та телекомунікаційних мереж, збільшення потоків персональних даних і підтримання суверенітету держави визначають об’єктивну необхідність захисту прав людини та основних свобод у сфері захисту персональних даних.

У провідних країнах світу спостерігаються такі загальні тенденції:

- формується інфраструктура щодо політичних, соціально-економічних, науково-технічних та технологічних засобів для вирішення проблеми захисту персональних даних;
- створюється та удосконалюється спеціальна законодавча база та правовий механізм організаційного забезпечення процесів у сфері захисту персональних даних;
- організуються спеціальні державні інститути уповноважених для нагляду і контролю за дотриманням прав у сфері захисту персональних даних.

Тому, необхідною важливою передумовою входження України повноправним членом до Європейського Співтовариства та світового інформаційно-комунікаційного середовища є гармонізація законодавчого та нормативно-організаційного забезпечення країни із відповідними Конвенціями та Директивами, що визначають європейське уявлення про права людини та основні свободи у сфері захисту персональних даних в умовах формування інформаційного суспільства.

Зазначене потребує підписання Україною Конвенції Ради Європи № 108, приєднання до Директиви 95/46/ЄС Європейського парламенту та Ради Європейського Союзу, законодавчого визначення загальних правил і умов у сфері захисту персональних даних (прийняття спеціального базового закону) та створення єдиного організаційно-правового механізму захисту персональних даних в Україні. Виходячи з рекомендацій Ради Європи та Європейського Союзу, позитивної практики провідних країн світу щодо секторального регулювання інформаційних відносин у сфері захисту персональних даних, вважається за необхідне рекомендувати розробку та прийняття у міністерствах та відомствах Кодексів практики/поведінки, які у наступному мають отримати статус галузевих нормативно-правових актів.

Актуальною проблемою в законодавчому плані залишається врегулювання питань інформаційної безпеки. Інформаційна сфера в нинішніх умовах є суттєвим чинником впливу на життя суспільства, його політичної, соціально-економічної, оборонної сторін і з огляду на це виключно важливими є питання, пов’язані з інформаційною безпекою, захищеністю національних інтересів в інформаційній сфері. Не можна не враховувати й права та інтереси громадянина в інформаційній сфері, які пов’язані, з одного боку, із забезпеченням реалізації конституційних прав громадянина на отримання своєчасної та вичерпної інформації в усіх сферах суспільно-економічних відносин – як внутрішніх, так і міжнародних, можливостями використання інформації для розвитку своєї особистості, для досягнень у науковій, мистецькій, підприємницькій діяльності, з іншого – захистом інформації, яка впливає на ступінь особистої безпеки.

Для забезпечення інформаційної безпеки на законодавчому рівні необхідно чітко визначити юридичний зміст поняття інформаційної безпеки, встановити правові основи забезпечення інформаційної безпеки, конкретизувати функції та розмежувати повноваження державних органів у цій сфері, визначити роль, місце та забезпечити можливість реального впливу на стан справ в інформаційній сфері громадських організацій та громадян.

На законодавчому рівні пропонується [9]:

закріпити підтримку національних виробників у розвитку інформаційної інфраструктури, забезпечити права, обов’язки та відповідальність суб’єктів, що надають інформаційні послуги;

стимулювати удосконалення засобів захисту інформації та інформаційних мереж, підвищення ефективності програмного забезпечення;

забезпечити неможливість несанкціонованого доступу до інформації, в тому числі неможливість її знищення, перекручування, фальсифікації тощо;

розробити ефективні механізми сертифікації обладнання та програмного забезпечення, засобів та механізмів захисту інформації тощо;

сформувати системи моніторингу показників інформаційної безпеки у найбільш важливих сферах життя суспільства.

Таким чином, логічним та обґрунтованим є питання розробки і прийняття єдиного документа у сфері інформації та інформатизації – кодифікованого акта України щодо сфери інформаційного права з урахуванням особливостей сучасного соціально-економічного та духовного розвитку країни.

Як бачимо, інформаційна безпека, як і правова інформатика, тісно пов’язана зі стратегіями інформаційного суспільства.

Висновки

Взаємозв’язок правової інформатики та інформаційної безпеки випливає з того, що вони тісно пов’язані зі стратегіями інформаційного суспільства, а також з того, що інформаційна безпека як наукове явище сьогодні формується на рівні міжгалузевого комплексного інституту (комплексної наукової дисципліни), який утворився на межі поєднання правової інформатики, інформаційного права та теорії організації соціальних систем.

Проведені дослідження дають змогу систематизувати знання про сутність та зміст правової інформатики та інформаційної безпеки.

Використана література:

1. Цимбалюк В.С. Окремі питання щодо визначення категорії “інформаційна безпека” у нормативно-правовому аспекті // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2004.– № 8.– С. 30-33.

2. Правова інформатика / [Швець М.Я., Брижко В.М., Задорожня Л.М., Коваль М.І., Хахановський В.Г. та ін.]. У 2-х т. – К.: Парламентське видавництво, 2004. – Т.1. – 416 с.

3. Правова інформатика /[Швець М.Я., Калюжний Р.А., Хахановський В.Г. та ін.]; за ред. М.Я. Швеця та Р.А. Калюжного. – К.: “ІВА”, 2003. – 168 с.

4. Цимбалюк В.С. Сутність і зміст правової інформатики (методологічний аспект) // Правова інформатика. – 2005. – № 4(8). – С. 18-30.

5. Швець М.Я. До питання визначення терміна “правова інформатика” // Правова інформатика. – 2004. – № 2. – С. 98.

6. Правовая информатика и кибернетика ; под ред. Н.С. Полевого. – М.: Юридическая литература. 1993. – 525 с.

7. Гаврилов О.А. Курс правовой информатики: учебник для вузов. – М.: Издательство “НОРМА”, 2000. – 432 с.

8. Бібліотека баз даних “Правова інформатика”. – (Періодичне видання на CD). //www.bod.kiev.ua/cdbd/index.html.

9. Задорожня Л.М., Коваль М.І., Брижко В.М. Питання вдосконалення законодавства України у сфері інформації та інформатизації: додаток до наукового журналу “Правова інформатика” ; за ред. чл.-кор. АПрН України М.Я. Швеця. – К.: НДЦПІ, 2005. – 31 с.

10. Електронне інформаційне суспільство України: погляд у сьогодення і майбутнє /[В.М. Фурашев, Д.В. Ланде, О.М. Григор’єв, О.В. Фурашев]. – К.: Інжиніринг, 2005. – 164 с.

11. Брижко В.М. Правовий механізм захисту персональних даних ; за ред. д-ра екон. наук, проф. М.Я.Швеця та д-ра юрид. наук, проф. Р.А. Калюжного. – К.: Парламентське видавництво, 2003. – 120 с.

12. Брижко В.М. Організаційно-правові питання захисту персональних даних: автореф. дис. ... канд. юр. наук: 12.00.07 / Національна академія державної податкової служби України. – Ірпінь, Київської обл., 2004. – 20 с.

УДК 342.9(075.8)

О. ЯРЕМЕНКО, *кандидат наук з державного управління, доцент,*
завідувач кафедрою правознавства Вінницького державного педагогічного університету ім. М.Коцюбинського

ПРАВОВЕ РЕГУЛЮВАННЯ ДОСТУПУ ДО ОФІЦІЙНОЇ ПРАВОВОЇ ІНФОРМАЦІЇ В УКРАЇНІ

Анотація. *Досліджено поняття “офіційна правова інформація” та її основні риси. Проаналізовано систему правового регулювання доступу до офіційної правової інформації в Україні.*

Право як основний соціальний регулятор може виконувати своє призначення тільки за умови вільного доступу суб’єктів суспільних відносин до всіх його інформаційних проявів. За допомогою правової інформації громадяни отримують відомості про структуру і діяльність держави та її інституцій, їх права та обов’язки, міру належної поведінки, дозволи, заборони, юридичні санкції, що обумовлює високий рівень її соціальної значимості і актуальність наукових досліджень проблем доступу до неї.

Інформація загалом, і правова зокрема, є об’єктом наукового аналізу в працях вітчизняних та зарубіжних дослідників А.Б. Агапова, Ю.М. Батуріна, І.Л. Бачило, К.І. Белякова, В.М. Брижка, В.Д. Гавловського, А.Б. Венгерова, Л.М. Задорожної, Р.А. Калюжного, В.А. Копилова, Н.В.Кушакової, П.І. Орлова, Г.Г. Почепцова, М.М. Рассолова, В.Г. Хахановського, М.Я. Швеця та інших учених. У їхніх працях досліджено взаємозв’язок інформації та права; роль інформації в процесі державного управління, управління в галузі права та внутрішніх справ; проблеми інформаційної безпеки громадян, корпорацій та держави; правові проблеми інформатизації, окремі аспекти права на інформацію тощо.

У той же час подальшого дослідження потребують проблеми правового регулювання доступу до правової інформації як однієї із найважливіших складових інформаційних ресурсів держави, що і ставить за мету дана стаття.

У Законі України “Про інформацію” *правова інформація* визначається як *сукупність документованих або публічно оголошених відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними, їх профілактику тощо* [1]. На нашу думку, включення до дефініції правової інформації конкретного переліку відомостей юридичного характеру виглядає не зовсім доцільним, оскільки правова сфера відноситься до надзвичайно складних системних утворень із багатьма складовими, перерахувати які в одному визначенні досить важко. До того ж, в цьому законі в окрему групу виділяється інформація державних органів та органів місцевого самоврядування, під якою розуміється офіційна документована інформація, яка створюється в процесі діяльності законодавчої, виконавчої та судової влади, а також органів місцевого самоврядування і основними джерелами якої визнаються нормативні та ненормативні акти, що свідчить про ототожнення цієї інформації з правовою. Таким чином, легітимне визначення правової інформації потребує вдосконалення і наукового обґрунтування.

В юридичній науці існує два основних трактування поняття “правова інформація”: широке та вузьке. Прихильниками першого є А.Б. Венгеров, О.А. Гаврилов, М.М. Рассолов, Л.В. Туманова, А.А. Снитніков та ряд інших. Так, на думку А.Б. Венгерова, терміном

“правова інформація” охоплюються нормативні акти, відомості про юридичні і навколо юридичні явища, а також інформація, що має характер приписів [2, – С. 73]. О.А. Гаврилов трактує правову інформацію як відомості про факти, події, предмети, явища, які протікають в правовій сфері, що містяться в різних джерелах і використовуються державою та суспільством для вирішення завдань правотворчої, правозастосовної та правоохоронної діяльності, захисту прав та свобод особи [3, – С. 15]. М.М. Рассолов під правовою інформацією розуміє сукупність відомостей про події, що відбуваються в правовій системі суспільства, її підсистемах і елементах, а також в зовнішніх по відношенню до даних систем утвореннях, про зміну характеристик правових системних утворень і зовнішнього середовища [4, – С. 109]. Л.В. Туманова та А.А. Снитніков вважають, що до правової інформації відноситься зміст даних, використання яких дає можливість вирішити ту чи іншу правову проблему [5, – С. 13].

Аналогічний підхід спостерігається і працях з правової інформатики західних країн, в яких під правовою інформацією розуміються відомості, факти, знання, що мають офіційне походження і містяться в нормативних актах, міжнародних угодах, правових прецедентах, висновках юридичної соціології та правової статистики, інших наукових джерелах [6, – С. 53].

У той же час, юридична наука оперує вузьким трактування цієї категорії. Зокрема, Кудрявцев Ю.В., визначає правову інформацію як відомості, що містяться виключно в нормах права. На його думку, процес створення і поширення правової інформації полягає у виданні державою правових приписів і доведенні їх до адресатів [7, – С. 15].

На наш погляд, широке трактування поняття “правова інформація” більш точно відображає її сутність. Без сумніву, нормативна правова інформація є найбільш актуальною для держави та суспільства через її регулятивний характер, однак інші відомості про юридичні та навколо юридичні явища і процеси також мають значну теоретичну і практичну цінність та не можуть бути винесені поза рамки правової інформації.

Важливе значення має також часова характеристика правової інформації. Право є явищем історичним, яке перебуває в стані постійної динаміки. Відомості про процес його розвитку, історичні пам’ятки права, недіючі нормативні акти є досить важливими, так само як і дані про акти, що будуть прийняті або наберуть чинності в майбутньому.

Виходячи із вищезазначеного, *правову інформацію* можна визначити як *відомості про юридичні та безпосередньо пов’язані з юридичними явищами процеси, що мали, мають або будуть мати місце в суспільстві та державі*.

Особливе значення має офіційна правова інформація, якій притаманні ряд характерних рис:

- офіційна правова інформація видається від імені держави її інституціями;
- вона є важливим ресурсом, що забезпечує виконання державою основної функції – управління суспільством;
- ця інформація виникає в процесі реалізації державними органами та органами місцевого самоврядування компетенції, закріпленої законодавством;
- офіційна правова інформація є результатом інтелектуальної діяльності депутатів різних рівнів, державних службовців та посадових осіб, на яку, в переважній більшості, не поширюються права інтелектуальної власності;
- цей вид інформації матеріалізується у формі документа, фіксується на папері і має ідентифікаційні реквізити.

Офіційну правову інформацію можна класифікувати на основі багатьох взаємопов’язаних критеріїв, ключовим серед яких є роль, яку вона виконує в системі

суспільно-правових відносин і на основі якої її можна поділити на нормативну та ненормативну. Додатковим критерієм поділу офіційної правової інформації на ці два види є режим доступу до неї. Так, з моменту виникнення феномену права і до сьогодні відносно нормативної правової інформації існує презумпція відкритості, оскільки вона є результатом здійснення державними органами нормотворчих функцій, носить регулятивний характер і має високий рівень загальносоціальної значимості. Ще в давні часи закони доводились до відома громадян у спосіб, який дозволяв тогочасні технології: різьба на камені, написання на різних матеріальних носіях, усне оголошення глашатаями тощо. По мірі розвитку права формувались принципи щодо знання державних приписів: уже в римському праві було сформульовано правило, згідно з яким незнання закону не може бути виправданням його невиконання.

У процесі ускладнення державно-правових явищ, збільшення кількості нормативних актів та їх обсягів, зростання їх суспільного значення виникла необхідність юридичного закріплення права на доступ до правової інформації та механізмів його реалізації.

Аналіз міжнародних документів та конституцій різних країн світу свідчить про те, що на сьогодні, в більшості випадків, право на доступ до правової інформації є складовою загального права на отримання інформації або свободи інформаційної діяльності. Так, в Загальній декларації прав людини 1948 року право на доступ до інформації розглядається як складова вільного виявлення своїх переконань. У статті 19 цього документа зазначено: *“Кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів”*.

Майже без змін формулювання цього права залишилось і в Міжнародному пакті про громадянські і політичні права 1966 року, який передбачає право кожної людини на вільне вираження свого погляду, що включає свободу шукати, одержувати і поширювати будь-яку інформацію та ідеї незалежно від державних кордонів, усно, письмово чи за допомогою друку або художніх форм вираження або в інший спосіб на свій вибір.

Аналогічні загальні норми містять і конституції європейських держав. Безпосереднє конституційне закріплення права на доступ до правової інформації є тільки в Конституції Португальської Республіки, яка гарантує доступ до правових актів та юридичної інформації [8, – С. 69].

В Україні гарантом права на доступ до інформації є Конституція України, стаття 34 якої надає право кожному вільно збирати, зберігати, використовувати і поширювати інформацію. Виходячи з цієї конституційної норми, вільний доступ до інформації надається тільки фізичним особам, а для всіх інших суб’єктів це право не передбачено. Більш широко сформульовано суб’єктний склад цього права у статті 9 Закону України “Про інформацію”, яка зазначає, що право на інформацію мають громадяни України, юридичні особи і державні органи. В цьому ж законі деталізовано об’єкт права на інформацію: відомості, які необхідні для реалізації прав, свобод і законних інтересів, а також ті які необхідні для здійснення завдань і функцій. Фактично під такі характеристики може потрапити будь-яка інформація, в тому числі правова.

Крім цього, Конституція України містить норми які гарантують право на доступ до окремих видів правової інформації. Так, в статті 57 зазначено, що кожному гарантується право знати свої права і обов'язки, а закони та інші нормативно-правові акти, що їх визначають, мають бути доведені до відома населення у порядку, встановленому законом.

Аналіз даного конституційного положення дає підстави зробити висновок про його недосконалість. Так, формулювання “закони та інші нормативно-правові акти, що визначають права і обов'язки громадян” суперечить пункту1 статті 92 Конституції, в якому зазначено, що права і свободи людини і громадянина, гарантії цих прав і свобод, а також основні обов'язки громадянина визначаються виключно законами України. Тобто ніякі інші нормативно-правові акти, крім законів, не можуть визначати права та обов’язки громадян. У той же час, на виконання таких законів необхідно видавати підзаконні акти, які тією чи іншою мірою зачіпають права та свободи людини. У зв’язку з цим, в даній статті слово “визначаються” варто замінити на “стосуються”.

Відповідно до цієї ж статті Конституції України порядок опублікування актів, що регламентують права та свободи громадян, повинен визначатися тільки законом. На сьогодні ця норма не дотримується і порядок публікації законів регулюється Регламентом Верховної Ради України та указами Президента України “Про порядок офіційного оприлюднення нормативно-правових актів та набрання ними чинності” [9] та “Про опублікування актів законодавства України в інформаційному бюлетені “Офіційний вісник України” [10]. Даними актами передбачено два види публікації нормативно-правових актів: офіційну та неофіційну.

Так, згідно з Регламентом Верховної Ради підписані Президентом закони та інші акти, прийняті Верховною Радою, публікуються у “Відомостях Верховної Ради України” протягом 30 днів, а також в газеті “Голос України” протягом 5 днів і є офіційною публікацією. Вищезазначені укази Президента офіційною публікацією визнають ту, що здійснена в інформаційному бюлетені “Офіційний вісник України”, який засновано і видається Міністерством юстиції України, обов’язковій публікації у якому підлягають закони України; укази і розпорядження Президента України; постанови і розпорядження Кабінету Міністрів України, що мають нормативний характер; акти Конституційного Суду України; нормативно-правові акти Національного банку України; міжнародні договори України, що набрали чинності; нормативні акти міністерств, інших центральних органів виконавчої влади.

Офіційність публікації передбачає, в першу чергу, те, що громадяни, державні органи, підприємства, установи тощо під час здійснення своїх прав і обов'язків повинні застосовувати закони України, інші акти Верховної Ради України, акти Президента України і Кабінету Міністрів України, опубліковані в офіційних друкованих виданнях.

У той же час, передбачається неофіційне оприлюднення нормативно-правових актів: публікація в друкованих засобах масової інформації, засновниками яких є фізичні та юридичні особи, обнародування по телебаченню, радіо, передача телеграфом. Неофіційне оприлюднення допускається лише після офіційного і носить інформаційний характер.

Окрема увага в законодавстві України приділяється оприлюдненню регуляторних актів, до яких відносяться два види документів:

- прийняті уповноваженим регуляторним органом нормативно-правові акти, спрямовані на правове регулювання господарських відносин, а також адміністративних відносин між регуляторними органами або іншими органами державної влади та суб'єктами господарювання;
- прийняті уповноваженим регуляторним органом інші офіційні письмові документи, які встановлюють, змінюють чи скасовують норми права, застосовуються неодноразово та щодо невизначеного кола осіб і які спрямовані на правове регулювання господарських відносин, а також адміністративних відносин між регуляторними органами або іншими органами державної влади та суб'єктами господарювання незалежно від того, чи вважаються ці документи відповідно до закону, що регулює відносини у певній сфері, нормативно-правовими актами [9].

Доступ до ненормативної офіційної правової інформації дещо складніший з юридичних, організаційних та технічних причин.

Ненормативна офіційна правова інформація не містить правових норм, виникає в процесі поточної діяльності державних органів та органів місцевого самоврядування і є досить різноманітною за змістом та юридичною природою. Джерелами цієї інформації є різні за характером, назвою, формою, змістом, юридичним значенням документи, спільною рисою яких є те, що вони, як правило, не підлягають обов’язковому оприлюдненню. Наприклад, процедура ухвалення закону супроводжується документами, кожен з яких має самостійне юридичне значення: рішення Верховної Ради, законодавчі пропозиції, проекти закону, поправки, стенографічні бюлетені засідань, висновки комісій, проекти рішень, однак публікації підлягають тільки закони та постанови Верховної Ради.

Унаслідок того, що в переважній більшості ненормативна правова інформація має менше суспільне значення ніж нормативна, в діючому законодавстві України відсутні норми про обов’язковість її оприлюднення. В той же час, виходячи з принципу інформаційної відкритості державних органів та свободи інформації, юридичні відомості ненормативного характеру також повинні бути доступні для громадськості. На це спрямований указ Президента України від 17.05.2001 р. “Про підготовку пропозицій щодо забезпечення гласності та відкритості діяльності органів державної влади”. Ним передбачено створення робочої групи до обов’язків якої входить розробка та внесення на розгляд законопроектів метою яких є створення умов для вільного доступу громадян до рішень органів державної влади та до інформації про діяльність цих органів, у тому числі щодо формування і реалізації державної політики в різних сферах суспільного життя; впорядкування механізмів надання громадянам органами державної влади інформаційних та інших послуг, насамперед тих, що стосуються реалізації їх конституційних прав, задоволення потреб та інтересів; забезпечення широкого доступу до документів, створених у процесі діяльності органів державної влади [12].

На основі цього указу була видана Постанова Кабінету Міністрів України від “Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади”. Згідно з цим документом на веб-сайті органу виконавчої влади розміщується інформація, що стосується статусу того чи іншого органу; основні функції структурних підрозділів; плани підготовки органом проектів регуляторних актів та зміни до них; повідомлення про оприлюднення проектів регуляторних актів, проекти цих актів і аналіз їх регуляторного впливу; звіти про відстеження результативності прийнятих органом регуляторних актів; відомості про регуляторну діяльність органу; порядок реєстрації, ліцензування окремих видів діяльності у відповідній сфері; цільові програми у відповідній сфері; державні інформаційні ресурси з питань, що належать до компетенції органу; поточні та заплановані заходи і події у відповідній сфері [13] .

Крім цього, чинним законодавством України передбачено безпосереднє надання інформації зацікавленим суб’єктам. Цей механізм дає можливість ознайомитись із будь-якою ненормативною офіційною правовою інформацією і реалізується шляхом подання суб’єктами інформаційних відносин інформаційних запитів двох видів: щодо отримання офіційних документів та щодо отримання інформації про діяльність органів законодавчої, виконавчої та судової влади України. Обов’язком органів законодавчої, виконавчої та судової влади України є надавати інформацію, що стосується їх діяльності, письмово, усно, по телефону чи, використовуючи публічні виступи своїх посадових осіб [1].

Висновки

Правова інформація як відомості про юридичні та безпосередньо пов’язані з юридичними явища та процеси, що мали, мають або будуть мати місце в суспільстві та державі, має важливе суспільне значення, яке обумовлює її відкритість.

Систему правового регулювання доступу до офіційної правової інформації в Україні складає Конституція, Закон України “Про інформацію” та ряд інших нормативно-правових актів. Аналіз цих документів свідчить, що рівень доступу до правової інформації залежить від її виду. Найбільш чітко в національному законодавстві врегульовані питання оприлюднення нормативної інформації, яка підлягає обов’язковому опублікуванню в офіційних друкованих засобах масової інформації. Ненормативна офіційна правова інформація поширюється шляхом розміщення її в мережі Інтернет або може бути надана державними органами та посадовими особами на індивідуальні запити.

На сьогодні у зв’язку із постійним зростанням ролі правової інформації, ускладненням інформаційно-правових відносин, розвитком інформаційно-комунікаційних систем існує об’єктивна необхідність подальшого вдосконалення матеріальних та процесуальних норм щодо доступу до цієї інформації.

Окремого аналізу потребують процесуальні норми, що регламентують процедури доступу до окремих видів правової інформації, а також режим інформації з обмеженим доступом, яка видається державними органами, що може бути предметом подальших розвідок у цьому напрямі.

Використана література

1. Закон України “Про інформацію” // Відомості Верховної Ради України . – 1992. – № 48. – Ст. 650.

2. Венгеров А.Б. Категория “информация” в понятийном аппарате юридической науки // Советское государство и право . – 1977. – № 10. – С. 70-77.

3. Гаврилов О.А. Курс правовой информатики. Учебник для вузов. М.: Издательство НОРМА, 2000. – 432 с.

4. Рассолов М.М. Проблемы управления и информации в области права. – М.: Юридическая литература, 1991. – 229 с.

5. Снытников А.А., Туманова Л.В. Обеспечение и защита права на информацию. – М.: Городец-издат, 2001. – 344 с.

6. Информатика и право: теория и практика буржуазных государств: сборник обзоров. – М.: Институт научной информации по общественным наукам. – 1988. – 225 с.

7. Кудрявцев Ю.В. Нормы права как социальная информация. – М.: Юридическая литература, 1981. – 144 с.

8. Конституции зарубежных государств: учебное пособие ; сост. проф. В.В. Маклаков. – 3-е изд. – М.: Издательство БЕК, 2001. – 592 с.

9. Указ Президента України “Про порядок офіційного оприлюднення нормативно-правових актів та набрання ними чинності” // Офіційний вісник України. – 1997. – № 24. – с. 11.

10. Указ Президента України “Про опублікування актів законодавства України в інформаційному бюлетені “Офіційний вісник України” // Урядовий кур'єр. – 19 грудня. – 1996 р.

11. Закон України від 11.09.2003 № 1160-IV “Про засади державної регуляторної політики у сфері господарської діяльності” // Офіційний вісник України. – 2003. – № 41. – ст. 2157. – с. 15.

12. Указ Президента України від 17.05.2001 № 325/2001 “Про підготовку пропозицій щодо забезпечення гласності та відкритості діяльності органів державної влади” // Урядовий кур'єр. – 22 травня. – 2001 р.

13. Постанова Кабінету Міністрів України “Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади // Офіційний вісник України . – 2002. – № 2. – С. 234. – Ст. 57.

УДК 351.713

В. МАЦЮК, *кандидат юридичних наук*

ПРАВОВІ АСПЕКТИ ІНФОРМАТИЗАЦІЇ

Анотація. *У статті йдеться про удосконалення інформаційно-правової сфери і управління у зв’язку із використанням технічних засобів інформатики. Дається визначення правовій інформатиці як інтегрованій дисципліні, яка ввібрала в себе науку інформатики і права з системою таких понять, як: математична теорія зв’язку, інформація, ентропія, інформаційний шум, надлишок біт, байт та ін.*

Однією із відмінних ознак світової цивілізації є постійне зростання значимості інформації.

Бурхливий розвиток інформаційної індустрії, наближення України до Євросоюзу вимагає необхідності переглянути ставлення до інформаційного середовища, його ролі, місця в суспільстві.

Після помаранчевих подій в Україні активно набуває розвитку національна законодавча система регулювання суспільних інформаційних відносин і процесу інформатизації. В умовах демократії нагальним є впровадження державної політики, зокрема в інформатизацію, основою розвитку якої є впровадження інформаційних технологій, створення інформаційних ресурсів.

Під державною інформаційною політикою розуміється регулююча діяльність державних органів, яка направлена на розвиток національного інформаційного середовища, що включає не тільки телекомунікації, інформаційні системи і засоби масової інформації, а й всю сукупність виробництва та відносини, пов’язані зі створенням, зберіганням, обробкою, демонстрацією, передаванням інформації [1, – С. 252].

Удосконалення правової інформації на законодавчому рівні означає упорядкування, врегулювання відносин шляхом прийняття законів, підзаконних актів.

Для адаптації української економіки до норм ЄС необхідно внести зміни і доповнення до 350 законів України, переглянути та скасувати 150 постанов уряду, 1300 відомчих актів [2]. Адаптація законодавчої бази України, правової інформації до норм Світової організації торгівлі (СОТ) потребує значних матеріальних затрат та часу.

Інформаційна сфера формується не стільки державою, скільки ринком, тому написання програм, концепцій – це часткове вирішення суспільних проблем, для вирішення яких необхідно юридично визначитися в найбільш важливих правових нормах поведінки суб’єктів правовідносин, у тому числі при здійсненні основної функції правоохоронних органів: попередженні злочинів і боротьбі з правопорушеннями. Розширюється коло завдань, що вирішуються шляхом математичного моделювання.

“Мова сучасної математики – це мова алгоритмів і програм, яка включає в себе мову формул”, – зазначав академік В.М. Глушков [3, – С. 59-60]. Мова математики придатна для опису параметрів і залежностей будь-якого характеру. На базі даних математики, логіки та інформатики можливе визначення вірогідного характеру знань, визначення істини або неправдивих даних.

У сфері правового регулювання та управління серед класичних експериментальних методів все більше використовується метод математичного моделювання. Б.В. Гніденко

зазначає, що від математизації наші знання стають більш повноцінними, бо є можливість попередньо прораховувати хід явищ, дізнатися про рівень досконалості наших знань, а кількісне порівняння наших закономірностей з реаліями відповідних явищ надає нам таку можливість [4, – С. 82].

Змінилося ставлення спеціалістів до інформаційних технологій. Якщо раніше, за висловом Н.І. Козюбри, ”правознавці користувалися математичним апаратом дуже скромно” [5, – С. 64], а на думку англійського юриста Д.Стреттона “коли йдеться про комп’ютери, представники юридичної професії переходять від апатії та істерії до паніки і врешті-решт, до повного заспокоєння без будь-якої спроби зрозуміти їх сутність”[6, – С. 353], то сьогодні кожний фахівець розуміє, що тільки той, хто озброєний комп’ютером, може володіти інформацією оперативно. В частині юридичного врегулювання права на доступність і безплатність вищої освіти актуальною є практична реалізація “Національної доктрини розвитку освіти” [7].

Необхідним атрибутом будь-якого дослідження, що реалізується з використанням інформаційних технологій, є знакові системи (символи, сигнали – синтез юридичного матеріалу і мови інформатики), що виконують функцію заміни собою великої кількості слів. Для забезпечення правової діяльності на базі знакових систем розробляються методики інформаційного пошуку в інформаційних системах, які створюються на базі інформаційних технологій. При цьому пізнавальне відображення досягається не стільки через окремі знаки, скільки через їх певне злиття, зв’язок і структуру, через систему знаків, як зазначали Р.С. Бєлкін і А.І. Вінберг [8, – С. 232]. За німецьким філософом Георгом Клаусом: “Наука знаходить все більш надійні знаки, за допомогою яких вона відображає дійсність, а нечіткі або розпливчасті слова поступово зникають з її мови” [9, – С. 45].

Збільшення масштабів інформаційних технологій, посилене проникнення їх у практику соціального управління висвітило ряд проблем, які відносяться до всього технологічного циклу збору, переробки і застосування інформації, проблеми змістовності інформаційних процесів і значення інформаційних технологій, які виникають як засіб протиріччя між накопиченими знаннями і тими, що продовжують накопичуватися, а також можливостями і масштабами їх соціального використання.

Розвиток інформаційних технологій, їх впровадження “породжує” “комп’ютерну злочинність” – нову категорію злочинів, предметом яких є інформаційні системи, інформація і програмне забезпечення. Наявність таких злочинів накладає свій відбиток на діяльність правоохоронної системи, змінюючи не тільки характер її основних функцій, завдань, напрямів діяльності, але й структуру. Поряд з функцією попередження злочинів і боротьби з правопорушеннями з’являються нові функції, завдання, зокрема – організація системи захисту відомчої інформації, діяльність щодо протидії “комп’ютерній злочинності” в межах наданих повноважень. Цей вид діяльності носить загально соціальний характер, тому що безпосередньо впливає на процеси управління інформатизацією суспільства в цілому. Здійснення такої функції тягне за собою ряд проблем комплексного характеру, які можливо вирішити шляхом реформування, в т.ч. інформаційно-правової роботи, раціоналізації організаційно-управлінських основ правового механізму, зміни кадрового складу.

З поняттям “інформаційно-правова робота” тісно пов’язане поняття “інформаційно-правове поле” (системне поняття, існує як ціле), до якого повітряні комунікаційні зв’язки входять як один з елементів. Головним завданням інформаційно-правової сфери та управління є розвиток інформаційно-правових процесів, використання технічних засобів інформатики, підготовка інформаційно-правового поля.

Фактори (як елементи однієї соціально-правової системи) інформаційно-правового поля забезпечують появу нових правових знань, їх переробку, передачу, використання і вплив на об’єкти системи.

Формування інформаційно-правового поля залежить від людського фактора, в т.ч. від організаційної структури, рівня підготовки фахівців як користувачів, принципів стимулювання, контролю, методів і форм управління, документопотоків, форм документів, процедур, регламентів, юридичних норм, і являє собою систему з її правовими і технічними елементами. До останніх, зокрема, відносяться апаратні засоби, програмне забезпечення, телекомунікації.

Інформаційне поле не можливо створювати частинами. Якщо не підготовлений хоча б один із його елементів, робота зі створення умов його використання зводиться до нуля. Окремі елементи нічого не варті, якщо відсутні зв’язки між ними.

Поняття інформаційно-правового поля (поняття правової інформатики, науки, яка розглядає інформаційні процеси в правовій діяльності) і управління має суттєве навантаження у зв’язку з інформатизацією правової діяльності і управління, включає в себе всі умови для технологічної переробки і ефективного використання саме правових знань у вигляді інформаційного ресурсу організаційно-правової діяльності.

В інформаційно-правовому полі функціонує юридично значуща інформація, зокрема організаційно-правові знання, на відміну від інтелектуального середовища, де функціонує весь потенціал знань. При цьому інформаційне середовище є елементом інформаційно-правового поля. Саме підхід до юридичної діяльності і управління з точки зору інформаційно-правового поля означає розуміння системності, динамічної цілісності всіх елементів, які забезпечують інформдинаміку (функціонування інформаційно-правового інформаційного ресурсу). Правовою інформдинамікою вчені називають науку про розвиток сфери соціального управління під впливом її інформаційного ресурсу.

Інформаційний ресурс організаційно-правової діяльності є головним, “власним” поняттям правової інформатики, формується на перетині інформаційно-технологічного і семантичного напрямів досліджень систем правової діяльності і управління. Для інформаційного ресурсу організаційно-правової діяльності характерним є процес перетворення юридичних знань на силу переконань.

Сутність, закони функціонування організаційно-правового інформаційного ресурсу, механізми взаємодії з іншими ресурсами, його вплив на сферу управління і правового регулювання є предметом правової інформатики.

Інформаційний ресурс (корисні, правові відомості і дані, юридично значуща інформація у вигляді понятійного правового знання) дозволяє правовій інформатиці посісти важливе місце в системі правових наук.

Правова інформатика виступає інтегрованою дисципліною, яка ввібрала в себе науку інформатики і права та використовує систему понять, зокрема поняття “математична теорія зв’язку”, “інформація”, “ентропія”, “інформаційний шум”, “надлишок”, “біт”, “байт”, “ціль”, “управляюча і управляючої підсистеми”, “прямий і зворотній зв’язки”.

Розгляд інформаційного ресурсу з точки зору організаційно-правового ресурсу означає перехід до вивчення внутрішніх зв’язків і закономірностей динаміки права, котра, власне, і є невід’ємною рисою правового регулювання, розуміння поняття, яке подають у своїх публікаціях П.М. Рабинович та О.Ф. Скакун і визначають його як здійснюваний державою за допомогою всіх юридичних засобів владний вплив на суспільні відносини з метою їх упорядкування, закріплення, охорони й розвитку [10, 11].

Розуміння інформаційного ресурсу організаційно-правової діяльності і його ролі як основи правового інтелекту пов’язано з розумінням інформаційної природи юридичного (правового) знання. Категорія “інформаційний ресурс” орієнтує на якісне визначення його правових та соціально-правових аспектів, зокрема на визначення корисності правових інформаційних систем.

Зрозуміти значущість інформації можливо, якщо розглядати інформаційну роботу в її повному циклі, від моменту створення інформації до її використання для цілей системи.

Учений К.Бєляков зазначає, що поняття повного інформаційного циклу необхідно розглядати – від енергії, що витрачається на створення інформації, її передачу і використання, до енергії, що додатково вивільняється в системі за рахунок ентропії (невизначеності) останньої, що надає можливість трактувати інформацію як інформдинаміку [1, – С. 213] та визначати коефіцієнт корисної дії інформаційної системи (залишок від роботи, що витрачений на компенсацію невизначеності самого спостерігача, невпорядкованості і початкової ентропії об’єкта). Обмеженість канонічної теорії інформації в тому, що вона включає не весь інформаційний цикл, а лише один із її ланцюжків – зв’язок, передачу відомостей.

Одна частина інформаційної роботи компенсує невизначеність спостерігача і внутрішню ентропію об’єкта, інша, корисна, – компенсує додану ентропію (невизначеність) об’єкта (її зростання – позитивний показник), яка направлена на досягнення нового, більш інформативного рівня функціонування (віддачу).

Кількісне визначення постійної (вплив енергетичних витрат на управління щодо їх енергетичної віддачі) інформації дозволить регулювати процеси фазового переходу знань в силу переконань, визначати коефіцієнт корисної дії інформаційних систем.

Зменшенням невизначеності управляючої підсистеми початкової величини невизначеності об’єкта, зріст якої є негативним показником (свідчить про невикористані інформаційні ресурси та про невпорядкованість об’єкта), досягається збільшення інформаційного потенціалу інформаційної системи.

Використана література

1. Беляков К. Управление и право в период информатизации: монография. – К., 2001, – 308 с.

2. Чечко Н. Український освітній центр реформ: за матеріалами сайта ”Український монітор”. Нова Оболонь № 8, серпень 2005.

3. Глушков В.М. Роль математики в современной науке / Современная культура и математика. – М., 1975.

4. Гнеденко Б.В. Вопросы математизации современного естествознания / Диалектика и современное естествознание. – М., 1970.

5. Козюбра Н.І. Юридична наука і перспективне прогнозування // Методологічні проблеми юридичної науки. – К., 1990.

6. Вказівка першого заступника міністра внутрішніх справ України Л.В. Бородича “Про типову форму повідомлення про комп’ютерні злочини від 16 грудня 1996 року”. Додаток 2.

7. Національна доктрина розвитку освіти: затверджено Указом Президента України від 17 квітня 2002 р. // Освіта України. – 2002, 23 квітня. – С.4-6.

8. Бєлкин Р.С., Винберг А.И. Язык науки и применение знаковой теории в криминалистике // Криминалистика. Общетеоретические проблемы. – М., 1973.

9. Клаус Г. Сила слова (гносеологический и прагматический анализ языка). – М., 1967.

10. Рабинович П.М. Теория государства и права. – Харьков, 2000. – С.529.

11. Скакун О.П.Основи загальної теорії держави та права. – К., 2001. – С.153.

УДК 303.725.37:343.35

В. ЛОЖКІН, *кандидат історичних наук, доцент*
В. ЦИМБАЛЮК, *кандидат юридичних наук*

ВИКОРИСТАННЯ ЗДОБУТКІВ ПРАВОВОЇ ІНФОРМАТИКИ У БОРОТЬБІ З КОРУПЦІЄЮ

Анотація. *У статті розкриваються питання використання здобутків правової інформатики у боротьбі з корупцією в Україні. Пропонується методологія адаптації Інтернет-технологій для організації моніторингу громадської думки щодо корумпованості органів державного управління (на прикладі органів державної податкової служби).*

У порядку постановки проблеми у загальному вигляді та її зв‘язку із важливими науковими і практичними завданнями пропонується звернути увагу на те, що боротьба з корупцією була, є і буде актуальною для українського суспільства (як і для будь-якого суспільства). Соціологічні дослідження свідчать, що абсолютна більшість громадян України вважає корупцію негативним явищем, притаманним нашому суспільству [1]. Ця проблематика широко обговорюється вітчизняними політиками, науковцями-юристами, політологами, соціологами та іншими науковцями. Разом з тим, всі притримуються думки, що корупція є чинником, який загрожує національній безпеці України.

Аналіз останніх публікацій щодо дослідження проблематики свідчить, що протягом існування України як незалежної держави багатьма вітчизняними дослідниками були проведені ґрунтовні дослідження корупції в різних її аспектах. Серед таких дослідників можна відзначити М.І. Камлика, О.С. Новикова та інших [2, 3]. Подібні дослідження проводяться і за кордоном [4]. При цьому автори посилалися на різні результати соціологічних досліджень, які проводилися у минулому. Тобто досліджень, які відображали стан явища на певний момент часу, що вже сплинув [5-7]. При цьому не виключається латентність корупції. В основному її рівень визначається за експертними оцінками.

У той же час, у зарубіжних країнах існують і спроби встановити рівень латентності будь-яких видів злочинності за допомогою соціологічних опитувань [8-13]. Наприклад, при здійсненні віктимологічних досліджень заразом з’ясовується, чи звертались потерпілі від злочинних замахів до правоохоронних органів. У більшості випадків респондентам пропонують повідомити про кримінальні події упродовж останнього року. Так у США (National Grime Survey) двічі на рік починаючи з 1973 року, періодично організовують індикативні опитування населення. Для цього на підставі загальнонаціональної репрезентативної вибірки адрес створено так звану “Національну панель злочинності”, яка включає дослідження майже 60 тис. сімей.

У Великобританії, зокрема в Англії та Уельсі, подібні дослідження (British Crime Survey) проводяться починаючи з 1982 року. Вибіркова сукупність формується на основі систематизатора поштових адрес, опитують понад 10000 респондентів, періодичність – 2-4 роки.

Під егідою Міжрегіонального інституту ООН (UNICRI) наприкінці 1980-х на початку 1990-х років були здійснені транснаціональні порівняльні дослідження у країнах центральної та східної Європи, зокрема у Польщі, Росії, Грузії, Естонії, Словенії.

Слід зазначити, що проведення соціологічних досліджень за такою методикою є досить затратним. При цьому є й суто наукові, методичні та організаційно-правові проблеми

забезпечення своєчасності, оперативності, а отже й достовірності отриманої соціологічної інформації для прийняття відповідних політичних, правових, економічних та інших рішень органами державної влади.

У порядку визначення не вирішених раніше частини загальної проблематики, котрій присвячується стаття, пропонується звернути увагу на методики організації інформаційного забезпечення проведення нових системних соціологічних досліджень щодо результатів правотворчості, правозастосування та правоосвітньої діяльності протидії корупції, зокрема з використанням комп‘ютерних технологій у контексті методології постійного моніторингу громадської думки.

Мета даної статті – висвітити в зазначеному вище контексті деякі результати проведеної роботи в Науково-дослідному центрі з питань оподаткування Національної академії державної податкової служби України. У рамках науково-дослідної роботи на замовлення Державної податкової адміністрації України розробляються методики моніторингу громадської думки щодо корумпованості податкових органів України з використанням можливостей Інтернет. На наш погляд, ці методики можуть бути використані в дослідженнях громадської думки і в інших органах державної влади.

Виклад основного матеріалу дослідження з обґрунтуванням отриманих результатів пропонується почати з тези, що ставлення громадськості до корупції в податкових органах, оцінка рівня її суспільної небезпеки та визначення рівня корумпованості серед працівників податкових органів є одним з важливих соціальних індикаторів якості діяльності всієї Державної податкової служби України (ДПСУ).

Організація ефективного моніторингу громадської думки щодо корумпованості органів державної податкової служби України набуває особливої актуальності з кількох обставин.

По-перше, результати вже проведених соціологічними службами досліджень з використанням паперових технологій свідчать, що переважна більшість респондентів, у тому числі представників бізнес-середовища України, вважають органи ДПСУ лідерами за рівнем корумпованості серед органів державної влади [5].

По-друге, нині на державному рівні реалізується Програма модернізації ДПСУ, одним із завдань якої є зниження рівня корупції в податковій службі. Результати, отримані на підставі ситуаційного моніторингу з використанням традиційних паперових технологій, до певної міри дають можливість скласти уяву про ефективність заходів модернізації податкових органів на певний час у минулому.

По-третє, корупції як в цілому серед державних органів влади, так і в органах ДПСУ притаманний високий рівень латентності, що не дозволяє офіційній статистиці віддзеркалити фактичну масштабність корупційних діянь, їх прояви та динаміку [6].

Останніми роками бурхливий розвиток Інтернету кардинально змінює життя мільйонів людей [14-16]. Електронна світова мережа розвивається швидкими темпами, кількість її користувачів з кожним роком збільшується. Процес інформатизації суспільства, у тому числі в Україні, надає потужного імпульсу відкритості суспільного устрою, дієвості феномену громадської думки в управлінні державними справами. Так званий кіберпростір сформував таке явище, яке набуло умовної назви “комьюнітіс” – групи, спільноти людей, яких пов’язує певний спільний інтерес і які встановлюють стійкі зв’язки між собою завдяки Інтернету. Через Інтернет відбувається вільне

залучення людей до комунікації без певних психологічних комплексів, притаманних “живому спілкуванню”.

Формування глобального інформаційного кіберсуспільства, зокрема на основі Інтернет технологій, створює нові можливості урядування, що набуло умовної назви – “електронного урядування” (е-уряду) [17,18]. Як і будь-яке урядування, воно повинно базуватися на соціологічних дослідженнях, у тому числі громадської думки. У зв‘язку з цим, організаторам та розробникам методик проведення соціологічних досліджень в Україні пропонується звернути увагу на можливість використання в своїй роботі сучасних Інтернет-технологій як складових е-уряду. Нині це розглядається як один з напрямів правової інформатики.

Перед висвітленням можливостей застосування таких технологій варто зазначити декілька методологічних положень проведення соціологічних досліджень. Будь-яке соціологічне дослідження проходить певні етапи. У науковій літературі виділяють, як правило, чотири етапи: 1) підготовка дослідження; 2) збирання первинної юридико-соціологічної інформації про об’єкт, що вивчається; 3) підготовка зібраної інформації до обробки й аналізу; 4) аналіз обробленої інформації та підготовка звіту за наслідками дослідження [7].

Як свідчить практика, другий етап, під час якого отримують неузагальнені відомості (окремі відповіді респондентів або експертів), найбільш трудомісткий, він вимагає залучення великої кількості інтерв’юерів та вкладання значних коштів. Саме в ході проведення цього етапу дослідники мають змогу використати в своїй роботі сучасні комп‘ютерні інформаційно-телекомунікаційні технології. Можливості застосування цих технологій в правових науках (зокрема, кримінології, правовій статистиці, юридичній соціології тощо) до нинішнього часу залишаються малодослідженими.

Використання Інтернет-технологій при проведенні соціологічних досліджень надає цілий ряд переваг. Перш за все, дослідження через Інтернет дозволяють зекономити час, гроші, людські ресурси, а також підвищити якість зібраної інформації. Завдяки інформаційно-телекомунікаційним технологіям існує можливість надання індивідуального зворотного зв’язку безпосередньо після заповнення анкети, що може стимулювати респондента до постійної участі в Інтернет-опитуваннях, а також бути фактором залучення інших респондентів.

Інтернет-технології дозволяють легше та швидше проводити адміністрування опитувань з єдиного центру їх організації, зокрема оперативно вносити необхідні зміни до тексту електронної анкети. Крім того, вони забезпечують високий ступінь так званої екологічної валідності.

Умови заповнення електронної анкети більш сприятливі для респондента, який знаходиться в комфортних для себе умовах – наодинці з комп‘ютером, що підключений до Інтернет. Відсутній візуальний контакт соціолога з респондентом зменшує психологічний дискомфорт та збільшує рівень щирості відповідей. Тобто в Інтернет-опитуваннях зменшується ступінь негативного впливу того, хто проводить опитування. У зв‘язку з цим Інтернет-технології сприяють отриманню більш широких відповідей, що має значну цінність при проведенні опитувань з «гострих» або делікатних проблем. Респондент не намагається давати соціально бажані відповіді, що досить часто спостерігається при безпосередньому спілкуванні з інтерв’юером [8].

Разом з тим, слід зауважити декілька проблем при застосуванні Інтернет-опитувань. Перша проблема виникає у зв’язку з тим, що доступ до Інтернет має обмежена кількість людей (особливо це стосується України). Але ця проблема компенсується тим, що до Інтернету мають доступ люди, які вважаються найбільш інтелектуально активними.

При Інтернет-опитуваннях велика ймовірність викривлення інформації про себе з боку респондентів та багаторазової участі одних і тих же осіб в опитуванні. Але ця проблема може бути вирішена шляхом кореляції репрезентативності, врахування частоти звернення до електронної анкети при її аналізі з огляду на регіон (чи адресу) надходження даних.

У світовій практиці існує сім найбільш розповсюджених електронно-телекомунікаційних технологій проведення соціологічних досліджень: розсилка анкет електронною поштою (e-mail); розміщення текстових анкет у групах новин (newgroups); Інтернет-форуми, телеконференції (Bulletin Boards); веб-сторінки організацій, які проводять дослідження (анкети в форматі HTLM); стандартна веб-анкета державних установ; веб-анкета, що автоматично завантажується при зверненні до певного банера; on-line-фокус групи (визначених груп, які мають доступ до Інтернет та дали попередню згоду брати участь у різних соціологічних дослідженнях на певних умовах).

Довгий час Інтернет-соціологами використовується як універсальний метод соціологічного дослідження за допомогою електронної пошти. Техніка дослідження мало чим відмінна від традиційної техніки опитувань за допомогою ручки, паперу та звичайної пошти. Електронна анкета у вигляді текстів розсилається респондентам електронними листами. Для розсилки анкет використовуються списки e-mail адрес, які можуть формуватись у різний спосіб. Сучасні e-mail-опитування дозволяють за допомогою спеціальних комп‘ютерних програм проводити обробку результатів напівавтоматичне при отриманні заповнених анкет.

Як і в традиційному поштовому опитуванні, здійснюється декілька інтерактивних контрольних перевірок. Головними перевагами e-mail-опитування є його простота, дешевизна та висока швидкість збору даних.

Для розміщення текстів анкет в Інтернет використовуються також групи електронних новин певних інформаційних агентств (newgroups). Такі групи створюються для обслуговування певних тем новин, тому що мають велику цільову аудиторію користувачів. Кожна група має свій список учасників, який може використовуватися для складання вибіркового списку. Анкета відсилається у вигляді текстового повідомлення на сайт newgroups. Опитування респондентів відбувається інтерактивно або автономно. Маючи електронну копію анкети, респонденти можуть брати участь у дослідженні, зробивши необхідні відмітки чи набравши текст відповідей на клавіатурі свого комп‘ютера. Дані від респондентів надходять у вигляді електронних текстів, які потім дослідники самостійно обробляють.

Слід відзначити, що опитування в newgroups не можуть бути бездоганними, хоча вони мають певну перевагу: за потреби анонімність респондента реалізується шляхом відправки анкети через інші канали телекомунікацій. Існують певні цільові групи респондентів, які вважаються важко досяжними при проведенні досліджень, тобто яких у дійсності можна опитати тільки за допомогою цієї методики.

Технологія проведення опитування в Інтернет-форумах або телеконференціях відносно проста і не потребує значних витрат часу та фінансів. Інформація збирається протягом визначеного проміжку часу. Для цього необхідно знайти телеконференції з аудиторією, яка цікавить дослідників. Але для цього доцільно деякий час слідкувати за дискусіями в телеконференціях. Після цього, за згодою учасників, можна розмістити в телеконференції питання анкети. Вказана технологія особливо ефективна при опитуванні певної групи експертів.

Технології з використання веб-сторінок – це звичайна текстова анкета в HTML-форматі яка розміщується в електронному веб-середовищі (WWW). Всі питання

текстової анкети набувають форми єдиної сторінки. При цьому анкета може містити необмежену кількість запитань, які можуть бути як закритими (респондент відмічає необхідну відповідь), так і відкритими (респондент набирає необхідну відповідь за допомогою клавіатури на своєму персональному комп‘ютері). Відповіді респондентів можуть бути безпосередньо записані в базу даних чи надіслані на певну адресу електронної пошти в реальному часі (можливі комбінації обох процедур). Для проведення короткострокових простих досліджень, які не потребують комплексної обробки даних, веб-сторінка зарекомендувала себе як досить ефективна. Однак можливість зробити вибірку і цілеспрямовано залучати респондентів до участі в опитуванні при застосуванні цієї методики досить мінімальна.

Стандартна веб-анкета – це комп‘ютерна програма, яка містить питання анкети в стандарті HTML-форматі та розміщується на сайті певної організації в середовищі Інтернет. Ця анкета має деякі переваги: вона може містити максимально привабливу графіку та надавати максимальну кількість пояснень для респондентів. Такі технології дають можливість створювати більш складні електронні анкети. Стандартна веб-анкета може містити декілька веб-сторінок, які завантажуються по черзі. При запуску комп‘ютерної програми спочатку з’являється сторінка з анотацією дослідження та інструкцією до анкети. Гортаючи сторінки, респондент відповідає на питання, які одне за одним висвічуються на екрані монітора. Це дає змогу респонденту не відволікатись на попередні та наступні запитання анкети. На окремій сторінці респондент заповнює свої особисті дані, а потім вводить весь масив відповідей в базу для обробки. За допомогою високотехнологічних та адаптаційних комп‘ютерних програм, які створюють веб-анкету, дослідник може заздалегідь встановити стандарти більш гнучкого управління процесом вивчення on-line-середовища .

Вартість дослідження, проведеного із застосуванням технології веб-анкети значно вища, оскільки розробкою комп‘ютерних програмних пакетів для веб-анкети займаються фахівці (чи спеціалізовані компанії, провайдери Інтернет), які потім здійснюють і хостинг веб-ресурсів. Для подібних досліджень респонденти можуть запрошуватися уповноваженими особами цих компаній електронною поштою.

Веб-анкета, що самозавантажується, – один з найсучасніших методів on-line дослідження. Така анкета завантажується з Інтернет та запускається на заздалегідь встановлене комп‘ютерне програмне забезпечення, що підтримується безпосередньо дослідником. Це переміщує процедуру обробки даних з веб-сервера на комп’ютер респондента. Процедура заповнення анкети мало чим відрізняється від попередньої технології. Існує й інший варіант цієї методики – замовлення повної програми дослідження, яка може завантажуватись для одноразового використання [9].

On-line-фокус група по суті є on-line-інтерв’ю в реальному часі з кількома респондентами одночасно. Користувачі через Інтернет входять до сеансу дискусії, знаходять на екранах моніторів запропоновані модератором питання, а потім вводять свої відповіді з клавіатури власних персональних комп‘ютерів.

На сьогодні виділяють три види вибірки для on-line-опитування: необмежена, відібрана та “соціально завербована”.

В необмеженій вибірці може опинитись будь-який користувач Інтернету, який бажає прийняти участь в опитуванні. Ця вибірка визначається слабкою репрезентативністю та формується через список e-mail-адрес, які отримують різними доступними для дослідника методами. Разом з тим, ці списки не завжди реальні і відбивають бажану репрезентативність.

Відібрана вибірка формується з числа респондентів, які самі прийняли рішення про участь в опитуванні. Як правило, цю вибірку здійснює комп‘ютерна програма веб-анкети, в яку закладаються певні критерії бажаних респондентів. Потенційний респондент спочатку вводить свої особисті дані, а потім, за умови їх відповідності критеріям вибірки, переходить до заповнення анкети. У разі невідповідності вимогам вибірки респонденту може бути запропоновано відповісти на декілька несуттєвих для дослідження питань.

Слід зазначити, що при організації роботи в Інтернет необхідно дотримуватись всіх правил етики поведінки у цьому інформаційному середовищі. На цьому наголошують і автори, які описують методологію on-line-досліджень. У противному – можна отримати негативну реакцію тих, до кого звертаються з опитуваннями [10-13].

За експертною оцінкою найбільш сучасною і надійною є “соціально завербована” (панельна) вибірка, яка формується за допомогою Інтернет-панелі. Фактично – це база даних респондентів, яка постійно формується та оновлюється. Вона містить респондентів, які заповнили попередню анкету, та розподіляє їх за групами у відповідності до соціально-демографічних показників. Інформація, яку респондент добровільно повідомляє про себе, зберігається в таємниці і не може бути використаною в інших, не заявлених в дослідженні цілях. Фактично, Інтернет-панель надає дослідникам можливість до початку опитування отримати добровільну згоду респондента на участь у ньому. Якщо респондент зареєструвався, то це означає, що він згоден узяти участь в опитуванні і готовий не лише отримати електронне запрошення, але й адекватно реагувати на нього.

При створенні Інтернет-панелі необхідно намагатися, щоб на ній реєструвалися різні за статтю, віком та соціальним статусом респонденти. Тому залучення респондентів має бути випадковим, зазвичай це робиться за допомогою банерної реклами в Інтернеті на сайтах різної тематики. Крім того, дослідники значну увагу повинні приділити текстам для осіб, які ознайомлюють з панеллю, та інструкції з реєстрації на ній.

Інтернет-панель дає можливість залучати до участі в дослідженнях нових користувачів. При цьому збільшується керованість процесом формування вибірки і ефективність дослідження зростає. Деякі дослідницькі Інтернет-компанії спеціально створюють панелі, щоб формувати бази даних потенційних респондентів для тих організацій, які проводять соціологічні дослідження із використанням інформаційно-телекомунікаційних технологій.

У порядку перспектив подальшого розвитку напряму дослідження можна зазначити таке. Досить актуальним при проведенні соціологічного дослідження щодо правозастосування, зокрема у протидії корупції, із застосуванням комп‘ютерних інформаційних технологій залишається питання організаційно-правового забезпечення залучення респондентів до участі в опитуванні. Щодо цього, можна вести мову про напрацювання наукою інформаційного права теоретичних положень для практики правозастосування при проведенні соціологічних досліджень.

Висновки

Методики проведення соціологічних досліджень з використанням комп‘ютерних телекомунікаційних технологій постійно удосконалюються як у пошуках адекватного комп‘ютерного програмного забезпечення та дослідницького інструментарію, так і відносно можливостей дослідників оптимально керувати ходом опитування. Це дає підставу стверджувати, що подібні методики можуть ефективно бути використані в ході

впровадження моніторингу громадської думки щодо стану корумпованості не тільки у податкових органах України, й в інших державних органах влади.

Використана література

1. Українське суспільство-2003: Соціологічний моніторинг: зб. аналіт. матеріалів. – К., 2003. – С. 97.

2. М. Мельник. Корупція: сутність, поняття, заходи протидії: монографія. – К., 2001. – 304 с.

3.М. Мельник. Корупція – корозія влади (соціальна сутність, тенденції та наслідки, заходи протидії): монографія. – К., 2004. – 400 с.

4. Глазырин В.А. Коррупция в российском обществе (юридическая социология): учебн. – М., 2000. – С. 261-274.

5. Корупція в повсякденному житті підприємців та роль громадських організацій у її подоланні: результати соціологічних досліджень АЦ “Академія” // Підприємництво в Україні. – 2004. – № 34. – С. 19-20.

6. Кузьменко Б. Корупція та економічна злочинність у сучасній Україні: вплив на національну безпеку держави // Право України. – 1997. – № 7. – С. 12-14.

7. Іванюк Р. Основні етапи соціолого-правового дослідження проблем корупції та хабарництва // Вісник прокуратури. – 2003. – № 9. – С. 113.

8. Филиппова Т.В. Социология в интернете / Социологические исследования. – 2000. – № 5. – С. 134-135.

9. Филиппова Т.В. Интернет как инструмент социологического исследования / Социологические исследования. – 2001. – № 9. – С. 117-119.

10. Comley P. The use of the Internet as a date collection method / 1996. http://www.sga.co.uk.

11. Mehta R., Sivadas E. Comparing respouse rates and respouse content in mail versus electronic mail surveys // Journal of the Market Research Societi. – 1995. – P. 429-439.

12. Batinic B. How to make an internet based survey?, http://194.77.76.10.

13. Coomber R. Using the Internet for Survey Research, http://www.socresonline.org.uk.

14. Вступ до інформаційної культури та інформаційного права: монографія /[В.Цимбалюк, В.Гавловський, Р.Калюжний, М.Попович, М.Швець, О.Яременко]; за ред. М.Швеця та Р.Калюжного. – Ужгород: ІВА, 2003. – 240 с.

15. Правова інформатика: система інформатизація законотворчої, правозастосовсовчої, правоохоронної, судочинної та правоосвітньої діяльності в Україні: монографія /[М.Швець, В.Брижко, В.Гавловський, Л.Задорожня, Р.Калюжний, Ю.Клімашевська, В.Хахановський та ін.] ; за ред. М.Швеця, Р.Калюжного. – Ужгород: ІВА, 2003. – 168 с.

16. Правова інформатика /[Швець М.Я., Брижко В.М., Задорожня Л.М., Коваль М.І., Хахановський В.Г. та ін.]. У 2-х т. – К.: Парламентське видавництво, 2004. – Т.1. – 416 с.

17. Брыжко В. е-будущее и информационное право / [В. Брыжко, А.Орехов и др.] ; под. ред. Р.Калюжного и Н.Швеца. – К.: “Интеграл”, 2002. – 264 с.

18. Брижко В. Інформаційне суспільство. Дефініції… / [В. Брыжко, А.Орехов и др.] ; під. ред. Р. Калюжного і М. Швеця. – К.: “Інтеграл”, 2002. – 220 с.

УДК: 347.51:323.266

М. КРАСНОСТУП, генеральний директор ТОВ
“Центр інформаційної безпеки”
Г. КРАСНОСТУП, *магістр права*,
НДЦ ПО Національної академії ДПС України

ПИТАННЯ ВІДПОВІДАЛЬНОСТІ ЗА ПОШИРЕННЯ НЕДОСТОВІРНОЇ ІНФОРМАЦІЇ, ОТРИМАНОЇ В МЕРЕЖІ ІНТЕРНЕТ

Анотація. *У статті досліджено питання відповідальності за поширення недостовірної інформації в мережі Інтернет.*

Відвідувач у бібліотеці:
“Перепрошую, я бачу каталог книг, газет, журналів...
А де каталог Інтернету?” [1].

Відповідно до частини другої статті 32 та частини другої статті 34 Конституції України кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Частиною другою статті 46 Закону України “Про інформацію” встановлено, що не підлягають розголошенню відомості, що становлять державну або іншу передбачену законодавством таємницю.

Всесвітня інформаційна мережа під назвою “Інтернет” стала одним із найбільш впливових засобів поширення інформації у XXI столітті і водночас місцем зберігання цієї інформації.

Сьогодні у світі виникла ситуація, коли об’єм інформації, що став доступним користувачам Інтернету лише за 5 років XXI століття, майже дорівнює усій інформації, з якою працювало людство у XX столітті. Темпи накопичення інформації в інформаційному просторі продовжують стрімко зростати. Це пов’язано з різким збільшенням кількості людей які отримують доступ до мережі Інтернет, розширенням методів та пристроїв, що забезпечують вказаний вище доступ тощо. Сьогодні вже тисячі газет, журналів, телерадіоорганізацій поширюють інформацію не тільки на аркушах паперу або в радіоефірі, але й в мережі Інтернет. Значна частина медіа-видань вже існує виключно в Інтернеті, тобто медіа-простір розширюється за допомогою мережі Інтернет. Частка таких видань у майбутньому буде стрімко зростати, тому що витрати на створення медіа-ресурсу набагато менші, якщо він створюється в мережі Інтернет, а потенційна аудиторія – набагато більша порівняно з іншими мас-медіа.

Мережа Інтернет зараз перебуває у справжньому інформаційному бумі, і, як будь-яка інша подія у житті планети, цей бум має як позитивні, так і негативні наслідки.

З одного боку – це зростання обсягу інформації, що стала доступною для обробки та використання користувачами Інтернету, та прискорення обміну цією інформацією на планеті стає базою для стрімкого розвитку технологій та підвищення свідомості громадян різних країн.

З іншого – всесвітня інформаційна мережа є місцем, де можуть анонімно спілкуватися

терористи, пропагуватися расова та релігійна ворожнеча, дитяча порнографія тощо. Інтернет став місцем, де з’являється багато недостовірної інформації (тобто інформації, що не відповідає дійсності), яка інколи створюється з метою дискредитації певних осіб та урядів, а інколи і країн в цілому, що може призвести до страшенних наслідків у вигляді громадянських війн та військових конфліктів і, як наслідок, – до фізичної загибелі тисяч і тисяч людей.

Мережа Інтернет стала місцем розгортання інформаційних війн, що призводить до моральних, матеріальних, фінансових та людських втрат. Як зазначено в роботі С.П. Расторгуєва “Информационная война”: *“Сьогодні вже немає ніякої різниці між реальними бойовими діями та інформаційними війнами, тому що наслідки цих подій однакові”* [2].

Таким чином, ситуація, що складається у всесвітній інформаційній мережі та всесвітньому інформаційному просторі, як ніколи раніше потребує постійної уваги держави та її виконавчих органів. Теза “хто володіє інформацією, той володіє світом” стає актуальною як ніколи раніше.

Початковий опис проблеми був викладений у публікаціях ряду вітчизняних учених: В.А. Копилова, В.С. Цимбалюка та інших, і сьогодні можна стверджувати, що ця проблематика стала дуже актуальним напрямом наукових досліджень в Україні.

Мета статті – висвітлення кола суспільних відносин та засобів правового регулювання щодо відповідальності за поширення недостовірної інформації, отриманої з мережі Інтернет.

Усі питання, пов’язані з технологічним розвитком та інформаційним наповненням Інтернет, що потребують уваги держави можна умовно поділити на три напряму:

1. Розвиток інформаційного простору держави.
2. Захист державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу країни, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці. Попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності у сфері управління і економіки та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам країни.
3. Організаційно-правове забезпечення інформаційної діяльності на території країни.

Заходи щодо забезпечення пункту 1 здійснюються сьогодні Міністерством транспорту та зв’язку України.

Заходи щодо забезпечення пункту 2 сьогодні здійснюються Службою безпеки України. Відповідно до частини першої статті 2 Закону України “Про Службу безпеки України” на Службу безпеки України покладається у межах визначеної законодавством компетенції захист державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці. До завдань Служби безпеки України також входить попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності у сфері управління і економіки та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України.

Для вирішення різноманітних питань, які виникають у правоохоронних органів, урядами багатьох країн створені для них різноманітні системи контролю інформації, що

циркулює у мережі Інтернет, як глобальні, так і локальні. Найвідоміші з них – це американська глобальна система інформаційного контролю “ECHELON” та російська система “СОРМ”. Слід зауважити, що система “ECHELON” контролює не тільки інформацію, що поширюється у мережі Інтернет, але й ту, що поширюється з використанням радіоефіру взагалі (мобільний, телефонний, супутниковий, тропосферний та радіозв’язок тощо), а також практично увесь медіа-простір (газети, журнали, телебачення тощо) майже по всій земній кулі. Ця система контролюється Агентством національної безпеки США (NSA). Ознайомитися з інформацією про глобальну американську систему “ECHELON” можна по URL: *http://www.itc.ua/article.phtml?ID=3096*.

У США з урахуванням глобального росту терористичної загрози створено єдиний оперативний центр (JOI) Національного агентства розвідки геопростору (NGA, колись – NIMA, National Imagery and Mapping agency). Новий центр покликаний забезпечити більш повну інтеграцію всіх розвідувальних даних, отриманих найрізноманітнішими типами сенсорів. В JOI будуть використовуватися всі напрацювання NGA для збору, обробки й аналізу даних. Крім того, центр дозволить використати дані американської служби NSG для виконання спільних досліджень і забезпечення потреб безпеки США [3].

Ознайомитися з інформацією про російську систему “СОРМ”, яка контролюється ФСБ Росії, можливо по URL: *http://www.libertarium.ru/libertarium/sorm*.

Але створення подібних систем також має як позитивні, так і негативні наслідки, детальний аналіз яких містить стаття під назвою “Специальные разведывательные технологии США” з якою можна ознайомитися по URL: *http://www.bezpeka.com/ru/lib/sec /intell/art521.html*.

Стосовно заходів щодо забезпечення пункту 3, то слід зауважити, що відповідно до Постанови Кабінету Міністрів України від 04.03.2004 р. № 263 “Деякі питання поліпшення організації законопроектної діяльності” з 1 січня 2006 р. на Міністерство юстиції України згідно з Указом Президента України від 26.11.2003 р. № 1348 “Про поліпшення організації законопроектної діяльності” покладено функції головного розробника всіх проектів законів.

В Україні постало питання щодо можливості контролю на законодавчому рівні за достовірністю інформації, яка розміщена у мережі Інтернет на сайтах (сторінках), що є власністю фізичних або юридичних осіб.

Іншими словами, слід відповісти на питання – чи можливо, а якщо можливо – то як на законодавчому рівні врегулювати суспільні відносини щодо контролю за достовірністю інформації, що поширюється мережею Інтернет та в подальшому використовується іншими засобами масової інформації, які належать до так званого медіа простору, тобто газетами, журналами, теле-, радіоканалами тощо?

З метою вирішення згаданої проблеми слід знайти відповідь на низку питань, а саме:

- Що таке мережа Інтернет?
- Чи можливо сьогодні в Україні з її матеріальними, технічними та фінансовими ресурсами створити *систему контролю змісту інформації* в мережі Інтернет?
- Яку відповідальність несе провайдер доступу до мережі Інтернет?
- Хто може відповідати за достовірність інформації, що поширюється в Інтернеті?

Спробуємо відповісти.

Легальне визначення Інтернету встановлюється абзацом п'ятнадцятим статті 1 Закону України “Про телекомунікації”. Інтернет – *всесвітня інформаційна система*

загального доступу, яка логічно пов'язана глобальним адресним простором та базується на *Інтернет-протоколі, визначеному міжнародними стандартами.*

Для тих, хто не зовсім розуміє наведене визначення, зазначимо, що для отримання доступу в мережу Інтернет можливо використання супутникового зв’язку, телефонних ліній, мобільних телефонів, виділених ліній, радіостанцій тощо. Інформація, яку поширюють в мережі Інтернет, не має державних кордонів, тобто її розміщення можливо на серверах (комп'ютерах, веб-сайтах), фізично розміщених у будь-якій країні світу. І коли громадянин України отримує інформаційні матеріали з Інтернету, він не замислюється над тим, що фізично вони можуть бути розміщені на сервері, наприклад, в Зімбабве.

Таким чином, Інтернет – це інформаційний простір, який не має чітких державних кордонів, тобто зареєстрований інформаційний ресурс резидента України може знаходитися на сервері, що орендується на території США.

Висновок – для того щоб контролювати зміст інформації в мережі Інтернет, потрібно створення не локальної, в кордонах України, а глобальної системи *перехоплення* інформації, аналогічної американській системі “ECHELON”.

Слід підкреслити, що сьогодні в Україні *не існує жодного нормативно-правового акта* яким визначені такі поняття, як “Інтернет”, “Інтернет-ресурси”, *що відповідають реаліям сьогодення.*

Спробуємо розв’язатити згадану проблему за допомогою моделі юридичної відповідальності, коли на провайдерів буде покладено обов’язок відповідати за достовірність інформації поширеної (розповсюдженої, наведеної) в мережі Інтернет. І це тільки за умови, що провайдер розташований на території України і діє в межах законодавства України (хоча сьогодні можливо підключення користувача до провайдерів інших країн).

Відповідно до частини четвертої статті 38 цього ж Закону провайдери телекомунікацій діють у сфері телекомунікацій на підставі договору з оператором телекомунікацій – резидентом України та копії ліцензії цього оператора на відповідний вид діяльності у випадках, передбачених законом.

Згідно з пунктом 1 частини другої статті 63 цього ж Закону однією із умов надання телекомунікаційних послуг є укладення договору між оператором, провайдером телекомунікацій і споживачем телекомунікаційних послуг відповідно до основних вимог до договору про надання телекомунікаційних послуг, установлених Національною комісією з питань регулювання зв'язку.

Слід зауважити, що за станом на 16 серпня 2005 року вимоги до договору про надання телекомунікаційних послуг Національною комісією з питань регулювання зв'язку не встановлені. Слід також зауважити, що частиною третьою статті 16 Цивільного кодексу України встановлено, що суд може захистити цивільне право або інтерес в інший спосіб, що встановлений договором або законом.

Частиною другою статті 27 Закону України “Про телекомунікації” встановлено, що право власності та право на технічне обслуговування і експлуатацію телекомунікаційних мереж може належати будь-якій фізичній особі – суб'єкту підприємницької діяльності або юридичній особі, які є резидентами України, незалежно від форм власності.

Враховуючи наведене, оскільки доведення телекомунікаційних послуг через телекомунікації до споживача здійснюється на договірній основі, саме в ньому пропонуємо встановити обов'язок провайдера з'ясовувати повну інформацію щодо сторони за договором та перевіряти достовірність цієї інформації.

На цьому етапі дослідження проблеми постає логічне питання: а яким чином провайдер буде забезпечувати достовірність інформації щодо споживача (найменування, юридичної адреси, банківських реквізитів, достовірності печатки тощо) та змісту відомостей, які той поширює Інтернетом?

Зауважимо, що господарський договір укладається провайдером з користувачем на підставі документів, що надає споживач. Але провайдер не є оперативним підрозділом, який відповідно до частини першої статті 5 Закону України “Про оперативно-розшукову діяльність” має право здійснювати оперативно-розшукову діяльність (систему гласних і негласних пошукових, розвідувальних та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів). Крім того, сьогодні неможливо контролювати резидентів України та нерезидентів України, що знаходяться на території держави та поширюють інформацію в мережі Інтернет.

На цьому етапі дослідження слід зупинити увагу на практиці регулювання згаданих суспільних відносин в інших країнах. Так, в законодавстві США у сфері Інтернету діють два основних акти – прийнятий у 1996 році Закон про телекомунікації (“Telecommunication Act of 1996”, що є доповненням до федерального Закону “Communications Act of 1934” у вигляді нового параграфа 230 “Охорона особистого блокування і захист від образливих матеріалів”) і норми, що стосуються регулювання змісту Інтернет-ресурсів. Зазначені норми визначають, що ані провайдер, ані користувач інтерактивної комп'ютерної послуги не несуть відповідальності за зміст інформації, що публікується іншим провайдером, а також, що провайдер звільняється від відповідальності за дії з обмеження доступу до інформації, що розцінюється як образлива, недостовірна та що пропагує насильство та ін., а також дії з поширення засобів, призначених для здійснення цих дій [4, – С. 106].

Важливим прецедентом в іноземному законодавстві, що регулює відносини у сфері Інтернету, є німецький Закон від 1 серпня 1997 року “Про інформаційні та комунікаційні послуги”. На відміну від американського підходу, німецькі законодавці покладають на провайдерів послуг відповідальність за зміст інформації трафіка, наданого третьою особою, якщо вони інформовані про цей зміст і блокування його є технічно можливим й обґрунтованим. Тут в імперативній нормі провайдерові пропонується обов'язок із блокування “незаконної” інформації. Він також покладає на провайдера послуг відповідальність за зміст власної інформації, яку вони надають користувачам. Провайдер звільняється від відповідальності за зміст поширеної в мережі інформації у разі, якщо він забезпечує тільки доступ до неї [4, – С. 108].

Найважливішого значення сьогодні набуває робота з формування актів міжнародного законодавства, тому що на цьому рівні необхідно регулювати основну групу відносин, які виникають у віртуальному середовищі Інтернету, що не має географічних кордонів [5, – С. 250].

Слід підкреслити, що спроба контролювати достовірність інформації державними органами шляхом втручання в творчу діяльність журналістів може кваліфікуватися як цензура, а відповідно до статті 15 Конституції України цензура заборонена.

Постає логічне питання, а що слід зробити для того, щоб фізична або юридична особа не мала можливості поширювати інформацію в мережі Інтернет?

Відповідь одна – позбавити цю особу телефонного та мобільного зв’язку, комп’ютера, заборонити відвідувати Інтернет-кафе та інше.

Цікавим є те, що сьогодні можливо поширювати інформацію в мережі Інтернет таким чином, що не буде технічної можливості встановити цю особу, навіть за наявності такої глобальної системи перехоплення інформації, як “ECHELON”. Це можна

прослідкувати на прикладі пошуку правоохоронними органами США терористів, належних до “Аль-Каїди”, які постійно публікують в мережі Інтернет свої звернення до світової спільноти та погрози уряду США.

Уявімо ситуацію, коли у мережі Інтернет поширюється будь-яка інформація, яка дискредитує особу або навіть державну владу, і потім цю інформацію використовують друковані мас-медіа, телебачення та радіомовлення з посиланням на мережу Інтернет як джерело інформації. Важливим є те, що ці дві різні операції можуть робити одні й ті самі особи.

А коли ми бачимо, що не існує можливості контролювати розповсюдження інформації та її достовірність у мережі Інтернет, спадає на думку інший шлях щодо врегулювання проблеми.

Наведемо ще один приклад. Існує особа, що може бути як резидентом, так і нерезидентом України, яка за вигаданим комп’ютерним ім’ям (ніком) створює на сервері, що знаходиться на території іншої держави так званий Інтернет-ресурс (веб-сторінку, форум тощо), де публікує будь-що: підробне (змонтоване за допомогою спеціальних комп’ютерних програм) фото перших осіб держави, видатних діячів культури та спорту в обставинах, що компрометують їх честь та гідність, або аналогічні аудіо матеріали. Далі ці матеріали можуть публікуватися в друкованих засобах масової інформації, транслюватися телебаченням з посиланням на Інтернет.

Постає питання: хто має нести відповідальність за такі дії, а саме – за поширення недостовірної інформації, отриманої в мережі Інтернет?

Відповідь: всі, хто поширює згадану інформацію.

Як можна зупинити поширення згаданої недостовірної інформації?

Відповідь: Для газет, радіо та телебачення України – тільки через суд з усіма подальшими наслідками.

Якщо сайт, який поширює недостовірну інформацію, знаходиться на сервері іншої країни, тоді можна вчинити спробу написати листа провайдеру-резиденту іншої країни, в якій знаходиться сайт, з проханням закрити цей сайт, або звернутись до правоохоронних органів цієї країни з аналогічним проханням. І можна не сумніватись, що нам нададуть відповідь, що це буде зроблено одразу після отримання рішення суду стосовно особи, яка порушила Закон (поширення недостовірної інформації).

Сьогодні багато хто вважає, що достовірність інформації, що поширюється в мережі Інтернет, має контролюватися Службою безпеки України. Але слід враховувати і те, що до завдань зазначеного органу не належить забезпечення контролю за достовірністю інформації, у тому числі тієї, що поширюється в мережі Інтернет.

Підсумовуючи наведене вище, можна дійти тільки одного висновку: вирішення питання можливе тільки за умови внесення змін до законів, що мають стосуватись відповідальності “за неперевірку достовірності інформації”.

Так, частиною другою статті 302 Цивільного кодексу України встановлено, що фізична особа, яка поширює інформацію, зобов'язана переконатися в її достовірності.

За визначенням, наведеним Великою Радянською Енциклопедією, достовірністю є вірне відображення об’єктивної дійсності у свідомості людини [6, – С. 383].

Виняток із загального правила встановлюється частиною третьою цієї ж статті Кодексу, згідно з якою вважається, що інформація, яка подається посадовою, службовою особою при виконанні нею своїх службових обов'язків, а також інформація, яка міститься в офіційних джерелах (звіти, стенограми, повідомлення засобів масової інформації, засновниками яких є відповідні державні органи або органи місцевого

самоврядування), є достовірною. Фізична особа, яка поширює таку інформацію, не зобов'язана перевіряти її достовірність і не несе відповідальність в разі її спростування.

Згідно з частиною четвертою статті 277 Цивільного кодексу України спростування недостовірної інформації здійснюється особою, яка її поширила.

Частиною шостою цієї ж статті Кодексу встановлено, що фізична особа, особисті немайнові права якої порушено у друкованих або інших засобах масової інформації, має право на спростування недостовірної інформації у тому ж засобі масової інформації в порядку, встановленому законом.

Висновки та перспективи подальшого розвитку напряму

На практиці людина повинна довести істинність, тобто дійсність і міць, поцейбічність свого мислення [7, – С.148].

Таким чином, вирішення проблеми поширення засобами масової інформації недостовірних відомостей, отриманих за допомогою мережі Інтернет, вбачається в приведенні у відповідність до Цивільного кодексу України законів України, якими регулюються суспільні відносини щодо поширення інформації.

Так, слід внести зміни до частини другої статті 41 Закону України “Про друковані засоби масової інформації (пресу) в Україні”, згідно з якою порушенням законодавства України про друковані засоби масової інформації є, зокрема, поширення інформації, отриманої в мережі Інтернет, без попередньої перевірки її достовірності.

З урахуванням наведеного, слід внести відповідні зміни і до статті 42 цього ж Закону, якою встановлено умови звільнення від відповідальності редакції та журналіста.

Аналогічних змін потребує таття 46 Закону України “Про телебачення і радіомовлення”. Певних змін потребує і Закон України “Про інформацію”, зокрема, стаття 45^1.

Разом з цим, слід зауважити, що Україна сьогодні потребує розробки та впровадження нових законодавчих актів, пов'язаних з перспективами вступу України до СОТ та ЄС та перспективами роботи медіа-структур України в медіа-просторі єдиної Європи.

Крім того, дуже актуальною є розробка та впровадження нових законодавчих актів, спрямованих на врегулювання статусу суб'єктів інформаційних відносин у мережі Інтернет та встановлення підстав їх відповідальності.

Як показує життя та стверджують провідні міжнародні експерти у галузі інформаційних технологій, XXI століття – це століття інтелектуальної власності та інформаційних технологій. Саме тому є необхідним включення питання про ІТ-розвиток України в п’ятірку головних пріоритетних напрямів державної політики. Тільки за таких умов можна буде створювати “український інтелектуальний ринок високих технологій”.

Використана література

1. http://www.studzona.com/prikol/77.html.

2. С.П. Расторгуев Информационная война. – М.: Радио и связь, 1998.

3. Інтернет-форум “Технології розвідки для бізнесу”. http://www.it2b-forum.ru/index.php?showtopic =451.

4. Брыжко В. е-будущее и информационное право / [В. Брыжко, А.Орехов и др.] ; под. ред. Р.Калюжного и Н.Швеца. – К.: “Интеграл”, 2002. – 264 с.

5. Копылов В.А. Информационное право: учебник. – 2-е изд., перераб. и доп. – М.: Юристъ, 2003. – 512 с.

6. Большая Советская Энциклопедия / Под ред. Б.А. Введенского, 2-е изд., Т.5, 1952.

7. Маркс К. и Энгельс Ф. Избранные произведения, Т.2, 1949.

УДК 681.3

Д. ЛАНДЕ, *кандидат технічних наук*

2GW – МАЙБУТНЄ ІНТЕРНЕТУ

Анотація. *Розглядаються проблеми сучасного інформаційного простору Інтернет, показано, що основні складності його ефективного використання пов'язані сьогодні зі специфікою традиційного подання інформації. Представлено новий підхід, який одержав назву “веб другого покоління” або 2GW, що базується на семантичних методах роботи з інформацією. Дано аналіз основних складових 2GW, особливостей їх реалізації на сучасному етапі, у тому числі й адаптивний інтерфейс уточнення запитів, реалізований за участю автора.*

За 15 років свого існування Інтернет перетворився на найбільший у світі розподілений інформаційний ресурс завдяки декільком закладеним у його основу принципам. До цих принципів відноситься реалізація гіпертексту, що дозволяє інтегрувати неоднорідні інформаційні ресурси, використання простої, доступної розумінню користувачів мови розмітки HTML (що обумовило легкість публікації документів у мережі), природну, адаптовану до людської логіки систему навігації в гіпертекстовому середовищі.

Разом з тим, можливості подання й доступу до інформації в Інтернеті обмежувалися статичністю мови HTML, що обумовлювала тільки навігаційний доступ до ресурсів, практичну відсутність підтримки метаінформації, недосконаліть ідентифікації інформаційних ресурсів, і, найголовніше, той факт, що розмітка HTML відносилася тільки до зовнішнього подання документів, не стосуючись їх семантики.

На початку існування Інтернету невелика кількість веб-сайтів публікувала інформацію окремих авторів для відносно великої кількості відвідувачів. Сьогодні ситуація різко змінилася. Самі відвідувачі веб-сайтів стають авторами контенту, широко розвилися форуми, “живі журнали” тощо. Це веде до різкого росту обсягів інформації: тільки у відкритій частині Інтернету міститься понад 20 млрд. документів.

У міру розвитку Інтернету першого покоління його можливості розширювалися, еволюційно були додані динамічні компоненти, можливість керувати стильовими рішеннями, були розроблені й деякі принципи подання контенту, зафіксовані як рекомендації. У процесі цієї еволюції з'явилися Java-аплети та Java-скріпти, численні мета-теги, мова каскадних таблиць стилів CSS та інше.

Разом з цим, традиційному веб все ж таки властиві такі недоліки, як високий рівень інформаційного шуму, неможливість гарантування цілісності документів, відсутність можливості змістовного пошуку, обмеженість доступу до “прихованого” веб.

Над вирішенням названих проблемам працюють численні колективи вчених і фахівців в усім світі, зокрема, консорціум W3C, де під керівництвом засновника Інтернет Тіма Бернерса-Лі реалізується концепція семантичного веб [1]. Поряд із цією концепцією, революційний прорив обіцяє дати більш загальний підхід, а саме – веб-2, або, як його називають, “веб другого покоління” (2GW) [2], що містить у собі реалізацію концепції Семантичного веб, багаторівневу підтримку мета-даних, нові підходи до дизайну й відповідного інструментарію, технологію глибинного аналізу текстів (Text Mining), а також ідеологію веб-сервісів, базуючись на інформаційних ресурсах, накопичених у веб першого покоління. Таким чином, 2GW передбачає перегляд усього комплексу стандартів й архітектурних принципів Інтернету.

Сьогодні очевидно, що центральною ланкою інструментарію подання й обміну даними буде Розширювана Мова Розмітки (XML) [3], що лежить в основі Семантичного веб. Передбачається також використання нового принципу ідентифікації інформаційних ресурсів, формування нової архітектури веб-простору на основі багаторівневого подання інформаційних ресурсів і стандартизованих веб-сервісів.

Передбачається, що 2GW на початку буде базуватися на ресурсах (базах даних, сайтах, Інтернет-співтовариствах) таких популярних Інтернет-компаній, як Google, Amazon, eBay тощо.

Семантичний веб

Однією з основних частин 2GW, яку її творці вважають абсолютно самодостатньою, є Семантичний Веб (Semantic Web). Концепцію Семантичного веб висунув Тім Бернерс-Лі, один з основоположників Worl-Wide-Web і голова веб-консорціуму (W3C) на міжнародній конференції XML-2000, що пройшла у 2000 році у Вашингтоні.

Основна ідея цього підходу полягає в організації такого подання даних у мережі, щоб допускалася не тільки їх візуалізація, але й ефективна автоматична обробка програмами різних виробників. Шляхом таких радикальних змін концепції традиційного веб- передбачається перетворення його на систему семантичного рівня. Семантичний веб повинен забезпечити “розуміння” інформації комп'ютерами, виділення ними даних, що найбільше підходять за тими або іншими критеріями, і вже після цього – надання інформації користувачам [4].

Семантичний веб можна представити як симбіоз двох напрямів, перший з яких охоплює мови подання даних. На сьогодні основними такими мовами є Розширювана Мова Розмітки XML (eXtensible Markup Language) і Засіб Опису Ресурсів RDF (Resource Description Framework). Існує також ряд інших форматів, однак XML й RDF надають більше можливостей, тому вони мають статус рекомендацій W3C.

Другий, концептуальний напрям несе в собі теоретичну уяву щодо моделей предметних областей, які в термінології Семантичного веб називаються онтологіями. 10 лютого 2004 року консорціумом W3C була затверджена й опублікована специфікація мови мережних онтологій OWL (Ontology Web Language).

У результаті дві гілки Семантичного веб спираються на три ключові мови (відповідно, технології) [5]:

- специфікація XML, що дозволяє визначити синтаксис і структуру документів;
- механізм опису ресурсів RDF, що забезпечує модель кодування для значень, певних в онтології;
- мова онтологій OWL, що дозволяє визначати поняття й відносини між ними.

Семантичний веб використовує також й інші мови, технології й концепції, зокрема, універсальні ідентифікатори ресурсів, цифрові підписи, системи логічного висновку тощо.

Практична реалізація Семантичного веб критично залежить від існування веб-сторінок, що містять мета-дані, формування яких не входить у стандартний процес веб-розробки. Навряд чи вдасться змусити авторів веб-сторінок вручну індексувати свої ресурси за допомогою термінологічних словників, онтологій Семантичного веб. Очевидно, що інтегрувати існуючі ресурси Інтернету в 2GW (що передбачено базовою концепцією) можна тільки автоматично. Дане завдання є дуже складним, вимагає глибинного аналізу текстів (Text Mining), якій, у свою чергу, сьогодні бурхливо розвиваються.

Як приклад реалізації такого підходу можна навести техніку й методологію австрійсько-швейцарської групи розробників, призначену для створення семантично

анотованих веб-сторінок. Технологія WEESA (Web Engineering for Semantic Web Applications) дозволяє здійснювати автоматичну генерацію мета-даних у форматі RDF для структурованого контенту веб-сторінок. Для генерації мета-даних використовується Java-програма, що бере контент одного або декількох атрибутів у якості вихідних даних і повертає стандартну тріаду RDF (“об'єкт – атрибут – значення”). За твердженням авторів технології, вони вже успішно застосували техніку WEESA для обробки веб-застосувань на сайті Міжнародного віденського фестивалю. Там були магазин квитків, більше 60-ти описів різних заходів, а також архів за останні 52 роки. Експеримент показав, що WEESA добре підходить для розробки веб-застосувань Семантичної Мережі.

Пошукові системи

Оскільки кількість веб-сайтів продовжує стрімко збільшуватися, користувачі 2GW мають потребу у більш ефективних пошукових системах. Пошукові машини наступних поколінь повинні будуть краще класифікувати інформацію й наочніше її представляти. У майбутньому пошук не буде обмежуватися лише обробкою уведених ключових слів. Наприклад, до уваги буде братися місце розташування користувача. Системи стануть відслідковувати інтереси користувачів, роблячи пошук більше цілеспрямованим. Нове програмне забезпечення буде працювати з мультимедійною інформацією так само легко, як з текстом. Нові пошукові машини будуть “бачити” опубліковані в мережі текстові, аудіо- і відеоматеріали, які в цей час недоступні.

Останнім часом одержали поширення адаптивні інтерфейси уточнення запитів [5], найчастіше реалізовані шляхом кластеризації результатів первинного пошуку. З'явилося таке поняття, як метод “папок пошуку” (Custom Search Folders), що не зв'язується з певним алгоритмом кластеризації, а являє собою безліч підходів, загальне в яких – спроба згрупувати результати пошуку й представити кластери у зручному для користувачів вигляді.

До подібних механізмів можна віднести, наприклад, австралійський пошуковий сервер Mooter (*http://www.mooter.com*), на якому застосовується візуальний підхід до надання результатів пошуку по оброблюваних запитах шляхом згрупування результатів первинного пошуку за категоріями. Інший пошуковий сервер iBoogie (http://www.iboogie.com) також групує результати пошуку, але відображає їх у вигляді, близькому до екрана провідника Windows. Слова й словосполучення в інформаційних портретах, застосовуваних, наприклад, у системі Галактика Зум, також дозволяють адаптивно уточнювати первинні запити.

В інформаційному центрі “Електронні вісті” за участю автора була розроблена система InfoStream [7], що застосовується для вирішення завдань автоматизованого збору новітньої інформації з веб-сайтів, її обробки й забезпечення доступу до неї в пошукових режимах. Ця система охоплює понад 1200 веб-джерел – більше 30000 унікальних новітніх повідомлень на добу, при цьому в ретроспективних базах даних зберігається понад 20 млн. повідомлень. Для ефективної роботи з такими обсягами інформації найпростішого інформаційного портрета виявилося замало – знадобився “інформаційний альбом” – багатоаспектна добірка параметрів вибірки за заздалегідь складеним запитом. І така можливість була реалізована. При цьому, на відміну від більшості подібних систем, в InfoStream уточнюючі параметри пошуку задаються не заповненням складної форми розширеного пошуку, а вказуються шляхом вибору з інформаційного альбому, одержуваного в результаті пошуку за первинним запитом. Сьогодні в системі InfoStream інформаційний альбом, що відповідає первинному запиту, містить такі параметри, як ключові слова, рубрики, мови, країни. Зокрема, в адаптивному інтерфейсі системи істотно полегшений множинний вибір джерел інформації, що відповідають заданому запиту. Крім того, користувачу надано

можливість визначення характеристик розмірів документів, що шукаються. Передбачено й такий “екзотичний” параметр, як рівень насиченості документів цифровою інформацією, що є корисним, наприклад, при пошуку аналітичних документів, цінових таблиць, рейтингів тощо.

Експериментальною реалізацією ідеї колективної роботи в Інтернеті, що входить у концепцію 2GW, стала пошукова система Snap (*http://www.snap.com*), що забезпечує не тільки пошук веб-сторінок за ключовими словами, але й надає додаткову інформацію, близьку інтересам користувачів. Наприклад, до результату пошуку щодо виробників цифрових камер додається порівняльна таблиця моделей, які раніше були викликані іншими користувачами системи. Розроблювач системи Білл Гросс вважає, що Snap стала першою системою з “хвостовими даними” (data trail), але незабаром таких систем стане більше. Ця пошукова система є провісником такого етапу розвитку Інтернет, на якому в ній будуть активно використовуватися результати роботи всього співтовариства користувачів.

Нові пошукові системи поліпшують якість результатів, усе глибше зариваючись у доступні сховища інформації, сортуючи її, і представляючи результати з обліком персональних користувальницьких переваг. Так недавно портали Amazon, Ask Jeeves й Google оголосили про впровадження механізму поліпшення результатів пошуку, який базується на персоналізації. Пошукові машини *www.A9.com* (проект Amazon) і *www.MyJeeves.ask.com* (проект Ask Jeeves) не тільки відслідковують запити й знайдені веб-сторінки, але й дозволяють зберігати їх у вигляді закладок. Користувач MyJeeves може багаторазово переглядати накопичені результати, які являють собою персонально організовану область Інтернету. Подібні функції підтримує й портал *www.A9.com*, на якому пропонується набір сторінок, сформований при аналізі особистої пошукової історії. Історії пошукових запитів на сайтах A9 й MyJeeves зберігаються на серверах пошукових систем. У системі Google користувач може вибрати з ієрархічного списку найбільш важливі для нього теми й указати ступінь свого інтересу до тієї або іншої області знань. Всі ці дані враховуються системою при оцінці результатів пошуку.

“Прихований” веб

2GW припускає відкрити доступ до “прихованого” веб. Більша частина змісту сайтів Інтернету першого покоління залишається недоступною для пошукових машин, тому що багато веб-серверів зберігають і переробляють інформацію не у тому вигляді, в якому вона надається відвідувачеві. При цьому багато веб-сторінок генеруються тільки тоді, коли користувачі звертаються до них. Традиційні мережні агенти не вміють працювати з подібними ресурсами й не в змозі визначити їх зміст. “Прихований” веб охоплює в першу чергу вміст он-лайнових баз даних [8]. Прихованою є й швидко обновлювана інформація – новини, конференції, он-лайнові журнали.

У 2000 році американська компанія BrightPlanet (*http://www.brightplanet.com*) опублікувала сенсаційну доповідь [9], в якій стверджувалося, що в Інтернеті в сотні разів більше сторінок, ніж їх удалося проіндексувати найпопулярнішими пошуковими системами.

На сьогодні розроблений цілий клас програм, що одержали назву пакувальників (wrappers). У цих програмах, щоб одержати доступ до “прихованого” змісту веб-сторінок, використовується звичний синтаксис пошукових запитів і стандартний формат он-лайн ресурсів. В інших системах реалізуються переваги програмного інтерфейсу, що дозволяє використати стандартний набір команд й операцій.

Для пошуку в “прихованій” мережі, а саме – в тому її сегменті, що становлять бази даних, сьогодні вже існують деякі спеціалізовані ресурси. Серед них, наприклад, системи BigHub (*http://www.bighub.com*) і InvisibleWeb (*http://www.invisible-Web.net*)

компанії IntelliSeek. Сайт Invisible Web містить у собі каталог баз даних, більшість із яких не проіндексовані відомими пошуковими машинами. При введенні запиту цей сайт видає посилання на ресурси, за допомогою яких пошук необхідної інформації стане найбільш оптимальним. На цьому сайті Криса Шермана (Chris Sherman) і Гарі Прайса (Gary Price) зібрані колекції посилань на різні бази даних, серед яких є чимало унікальних ресурсів, наприклад, збірник спічів політиків і бізнесменів. Програмний пакет BullsEye компанії IntelliSeek здійснює пошук більш ніж у 800 мережних ресурсах.

У 2005 році компанія Yahoo також запустила тестову версію пошукового сервісу, орієнтованого на роботу з базами даних сайтів. Він може проводити пошук не тільки у загальнодоступних сайтах, але й у ресурсах, що надають платну інформацію, – таких, як он-лайнова версія Wall Street Journal, що стягує з відвідувачів певну плату. Сервіс одержав назву DeepWeb і доступний поки що тільки для мешканців США та Великобританії.

Але все ж таки лідером серед навігаторів у “прихованому” веб є сайт CompletePlanet (*http://www.completeplanet.com*) компанії BrightPlanet. Цей сайт – найбільший каталог, що нараховує понад 100 тисяч посилань. Компанія BrightPlanet також створила персональну утиліту для пошуку в он-лайнових базах даних – LexiBot, яка може забезпечувати пошук у декількох тисячах пошукових систем “прихованого” веб. Метапошуковий пакет DeepQueryManager (DQM) цієї ж компанії забезпечує пошук у 55 тисячах “прихованих” веб-ресурсах.

Пошук і глибинний аналіз текстів

Пошукові технології 2GW повинні стати більш ефективними за рахунок потужних технологій, що поєднують пошук і глибинний аналіз текстів (Text Mining), знаходження аномалій і трендів у текстах. Одночасно ці технології будуть неявними завдяки операціям інтелектуального пошуку, що вбудовані в інтерфейси “за замовчуванням”. В остаточному підсумку пошук інформації в 2GW стане нерозривно пов'язаним з її осмисленням.

Існує чотири основних види застосувань технологій Text Mining, які повинні знайти своє втілення в веб другого покоління [10]:

- класифікація тексту, у якій використовуються статистичні кореляції для побудови правил розміщення документів у визначені категорії;
- кластеризація, що базується на ознаках документів та використовує лінгвістичні й математичні методи без використання визначених категорій. Результат – таксономія або візуальна карта, що забезпечує ефективне охоплення великих обсягів даних;
- семантичні мережі, або аналіз зв'язків, які визначаються дескрипторами (ключовими фразами) у документах для забезпечення навігації;
- витяг фактів, призначений для одержання деяких фактів з тексту з метою поліпшення класифікації, пошуку й кластеризації.

Нещодавно компанія Google представила свої наробітки й плани щодо кластеризації знайдених документів у рамках технології Text Mining. Демо-версія цієї системи дозволяє виділяти з документів назви компаній, які є основними критеріями кластеризації.

Можна назвати ще кілька завдань технології Text Mining, наприклад, прогнозування, що полягає в тому, щоб прогнозувати за значеннями одних ознак об'єкта значення інших. Ще одне завдання – знаходження аномалій, тобто пошук об'єктів, які своїми характеристиками сильно виділяються із загальної маси. Для цього спочатку з'ясовуються середні параметри об'єктів, а потім досліджуються ті об'єкти, параметри яких найсильніше відрізняються від середніх значень. Подібний аналіз часто проводиться після класифікації для того, щоб з'ясувати, наскільки остання була точною.

Трохи окремо стоїть завдання пошуку пов'язаних ознак (феноменів, понять) в окремих документах. Від прогнозування це завдання відрізняється тим, що заздалегідь невідомо, за якими саме ознаками реалізується взаємозв'язок; ціль саме в тому й полягає, щоб знайти зв'язки ознак. Це завдання подібне до кластеризації, але не за безліччю документів, а за безліччю властивих їм ознак.

І нарешті, для обробки та інтерпретації результатів Text Mining велике значення має візуалізація. Візуалізація в 2GW на основі систем Text Mining передбачається як засіб надання контенту всього масиву документів, а також для реалізації навігаційного механізму, що може застосовуватися при дослідженні документів та їх класів.

Веб-сервіси

Одним із ключових елементів 2GW є веб-сервіси – автономні, модульні додатки, призначені для реалізації інформаційних процесів у мережі (зокрема, бізнес-процесів [11]). Веб-сервіси спираються на ряд галузевих стандартів: WSDL (для опису), UDDI (для інформування й публікації) і SOAP (для обміну повідомленнями).

У серпні 2002 року, усвідомивши складність звернення до веб-сервісів у синхронному й асинхронному середовищах, корпорації BEA, IBM, Microsoft, SAP і Siebel у результаті спільних зусиль розробили мову реалізації бізнес-процесів для веб-сервісів (Business Process Execution Language for Web Services, BPEL4WS або просто BPEL). Мова BPEL дозволяє описувати бізнес-процеси й те, як вони пов'язані з веб-сервісами, а також як бізнес-процеси використовують веб-сервіси для досягнення поставлених завдань. BPEL можна розглядати як декларативно-процедурну мову програмування. BPEL являє собою діалект мови XML. Як й у будь-якій мові програмування, в BPEL визначені зарезервовані слова (теги XML):

- Виклик операції за допомогою веб-сервісу (<invoke>).
- Очікування зовнішнього повідомлення (<receive>).
- Генерація відповіді для вхідних/вихідних даних (<reply>).
- Очікування протягом деякого часу (<wait>).
- Копіювання даних між позиціями (<assign>).
- Індикація помилки або збійної ситуації (<throw>).
- Зупинка реалізації всього сервісу (<terminate>).
- Відсутність дій (<empty>).
- Визначення послідовності виконання дій (<sequence>).
- Розгалуження за допомогою оператора вибору (<switch>).
- Визначення циклу (<while>).
- Виконання одного з декількох альтернативних маршрутів (<pick>).
- Індикація того, що крок повинен бути виконаний паралельно (<flow>).
- Індикація обробки помилкової логіки за допомогою <throw> й <catch>.

На цей час уже існує безліч веб-сервісів, однак іншим програмам немає можливості розшукати в мережі веб-сервіс, що виконує ту або іншу функцію. Необхідний для підвищення ефективності роботи веб другого покоління процес, який називають виявленням сервісів, стане можливим лише після того, як поширеться наведена вище або подібна їй уніфікована мова, яка дозволяє описувати сервіси, для того щоб агенти могли “розуміти”, що дозволяє робити даний сервіс та яким чином ним користуватися. Наприклад, у рамках Семантичного веб-агенти виробника сервісу й агенти його користувачів можуть досягти розуміння один одного шляхом обміну онтологіями, що містять необхідні для спілкування термінологічні словники. Більше того, агенти зможуть навіть самі, знаходячи нові онтології, удосконалювати свої алгоритми.

Семантика мови опису сервісів (наприклад, BPEL) дозволяє агентові описувати, які саме функції він може виконувати і які вхідні дані йому потрібні. Технологія виявлення веб-сервісів відразу ж знайде своїх користувачів. Наприклад, у сфері малого бізнесу стане набагато простіше налагоджувати проведення трансакцій в області електронної комерції, що мають більший ступінь захисту й автоматизації.

Формат RSS

У веб другого покоління інформація небіто “відчужується” від джерела.. Відповідно, передбачається широке застосування формату RSS (Really Simple Syndication, Rich Site Summary, RDF Site Summary), спеціально призначеного для легкого й швидкого обміну змістом веб-сайтів [12]. RSS забезпечує погоджений засіб резюмувати зміст веб-сайтів, а крім того, його застосування дозволяє адміністраторам сайтів новин, он-лайнових щоденників, форумів та інших часто обновлюваних веб-ресурсів одержувати простий уніфікований метод подачі інформації про події, що відбуваються.

Сьогодні RSS прийнято розглядати у першу чергу як формат, призначений для публікації й забезпечення експорту новин на новинних сайтах. Після того як інформація перетворена у формат RSS, програма, орієнтована на цей формат, може завантажувати відомості про відновлення веб-сайтів і залежно від результату виконувати певні дії, наприклад, автоматично оновлювати список актуальних інформаційних повідомлень.

Користувачі можуть одержати доступ до даних у форматі RSS за допомогою спеціальних програм, які називають RSS-агрегаторами. Програма-агрегатор дозволяє групувати публікації з різних джерел, забезпечуючи можливість одночасно стежити за появою новин на всіх сайтах, не вимагаючи відвідування кожного сайта окремо. При цьому, звичайно ж, не потрібно завантажувати з мережі зайвої інформації, що стосується, наприклад, оформлення веб-сторінок.

Програми-агрегатори (або парсери) виконують синтаксичний розбір даних, наведених у форматі RSS, після чого можуть реалізовувати будь-які дії стосовно цих даних, приміром, відображати їх на обраному веб-сайті.

Перспективність і популярність RSS як стандарту обумовлена насамперед його доступністю й простотою. Сьогодні практично всі провідні інформаційні сайти у світі використовують RSS як інструмент оперативного подання своїх оновлень.

Про перспективність RSS уже сьогодні свідчать і спроби використання її в рекламному бізнесі. На конференції веб 2.0, що проходила у Сан-Франциско, один з керівників компанії Yahoo Ден Розенвейг (Dan Rosensweig) заявив, що їхня система контекстної реклами Overture буде експортувати посилання в RSS-канали.

Дизайн

2GW розглядається у першу чергу як ефективне середовище для роботи з контентом. Природно, нова концепція висуває нові вимоги до засобів візуалізації інформації, дизайну. Сьогодні створення інструментарію дизайнерів для роботи з веб другого покоління є передовим фронтом впровадження технологій 2GW. Уже сьогодні створюються інтерфейси, які агрегують інформацію з тисяч джерел. Так Amazon.com (*http://www. amazon.com*) дає доступ до своєї бази даних через відкритий API. Кожен бажаючий може створити персоналізований, більш дружній, на його думку, інтерфейс користувача, що володіє функціональністю сайта-першоджерела (наприклад, Amazon Light, *http://www.kokogiak.com/amazon*).

Як основну мову розмітки веб-сторінок передбачається використати XML. Колишні мови розмітки – HTML й XHTML – вирішували переважно завдання відображення інформації, у той час як XML призначений для її опису.

Передбачається, що у 2GW буде реалізовані персоналізована, незалежна навігація й керування веб-сайтом. Тобто користувач сам зможе контролювати візуальний інтерфейс. Разом з цим, передбачається, що дизайнер ресурсів 2GW буде у більшій мірі програмістом, якій за допомогою інструментальних засобів буде визначати елементи структури, навігації й дизайну веб-сайта [2]. Технологічні, інтуїтивні інтерфейси – це те, до чого повинні прагнути дизайнери сайтів 2GW. Як найбільше технологічні сайти нового покоління вже сьогодні можна назвати картографічний сервіс Google Maps (*http://www.maps.google.com*), фотосервіс Flickr (*http://www. flickr.com*), а також Інтернет-співтовариство Del.icio.us (*http://www.del.icio.us*).

Перспективи

Передбачається, що наступний щабель розвитку Інтернету буде визначатися технологіями роботи з величезним обсягом інформації, що накопився у мережі. Зокрема, веб другого покоління повинен характеризуватися переходом від мережі документів до мережі даних, які при необхідності агрегують у семантично зв'язані документи за допомогою веб-сервісів нового покоління. Передбачається існування єдиного інформаційного простору у вигляді безлічі одиниць даних, які можуть розміщатися на численних сайтах. Користувач буде одержувати документ шляхом агрегування у себе на комп'ютері інформаційних одиниць, розподілених в Інтернеті.

Перспективи 2GW будуть багато у чому залежати від інфраструктури, у рамках якої будуть працювати програмні продукти з боку веб-серверів і користувачів. На думку багатьох учених й учасників Інтернет-ринку, веб другого покоління буде більшою мірою, ніж сьогодні пристосований для автоматизованої обробки, використання комп'ютерами. Завдяки цьому споживачі будуть мати справу з інформацією, зібраною провідними інформаційними компаніями, і створювати нові сервісі.

Використана література

1. Tim Berners-Lee, James Hendler, Ora Lassila, The Semantic Web, Scientific American, May 2001 (http://www.sciam.com/article.cfm?articleID=00048144-10D2-1C70-84A9809EC588EF21).

2. Chris Preimesberger. Web 2.0: Possibly the best IT business conference of 2004 // NewsForge, 2004 (http://www.newsforge.com/article.pl?sid=04/10/08/0849201).

3. Ландэ Д.В. На границе стихий // ЧИП-Украина. – 2003. – №. 5. – С. 72-77.

4. Семантический Вэб: воплощение идеи Телеком. – 2005. – № 6. – С. 60-65.

5. Фурашев В.М., Ланде Д.В., Григор’єв О.М., Фурашев О.В. Електронне інформаційне суспільство України: погляд у сьогодення і майбутнє. – К.: Інжиніринг. – 2005. – 164 с.

6. Григорьев А.Н., Ландэ Д.В. Адаптивный интерфейс уточнения запросов к системе контент-мониторинга InfoStream //Труды Международного семинара “Диалог’2005”. – 2005. – С. 109-111.

7. Григорьев А.Н., Ландэ Д.В. Система мониторинга новостей InfoStream – информационное пространство из одних рук. Построение информационного общества: ресурсы и технологии : тезисы докладов и информационные материалы XI международной научно-практической конференции. – К.: УкрИНТЭИ. – 2005. – С. 17-20.

8. Ландэ Д.В. Затерянный вэб // “Телеком”. – 2005. – №. 1. – С. 46-51.

9. Danny Sullivan. Invisible Web Gets Deeper // The Search Engine Report. – 2002. (http://searchenginewatch.com/sereport/article.php/2162871).

10. Ландэ Д.В. Поиск знаний в Internet. Профессиональная работа. – М.: Издательский дом “Вильямс”. – 2005. – 272 с.

11. Шапошников И. Веб-сервисы Microsoft.NET. – СПб.: БХВ-Петербург. – 2002. – 334 с.

12. Ландэ Д.В, Морозов А.Ю. Новостной Интернет / “Телеком”, – 2005. – № 1-2. – С. 58-62.

УДК 681.3:004.5

В. ХАХАНОВСЬКИЙ, *кандидат юридичних наук, доцент*
В. СМАГЛЮК, *кандидат технічних наук, доцент*

ТЕРМІНОЛОГІЧНІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ СТВОРЕННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ ОВС УКРАЇНИ

Анотація. *Щодо застосування експертних систем для вирішення управлінських завдань в ОВС України.*

Відомо, що одним із заходів програми інформатизації органів внутрішніх справ України є затвердження технічного завдання на створення інформаційно-аналітичної системи ОВС України. Над цією проблемою працюють науковці і практичні працівники Департаменту інформаційних технологій МВС України. На наш погляд, існує необхідність висловити деякі думки, які можуть бути корисними при вирішенні зазначеного завдання.

Під *інформатизацією* взагалі розуміється сукупність взаємопов’язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб, реалізації прав громадян і суспільства на основі створення, розвитку, використання інформаційних систем, мереж, ресурсів та інформаційних технологій, побудованих на основі застосування сучасної обчислювальної та комунікаційної техніки [1]. Термін “*інформатизація*”, використаний вже у самій назві програми означає, що для вирішення завдань інформаційного забезпечення органів внутрішніх справ передбачене використання інформаційних технологій, які реалізуються відповідними засобами, а саме – *засобами інформатизації*, під якими розуміють електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, інформаційні системи або їх окремі елементи, інформаційні мережі і мережі зв’язку, що використовуються для реалізації інформаційних технологій [1].

Виходячи з використаної термінології – *“інформаційно-аналітична система”,* вона має забезпечувати автоматизацію як інформаційної, так і аналітичної роботи. Останнім часом з’явилося безліч публікацій, а також посилань та веб-сайтів у мережі Інтернет, де йдеться про інформаційно-аналітичні системи, розроблені в різноманітних галузях. На жаль, ці джерела носять, здебільшого, декларативний, констатуючий характер, в них, як правило, відсутні чітке визначення інформаційно-аналітичні системи та принципи її формування.

На нашу думку, для з’ясування поняття “інформаційно-аналітичні системи” необхідно проаналізувати такі складові цього системного утворювання, як “інформаційна робота”, “аналітична робота” тощо.

Інформаційна робота розуміється як діяльність із забезпечення посадових осіб відомостями, необхідними для розв’язання покладених на них завдань.

Аналітична робота розглядається як складова частина творчої діяльності і призначена для оцінювання інформації та підготовки прийняття рішень. Аналітична робота складає основний зміст повсякденної роботи кожного керівника і окремого працівника, вона полягає у приведенні розрізнених відомостей у логічно обґрунтовану систему залежностей (просторово-часових, причинно-наслідкових та інших), що дозволяють правильно оцінити як усю сукупність фактів, так і кожний з них окремо.

Під аналізом інформації розуміють сукупність методів формування фактичних даних, що забезпечують їх порівнянність, об’єктивну оцінку і вироблення нової вивідної інформації. У свою чергу вироблення нової інформації – це вилучення вмісту з всієї маси початкових даних, відшуковування зв’язків і взаємозалежностей між відомостями, що зіставляються [2].

Враховуючи викладене вище, на наш погляд, на етапі створення інформаційно-аналітичної системи ОВС України виникає багато запитань, а саме: це окрема, самостійна система чи розвиток існуючої системи інформаційного забезпечення ОВС України? Хто має бути користувачем цієї системи? Які завдання вона повинна виконувати?

Аналіз структури, складу, функцій існуючої нині системи інформаційного забезпечення ОВС свідчить, що ця система вже виконує завдання автоматизації інформаційної роботи (з тим чи іншим ступенем ефективності). Інформаційні підсистеми ОВС успішно вирішують притаманні їм задачі кількісного перетворення інформації (інформаційне згортання та консолідація значних інформаційних масивів у вигляді баз і банків даних) і її структурного упорядкування (систематизація, предметизація тощо). Тому доцільним було б до функцій існуючої системи додати аналітичну складову, тобто йти шляхом її розвитку до вирішення завдання якісно-змістовного перетворення інформації (виробництва нового знання на основі переробки наявної інформації з метою оптимізації прийняття рішень).

Визначення аналітичної роботи свідчить, що її виконує кожна посадова особа ОВС, однак очевидно, що повна автоматизація цієї діяльності сьогодні є неможливою й недоцільною з багатьох причин. Тому необхідно визначатись з функціональними і структурними пріоритетами.

Досвід створення та використання інформаційно-аналітичних систем у інших галузях свідчить, що головною сферою їх застосування є управлінська діяльність, оскільки аналітична робота є невід’ємною і найважливішою складовою управлінської діяльності і виступає не епізодичним, короткочасним актом, а функцією усіх ланок системи, яка здійснюється постійно.

Аналітична робота в органах внутрішніх справ – це постійна дослідницька діяльність (функція процесу управління), що охоплює своїм змістом широкий комплекс організаційних заходів і методичних прийомів для вивчення і оцінки інформації про стан злочинності та громадського порядку, результати практичної діяльності органів з виконання поставлених перед ними завдань, а також про умови, в яких ці завдання виконуються, і яка забезпечує цілеспрямоване управління та оцінку ефективності управляючих впливів [3]. Отже, система, насамперед, має бути орієнтована на забезпечення управлінської діяльності.

Аналітична робота в органах внутрішніх справ здійснюється всіма галузевими підрозділами на всіх рівнях. Вимоги до організації аналітичної роботи для кожного рівня системи різні у зв’язку з різними завданнями на цих рівнях і їх неоднаковими можливостями. Як складова управлінської діяльності аналітична робота притаманна кожному структурному підрозділу і працівнику. Однак, маючи забезпечувальний характер, вона більше розвинута на центральному рівні МВС України, а також на рівнях ГУМВС та УМВС, де існують відповідні аналітичні підрозділи [3]. Тому створення інформаційно-аналітичної системи ОВС України слід починати з центрального рівня системи управління, поступово переходячи на інші рівні зверху донизу (згідно з принципом системного підходу).

Слід зазначити, що автоматизація аналітичної роботи на сучасному етапі розвитку інформаційних технологій передбачає використання інтелектуальних програмних систем, серед яких найбільш поширеними є експертні системи (ЕС).

Експертні системи – це вид інтелектуальних програмних систем, які здатні отримувати, накопичувати, корегувати знання з деякої предметної галузі (що надаються в основному експертами), виводити нові знання, вирішувати на основі цих знань практичні завдання та пояснювати хід їх вирішення. Тобто, експертна система – це комп’ютерна програма, яка оперує знаннями у визначеній предметній галузі з метою вироблення рекомендацій або вирішення проблем [4]. При цьому під *знаннями* розуміють основні закономірності предметної галузі (факти, поняття, правила, оцінки, взаємозалежності, евристики, а також стратегії прийняття рішень у цій галузі), які дають людині змогу вирішувати конкретні професійні завдання. Знання – це сукупність відомостей, які створюють цілісний опис, що відповідає деякому рівню обізнаності про питання, предмет, проблему, що описуються. ЕС здатні вирішувати й неформалізовані завдання, тобто завдання, які мають такі характеристики: не можуть бути заданими в числовій формі; їх цілі не можуть бути відображені в термінах точно визначеної цільової функції; не існує алгоритмічного рішення завдань; алгоритмічне рішення існує, але його не можна використати через обмеженість ресурсів (час, пам’ять).

Сфера застосування ЕС постійно поширюється, досягнуті значні результати при вирішенні реальних завдань, у тому числі – в управлінні. Ці успіхи обумовили значну зацікавленість експертними системами не тільки фахівців-теоретиків, а й практичних працівників у різноманітних галузях людської діяльності. Так, ще у 1975 р. у Гейдельбергському і Дармштадтському університетах була розроблена одна з перших юридичних ЕС –“Judith”. Причини такого інтересу такі: по-перше, ЕС орієнтовані на вирішення широкого кола завдань у неформалізованій галузі, що раніше вважалося малодоступним для обчислювальної техніки; по-друге, ЕС призначені для роботи фахівців, які не мають навичок програмування, що дає змогу поширення сфери використання обчислювальної техніки; по-третє, ЕС призначені для вирішення практичних завдань і при цьому дають результати, не гірші (а часто навіть переважають) тих, що може отримати людина-експерт, користуючись традиційними засобами [5].

За типом використовуваних методів і знань ЕС поділяють на традиційні та гібридні. Традиційні ЕС використовують в основному неформалізовані методи і неформалізовані знання, отримані від експертів. Гібридні ЕС використовують як неформалізовані, так і формалізовані методи, а також дані традиційного програмування та математики. Для вирішення управлінських завдань на рівнях МВС України, ГУМВС, УМВС, де при підготовці рішень широко використовуються обчислювальні (формалізовані) методи, найбільш корисними можуть бути гібридні експертні системи.

Використана література

1. Закон України від 04.02.98 р. № 74/98-ВР “Про Національну програму інформатизації”.

2. И.Н. Кузнецов. Информация: сбор, защита, анализ: учеб. по информационно-аналитической работе. – М.: Яуза, 2001.

3. В.Плішкін. Теорія управління органами внутрішніх справ. – К.: НАВСУ, 1999.

4. Джексон П. Введение в экспертные системы ; пер. с англ. – М.: Изд. дом “Вильямс”, 2001.

5. Искусственный интеллект: Кн. 1. Системы общения и экспертные системы: справочник ; под ред. Э.В. Попова. – М.: Радио и связь, 1990.

УДК 342.721:681.3.02(477)

В.БРИЖКО, *кандидат юридичних наук,*
заслужений винахідник Республіки
М.ШВЕЦЬ, *доктор економічних наук, професор,*
член-кореспондент АПрН України

ДО ПИТАННЯ ЕКОНОМІЧНОГО АСПЕКТУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У КОНТЕКСТІ ПРАВА ВЛАСНОСТІ НА ІНФОРМАЦІЮ

Присвячується пам’яті Опанаса Андроновича Підопригори, доктора юридичних наук, професора, академіка Академії правових наук України, який одним з перших серед провідних фахівців у сфері цивільного права підтримав можливість запровадження в інформаційному законодавстві України нової юридичної категорії – “виключне право власності фізичної особи на свої персональні дані” [*]

Анотація. *Стаття стосується пошуку вирішення питань захисту інформаційних ресурсів, зокрема, персональних даних, які в реаліях глобалізації економіки повинні супроводжуватися законодавчим оформленням права власності на них.*

1. Широкі, майже безмежні можливості сучасних інформаційно-комп'ютерних технологій та мереж щодо збору, об'єднанню, класифікації персональних даних за певною ознакою (зокрема, ідентифікаційному номеру) дозволяють довідатися про людину все та взагалі використовувати персональні дані з невідомою та мабуть небажаною для неї ціллю (наприклад, складання та поширення її “інформаційного портрету”). Взагалі зазначені можливості є надзвичайно зручними для приватних інститутів і держави: не випадково основним мотивом запровадження автоматизованої обробки будь-яких даних є аргумент про посилення ефективності і зниження витрат управлінської діяльності.

Проте, процес обробки персональних даних у комерційних цілях усе більше перетворюється в процвітаючий бізнес [1]. За деякими джерелами, **світовий ринок персональних даних досягає 3 млрд. доларів у рік** [2].

Сьогодні відомості про людину збираються й акумулюються різними державними органами (при влаштуванні на роботу, податковими органами, органами внутрішніх справ, органами реєстрації юридичних осіб при народженні й одержанні у наступному різних документів актів цивільного стану, медичними установами, органами реєстрації прав на нерухоме майно, при створенні приватних підприємств, бюро технічної інвентаризації, комунальними службами та ін.) і приватними структурами (медичні, юридичні організації, стільникові компанії, туристичні фірми, магазини тощо). Наприклад, роблячи покупки в Інтернет-магазинах або отримуючи дисконтні картки, споживач змушений повідомляти свої персональні дані. Власники зазначених підприємств, з одного боку, зацікавлені у відомостях про стан попиту на ринку, який може бути оцінений завдяки відомостям про покупців та потенційних споживачів їх продукції, а з іншого – не завжди забезпечують захист персональних даних людини,

[*] Див. – О. Підопригора. Рецензія на дослідження щодо права власності людини на персональні дані по темі: “Організаційно-правові питання захисту персональних даних” // Правова інформатика. – 2004. – № 3. – С. 69-73.

навіть можуть збирати та пропонувати зазначені дані для продажу й отримання іншого виду прибутку, без диверсифікації щодо номенклатури продукції. Останнє в умовах ринку – значний важіль у конкурентній боротьбі, гарант від розорення при змінах кон’юнктури.

Американський журнал “Forbes” *(//www.Forbes.com)* відзначає, що відомості про ім'я, прізвище, адресу й інші персональні дані можна купити приблизно за 10 центів. Якщо ви володієте екстраординарною купівельною спроможністю, наприклад, здобуваєте програмне забезпечення для підприємств середнього бізнесу, то ім'я й адреса оцінюються ледве вище – 15 центів, а от ім'я плюс адреса е-пошти можуть потягнути на чверть долара. Відноситься це, у першу чергу, до добропорядних громадян. Відомості про осіб з темним минулим – товар особливий, а тому і ціна на нього зовсім інша.

Компанії типу Docusearch.com, Knowx.com, USsearch.com і Pac-info.com збирають персональні дані з офіційних документів, у тому числі із судових протоколів, і поширюють їх за винагороду. Фірма Docusearch за пошук інформації про одну людину бере плату в розмірі від 14 до 249 дол. США у залежності від змісту запитуваної інформації. Причому, це можуть бути будь-які відомості – від номерів телефонів, особистих стосунків, фото-, відео-зйомки до карного досьє.

Поряд з ринком “роздрібних інформаційних послуг“ існує і “оптовий інформаційний ринок” – продаж адресних списків. Не є проблемою й покупка, а точніше оренда адресної бази для поштового розсилання. Причому, за цілком помірну плату – *“від 75 до 125 дол. США за тисячу адрес”*, – стверджує Політ Краньяк, президент нью-йоркської компанії List Process, що надає подібні інформаційні послуги. *“Спеціалізована B2B адресна база може коштує дорожче – біля 150 дол. за тисячу імен”,* – зазначає Лайза Хордер, президент фірми L.I.S.T., що знаходиться в штаті Нью-Йорк. А список приватних адрес та е-пошти, власники яких підтвердили свою згоду одержувати електронні листи, може бути проданий ще дорожче – від 250 до 300 дол. за тисячу імен [3, – С. 30].

Інший приклад – фірма SRDS, яка розташована в штаті Іллінойс, займається наданням інформації для рекламної індустрії. Компанія пропонує більш 28.000 адресних списків, що відноситься до понад 220 ринкових категорій, таким, як “мистецтво”, “діти”, “робота” і т.п. Подібні адресні списки здаються в оренду, причому бази даних можуть бути отримані щотижня і послужити основою для створення нових інформаційних продуктів.

Сьогодні ті, хто займається маркетингом структур постійно вишукують нові, усе більш ефективні шляхи для збору будь-яких відомостей про своїх конкурентів та потенційних покупців: їх діяльність, оточення, стосунки, погляди, інтереси, характер, поведінка та багато ін. Для бізнесу персональні дані – зручне, а тепер і необхідне доповнення із усього того, що надає Інтернет або інші мережі. Уже цілком чітко усвідомлено, що з допомогою засобів е-середовища набагато легше збирати величезні обсяги різної інформації (ніж займатися звичайним промисловим шпигунством), а аналіз і взаємне ув'язування відомостей забезпечує істотні прибутки в бізнесі [4].

Критерії, відповідно до яких відомості про ту або іншу людину включаються до списку, призначеного для маркетингових заходів, як правило, очевидні. Так дані про людину, що має моторний човен, вносять до списку власників моторних човнів саме тому, що віна володіє човном. В основу прямого маркетингу покладене створення списків людей, поєднуваних загальними демографічними даними. І для цих цілей зовсім не потрібна конфіденційна інформація. Головне, щоб її було як можна більше, для створення, наприклад, небажаного для особи її негативного “портрету” у разі передвиборчої компанії.

Прихильники недоторканності персональних даних упевнені, що діяльність багатьох фірм таїть у собі погрозу постійного порушення прав громадян. Усі фірми переслідують мету у отриманні прибутку за свою роботу: пошук і збір інформації із різного роду джерел державних, муніципальних та приватних установ, а також від окремих осіб, які мають відповідну інформацію. Як правило, зв'язатися з суб’єктами, що реалізують бази даних, які містять персональні дані, можна дуже просто – за допомогою контактного телефону або е-пошти.

На теренах пострадянських країн, зокрема, у Російський Федерації, сьогодні на “чорному” ринку персональних даних збільшилася кількість баз даних різних структур [2]. У 2003 р. у продажу з'явилася БД абонентів одного з лідерів російського ринку операторів стільникового зв'язку “Мобільних ТелеСистем”. База даних містить такі персональні дані про абонентів компанії, як прізвище, ім'я, по батькові, дата народження, паспортні дані, адреса місця проживання, ідентифікаційний номер платника податків, юридичну та робочу адресу, контактний телефон та ін. Система пошуку дозволяє за кілька секунд одержати повний список абонентів “МТС”, що є працівниками того або іншого підприємства. Абонентами “МТС” є понад 5 млн. чоловік. Інформація про появу БД на диску поширювалася через Інтернет. Журналісти однієї російської газети спокійно придбали зазначений диск в метро за 450 рублів. Відповідні органи зреагувати не встигли або не змогли.

Практично одночасно стало відомо про наймасштабніший витік конфіденційної інформації. У Санкт-Петербурзі в продаж надійшла комбінована БД про абонентів найбільших телефонних компаній міста, у якій утримуються персональні дані мільйонів петербуржців: адреси, номера паспортів, стільникових і домашніх телефонів. Крім того, на трьох дисках зберігається інформація про всіх абонентів Північнозахідної філії ВАТ “Мегафон” (1,3 млн. записів), “Телеком XXI” (контролюється “Мобільними ТелеСистемами” і працює під цією торговою маркою; 500 тис. записів), “Дельта Телеком” (120 тис. записів), “РОКА Сот” (15 тис. записів), а також “Північнозахідний Телеком” і “Пітерстар” (2,5 млн. записів). Вартість БД – 1650 рублів. В офісах постраждалих компаній вважають, що інформація була украдена централізовано через одну з правоохоронних структур.

Разом з тим, у Новосибірську прокуратурою була порушена кримінальна справа у відношенні одного з менеджерів компанії стільникового зв'язку “Сибірські стільникові системи-900” (провайдер мережі “МТС”). Він обвинувачується в розголошенні відомостей про абонентів. Інформація стосувалася тільки номерів, по яких дзвонили абоненти, і тривалості розмов. Але і ці відомості є закритими. Обвинувачуваний був визначений у ході розслідування, проведеного співробітниками служби безпеки самої стільникової компанії, що і звернулися до правоохоронних органів. Справа порушена за статтею “Порушення таємниці листування і телефонних переговорів” (ч. 2 ст. 138 КК РФ), що передбачає штраф або арешт на термін від 2 до 4 місяців.

У цілому на російському ринку персональних даних доступні різні БД (*//www.kiev-security.org.ua/box /4/136.shtml*), власниками яких є, зокрема, державні органи (див. Таблицю).

Таблиця

Назва бази даних	**Обсяг**	**Ціна**
БД “ДАІ м. Москви” (містить повний набір відомостей про автомобілі (держ. номер, № кузова, двигуна, марка, модель і т.д.), про його власника (ПІБ, дата народження, прописка, № паспорта) і документи (ПТС, посвідчення про реєстрацію, довідка-рахунок, талон ТО)	2,5 Гб	500 р.

БД “Автотранспорт Московської області”	1,43 Гб	500 р.
БД “Прописка у Московській області”	430 Мб	400 р.
БД “Прописка у м. Москві”	1,2 Гб	500 р.
БД жителів Московського регіону (ПІБ, дата народження, місце народження та проживання, серія і номер паспорта, коли і ким виданий, підрозділ УВІР, ціль одержання)	541 Мб	400 р.
БД “Посвідчення водія у м. Москва”	611 Мб	500 р.
БД “Посвідчення водія у Московській області”	269 Мб	500 р.
БД “Порушення правил дорожнього руху”	208 Мб	500 р.
БД “Транспортних подій”	269 Мб	500 р.
БД “ДТП та постраждалі у м. Москва”	33 Мб	500 р.
БД “Викрадені автомобілі в Росії”	206 Мб	500 р.
БД “Московська ліцензійна палата” (про ліцензії)	240 Мб	400 р.
БД “Зареєстровані підприємства Росії”	3 Гб	500 р.
БД “Приватизовані квартири м. Москви”	1,22 Гб	400 р.
БД “Розшук 2003” (розшук викраденого автомобіля, пошук викраденої спецпродукції, федеральний розшук осіб)	775 Мб	400 р.
БД 2002 єдиної міської телефонної мережі м. Москви	3,6 Гб	500 р.
БД мобільних телефонів Московського регіону	1 Гб	500 р.
БД “МГТС 2003” (інформація щодо всіх номерів Московського регіону і більшості великих підприємств Росії)	3 Гб	500 р.
БД “Московська реєстраційна палата” (відомості про юридичних осіб і приватних підприємцях м. Москви)	1,16 Гб	500 р.
БД Московської обласної Реєстраційної палати	280 Мб	500 р.
БД Московського земельного комітету (інформація про власників (фізичних і юридичних осіб)	12 Мб	200 р.
БД “Антикримінал” (розшук-судимість, викрадення, викрадені документи)	551 Мб	400 р
БД “Банки Росії” (усі реквізити)	95 Мб	300 р.

З того ж джерела [2] можемо дізнатися й про іншу вартість персональних даних:

Назва бази даних	**Кількість записів**	**Ціна**
БД приватних осіб м. Москви та Московської області	1 126 486	150 дол. США
БД приватних осіб Росії та СНД (включає е-адресу)	12.000.000	200 дол. США
Програма для розсилки інформації за е-адресами		150 дол. США
БД телефонних номерів Росії		550 руб.
БД із експортно-імпортних операцій (постачальник, споживач, товар, вартість, банк обслуговування тощо)	5 442 574	1400 руб.
БД квартир та їх власників м. Москви	10 443 278	1000 руб.
БД прописки у м. Москва (ПІБ, адреса, дата народження, стать)	14 млн.	1000 руб.
БД фізичних осіб Московської області	6,2 млн.	1000 руб.
БД ДТП (інформація про потерпілих)	413 030	45450 руб.

У засобах масової інформації також повідомлялося про те, що в Естонії на “вільному ринку” вже з'явилися лазерні диски, що містять персональні дані. Продаються витяги з реєстру громадян країни, автомобільного реєстру, реєстрів нерухомості і майнового стану людей, таємні файли естонської дорожньої поліції, відомості про пікантні деталі приватного життя окремих осіб. Ціна такої продукції приблизно 3000 дол. [5, – С. 183].

2. Найважливішим напрямом інформаційної політики будь-якої держави є активне формування інформаційного ринку – ринку інформаційних об'єктів-товарів (ресурсів, продуктів, технологій) і інформаційних послуг. Ринок – це товар і товарно-грошові відносини продавця і покупця. В основі функціонування, зокрема, інформаційного ринку лежать суспільні відносини права власності на інформаційні ресурси, інформаційні продукти, інформаційні технології й інформаційні послуги.

Начебто з цим питанням усе ясно. Закон України “Про інформацію” 1992 року в частині другій статті 38 однозначно визначив: *“Інформація є об'єктом права власності громадян… Інформація може бути об’єктом права власності як у повному обсязі, так і об'єктом лише володіння, користування чи розпорядження”* [6]. Далі у статті 39 вказаного Закону передбачено: *“Інформаційна продукція та інформаційні послуги громадян та юридичних осіб, які займаються інформаційною діяльністю, можуть бути об’єктами товарних відносин, що регулюються чинним цивільним та іншим законодавством”*. Іншими словами, на інформацію поширюється режим інституту майнових прав власності.

На жаль, з радянських часів не тільки у “простих людей”, не обтяжених правовою освітою, але й у керівників усіх рівнів не зжите уявлення про інформацію як субстанцію, що у принципі не є чиєюсь власністю. Це уявлення, з одного боку, до кінця не переосмислено, а з іншого боку, одержало “підтримку” у зв'язку з виникненням електронно-інформаційного середовища (е-середовища). І якщо для того, щоб усі дотримували принципу, викладеного у статті 39 Закону України “Про інформацію”: *інформація – це товар, у якого є власник*, потрібен час, то з власністю на інформацію в е-середовищі справа значно складніше – веб-сторінку в руках не потримаєш.

Матеріальні об'єкти (речі), які є предметом права власності, поділяють на нерухоме (земельні ділянки, будинки і будівлі, квартири і нежитлові приміщення і т. п.) і рухоме (та інше) майно. Якщо тут поставити крапку, це буде не зовсім правильно. Інтелектуальна власність є об'єктом так званих виключних прав використання, які не відносяться до матеріальної власності. Але це не все. Є ще так звані об'єкти обмеженої оборотоздатності, наприклад, радіочастотний спектр, природні ресурси, зброя, а також об'єкти, “вилучені” з обороту, – повітря, небесні тіла, що взагалі не є предметами правовідносин [7].

Таким чином, об'єктний склад відносин власності між суб'єктами права досить складний і включає найрізноманітніші види. До них законодавство України відносить власне речі, результати інтелектуальної діяльності, роботи і послуги, інформацію та ін. Частина об'єктів матеріального світу до об'єктів цивільних прав не відноситься. Звернемо увагу на те, що “інформація” за визначенням законодавця не відноситься до об'єктів інтелектуальної власності. Тут явно проведене розходження між змістовною, “об'єктивною” інформацією і формами її представлення (у творах літератури і мистецтва, програмах для ПК, базах даних і т. д.).

Цікаво тут і те, що інформація може бути об'єктом інтелектуальної власності (тобто одержати відповідну юридичну форму охорони), якщо вона почне відповідати критеріям патентоспроможності (по патентному праву) або входити в коло об'єктів, що охороняються по авторському праву. Патент охороняє зміст інформації, а авторське право – тільки форму її представлення. Звідси і виникло право “копірайту”, тобто право на тиражування (копіювання).

Постає питання, а до якого з видів об'єктів цивільного права відноситься, скажімо, веб-сайт в Інтернет?

Це комплексний об'єкт, у якому є явна сукупність об'єктів, що відносяться до авторського права (наявність тексту, дизайнерського оформлення, технології

представлення відомостей і т. д.), так само як і різного роду інформаційні об'єкти, для яких найважливішим компонентом є їх зміст. Не можна забувати і про те, що сайт не існує “сам по собі”, без участі осіб, що підтримують його (провайдери доступу, хостінга і т.п.). Тут же постає і питання адресації сайта, що дозволяє однозначно одержати доступ до нього й ідентифікувати його власника через відповідні персональні дані – доменні імена. Можуть виникнути і додаткові питання.

По-перше, чи відноситься унікальна адреса мережного об'єкта до інтелектуальної власності, яка охороняється цивільним правом? (Хоча Цивільний кодекс України поняття “персональні дані” взагалі не використовує). Якщо ні, то хіба (за аналогією з “немережним” світом) не повинне бути забезпечене право суб’єкта певного доменного імені на недоторканність для того, щоб ним не міг користуватися хтось інший? Якщо так, то до якого встановленого законом виду об'єктів виключних прав доменне ім'я відноситься – товарний знак, фірмове найменування, об'єкт авторського права або щось інше?

По-друге, а чому, власне, ми говоримо про “господаря” веб-сайта, іноді навіть про його власника? Хіба сайти й інші інформаційні структури відносяться до матеріальних об'єктів (“речей”, “майна”) і можуть бути чиєюсь власністю, тобто знаходитися в чиємусь володінні, користуванні і розпорядженні? На це можна відповісти позитивно, і от чому.

Ми звикли до поняття “інформація” як до відомостей. Згідно зі ст.1 Закону України “Про інформацію” 1992 р.: *“Під інформацією цей Закон розуміє документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі”.*

Що таке “документовані відомості” – Закон визначення не дає. Виходячи з подальшого змісту Закону можна вважати, що термін має пряме відношення тільки до поняття “офіційний документ” – папір, на якому розміщені відомості.

Відомості як такі вимовляються, доводяться і т.д., тому, виходить, чиєюсь власністю бути не можуть. Якщо я поміняюся з колегою ручками, у кожного з нас залишиться по одній ручці. Якщо ми обміняємося з ним анекдотами – у кожного в пам'яті буде два анекдоти, хоча, звичайно, ненадовго. Таким чином, інформація – відомості цілком не відчужувана: авторучку продають, і вона в продавця відчужується, передається покупцеві. З відомостями такого не буває.

Однак, думка в голові людини ще не відомості і тим більше не інформація – це прояв начитаності й інтелектуальності (творчості), що для відповідного суб'єкта в цей час є його абсолютною монополією. Те, що розуміється під інформацією, тільки починає виступати як предмет передбачуваної власності: – ідеальний початок (мабуть, саме це Великий Платон вважав «ейдосом» – “ідеєю”).

Вимовляючи слова (користуючись папером, хвилями звуку, комп’ютером, радіохвилями тощо), людина висловлює “ідею”, трансформуючи її у відомості. І тільки тоді, коли відомості передаються будь-кому, народжується інформація. При цьому, людина вимовляє, доводить не думку як таку, а її копію, яка виражена у відповідній формі. Виникає матеріалізація думки. Ця матеріалізація у е-просторі є вже не “інформацією”, а “даними” (див. – [8]), до яких інформація прикріплена, пристосована. Тільки при поєднанні ідеального і матеріального з'являються “дані”. За відсутністю одного із зазначених елементів “дані”, а разом й інформація, – зникають.

Визначимо тут ще, що з часів Римського права (точніше, після введення в дію Кодексу Наполеона) *право власності – це тріада повноважень щодо володіння, користування і розпорядження майном*. Спроби застосувати цю тріаду до “чистої” інформації, тобто як до відомостей, безуспішні. Власник відноситься до відомостей (висловлюваної “ідеї”), що надаються, як до свого майна (матеріального об’єкта) і вправі

вимагати від будь-якої особи дотримання його права власності на це майно або поновлення цього права (статисфакції) у разі його порушення. Проте *володіти* відомостями без забезпечення доступу до них інших осіб по юридичних канонах неможливо, інакше (у випадках типу – знаю, але нікому не скажу) юридично губиться зміст володіння. *Користуватися* відомостями знову-таки може не тільки умовний власник (скажімо, автор твору), але й будь-яка інша особа, що одержала доступ до них. Причому на рівних з іншими умовами. *Розпорядження* відомостями також має, на відміну від майна, трохи інший зміст. Тому що зробити відчуження відомостей (або, приміром, віддати їх в оренду чи в заставу) неможливо, мова може йти про розпорядження у вигляді визначення порядку доступу до них.

Таким чином, для того, щоб відомості стали власністю, потрібний носій. І це стосується не тільки папера-носія. Це стосується будь-якого носія, де відомості можуть бути розміщені або пристосовані, наприклад, дискета, диск, електричний сигнал, електронна структура, звукова хвиля та ін.

З появою і широким поширенням понять “веб-сайт”, “веб-документ”, “веб-сторінка” документована інформація стала розглядатися як поняття, засноване на двоєдності відомостей і матеріального носія, на який вони заносяться у вигляді символів, знаків, літер, е-сигналів, е-структур та ін.

У результаті трансформації зазначеного розуміння “документування” відбувається ніби матеріалізація й упредметнення інформації. Відомості розміщують (пристосовують) на матеріальному носії і, тим самим, відокремлюють від свого творця. У підсумку виникає об'єкт права власності – “документована інформація” або інформаційний продукт. Цей інформаційний продукт є об'єктом правовідносин як для матеріального середовища: книжка, журнал, стаття та ін., так і для віртуального середовища: банк даних, веб-сайт, веб-сторінка, доменне ім'я та ін. Таким чином, документована інформація (інформаційний продукт) стає по суті справи матеріальним об'єктом, що дає підставу відносити його до категорії речей. А це означає, що на документовану інформацію поширюється право матеріальної (речової) власності.

Отже, власник інформаційного продукту, наприклад, веб-сайта, володіючи авторськими й іншими правами на компоненти, що складають об'єкт права (а в тому, що такі об'єкти існують, сумнівів немає, вони можуть реально продаватися і купуватися), забезпечує іншим особам (користувачам) доступ до них і визначає порядок доступу (наприклад, платний або безкоштовний). Зазначена юридична конструкція, на жаль, у термінах сучасного правового акта чітко не прописана. Відзначене, треба думати, варто юридично закріпити в інформаційному законодавстві.

Між власністю на річ і інтелектуальною власністю є істотні відмінності. Вони випливають з розходжень між матеріальністю об'єктів (речей) і нематеріальністю відомостей результатів інтелектуальної творчості людини. При розміщенні відомостей на носії виникає об'єкт документованої інформації. Він містить у собі права щодо його використання і права власності. Варто пам'ятати, що поняття *“інтелектуальна власність”* – це не власність у матеріальному (речовому) сенсі. Згідно зі ст.2 (VIII) Конвенції, що заснувала Всесвітню організацію інтелектуальної власності (1967 р.): *“інтелектуальна власність – це усі права, що виникають у зв'язку з результатами конкретної творчої діяльності людини”*, а *“обсяг правової охорони – конкретні результати цієї діяльності”.* Обсяг відзначених прав (виключних або невиключних) визначає лише географічну територію і час використання об'єкта творчості, які засвідчені державою у вигляді охоронного документа (патенту, свідоцтва).

Відомо, що нові наукові інститути нерідко утворюються на перетині наук, що визначається у їх назві, наприклад, як: астрофізика, радіоастрономія, біохімія та ін. Приклад подібного підходу, але вже в юриспруденції є – це пропозиція щодо введення “права власності фізичної особи на її персональні дані”, яке знаходиться на перетині “права власності на майно” та “права інтелектуальної власності”. Цей інститут запропонований у проекті Закону України *“Про захист персональних даних”* (реєстраційний № 2618 від 10.01.2003 р.), який у травні 2003 р. розглянутий Верховною Радою України та прийнятий за основу [9].

Відповідно до законопроекту персональні дані можуть становити предмет *“виключного права власності людини на свої персональні дані”*, якщо ця інформація використовується для задоволення економічних інтересів, наприклад, у зв’язку із витраченою працею по акумулюванню її в базах персональних даних та ін. При цьому, з одного боку, *“виключне право*” уособлює законодавче обмеження прав особи її на персональні дані з погляду майнових інтересів інших осіб – фізичних, юридичних та держави, а з іншого – наявність *“права власності”* людини на персональні дані додає її правам монопольний зміст щодо володіння, користування і розпорядження своїми даними. Сполучення негативної і позитивної характеристик повноважень людини на свої персональні дані, наданих відомими інститутами власності, дозволяє запровадити нову юридичну категорію і створити новий правовий механізм присвоєння і упорядкування суспільних відносин саме для сфери захисту персональних даних. Таке спільне використання різних інститутів власності для захисту персональних даних надає їм юридичну оболонку власності та нову якість щодо захисту прав людини у сфері персональних даних. Більш того, такий підхід надає не тільки додатковий захист персональним даним, але й сприяє введенню інформації про фізичну особу в товарно-грошовий обіг на визначених законом умовах.

Схематично зазначене може бути представлено за допомогою логічних кругів Ейлера (див. Рис.).

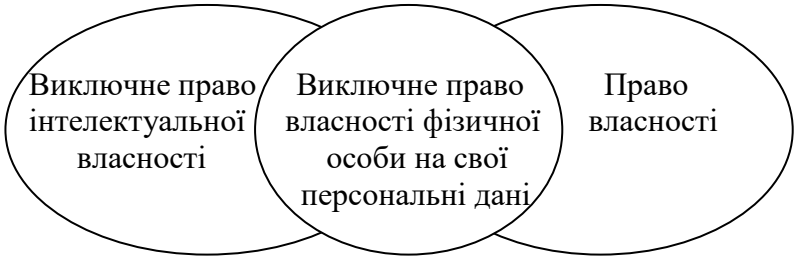


Рис.

Поняття, обсяги суттєвих ознак яких повністю або частково збігаються називають сумісними. У даному випадку вони такі, що знаходяться у відношенні пересичення (перехрещення), тобто обсяг ознак одного із них частково входить до обсягу ознак іншого [10, – С. 33]. Категорія “виключне право власності фізичної особи на свої персональні дані” знаходиться нібито на перетині двох відомих інститутів власності. У такому разі захист даних може здійснюватися або за допомогою норм права законодавства про інтелектуальну власність, або за допомогою норм права законодавства про власність на майно, залежно від мети, з якою відповідні персональні дані обробляються.

Що стосується відповідності обсягу правового поля зазначеній юридичній категорії (“виключне право власності фізичної особи на свої персональні дані”) – обсягу чинної в країні законодавчої бази, то запропонований у законопроекті новий юридичний інструмент – інститут права власності на персональні дані цілком відповідає обсягу положень ст. 22 Конституції України та ст. 54 Закону України “Про інформацію”.

Стаття 22 Конституції України передбачає: *“Права і свободи людини і громадянина, визначені цією Конституцією , не є вичерпними”.* А згідно зі змістом правової формули статті 54 Закону України “Про інформацію”: *“Інформаційний суверенітет України забезпечується виключним правом власності України на інформаційні ресурси”.* **Це виключне право власності України здійснюється через права** її **окремих** суб'єктів – **громадян**, а не тільки через права організацій, підприємств або держави.

Також можна стверджувати про те, що інститут права власності фізичної особи на свої персональні дані відповідає вимогам положень Конвенції № 108 Ради Європи від 28.01.81 р. *“Про захист фізичних осіб у зв’язку з автоматизованою обробкою персональних даних”* [11]. Конвенція є головним і єдиним міжнародним документом, що визначає зобов'язання держав із забезпечення умов гармонізації національного законодавства із загальноєвропейськими стандартами. У статті 11 Конвенції зазначається: *“Жодне з положень цієї глави не тлумачиться як таке, що обмежує або іншим чином перешкоджає можливості Сторони забезпечувати суб’єктам даних більший ступінь захисту, ніж передбачений цією Конвенцією”.*

Таким чином, ***будь-які відомості про фізичну особу є особливим видом приватної власності, що юридично виступає у формі виключного права власності та ототожнює собою право на самовизначення відповідної особи, монополія на власність якої обмежується Законом в інтересах дотримання прав і свобод інших осіб, а також в інтересах дотримання балансу прав особи, суспільства та держави***. Звідси витікає, що ніхто не вправі вимагати від людини і використовувати її персональні дані, якщо вона не дала на це згоду або якщо вимогу про право на доступ до персональних даних чітко не прописано в законах України.

Важливим є також наступне зауваження: якщо зазначене вище буде прописано у “законодавстві”, а не у “законах”, то органи влади будуть мати можливість визначати рівень захисту персональних даних у відповідній галузі за допомогою підзаконних актів, незважаючи на наявність у державі базового закону та вимог світових стандартів. Крім того, якщо держава має серйозні намір у створенні правового механізму захисту персональних даних, який відповідає принципам та положенням світових стандартів, то це потребує запровадження в системі судової влади держави Судової палати із питань захисту персональних даних та початку підготовки кваліфікованих фахівців для цієї сфери.

Деякі інші висновки

Новації щодо інформаційних ресурсів обов'язково повинні супроводжуватися законодавчим оформлення права власності на них. Інформаційні продукти мають охоронятися так само, як і об'єкти матеріального (речового) права. Повинна ширше застосовуватися й аналогія права, й аналогія закону до такого роду цивільних правовідносин. Адже стосовно об'єктів е-середовища: баз даних, доменних імен, веб-сторінок, веб-сайтів і адрес порталів, е-пошти та ін. – є цілком можливим використання принципів (підходів) регулювання відносин права власності на матеріальні об'єкти і регулювання відносин на об'єкти інтелектуальної власності. Причому, можливе і спільне використання принципів, підходів у регулюванні відомих інститутів власності і формування нового юридичного інституту, що знаходиться ніби на їх стику, тобто інституту власності на об'єкти інформаційних відносин у сфері захисту персональних даних.

Ділянка е-середовища, закріплена за певним власником за певною адресою (яку не можна довільно змінювати), тим більше, якщо на ній вже побудований з комерційними цілями веб-сайт, має так само охоронятися, як і земельна ділянка з будівлями, що знаходяться на ній. Якщо цього не відбудеться в якійсь країні, користувачі Інтернету “перетечуть” у таку юрисдикцію, де їх права (вкладені гроші та праця) будуть надійно захищені.

Світовий досвід свідчить про те, що в країнах, де право приватного власника захищене і економіка розвивається, і громадянське суспільство існує, і демократичні принципи під сумнів не ставляться. А от у країнах, де системи захисту прав власників не існують або існують декоративно (зокрема, у відношенні до інформації), поки що все неблагополучно і в економіці, і в політиці. Більш того, серед закордонних юристів дістала поширення теорія про те, що капітал (“багатство”) – усього лише інформація про закріплені (оформлені) права власності на нерухомість, на гроші (у банках), на матеріальні активи. Ця інформація повинна бути добре захищена. Якщо в якійсь країні належного захисту прав власності на комерційну інформацію немає (наприклад, ненадійність банківської системи, яка не захищає вкладені в банк гроші або персональні дані про їх вкладників), то з такої країни капітали “витікають”, а гроші, що залишаються в ній, помирають в чужоземних асигнаціях і не працюють на національну економіку. От чому права власності на інформаційні ресурси та, зокрема, на персональні дані, повинно захищати так само, як і права на інші об'єкти, що мають матеріальний, майновий зміст.

Якщо наведена у роботі аргументація щодо необхідності запровадження у державі **спеціального правового механізму (інституту) захисту прав фізичної особи на свої персональні дані**, не досить переконлива, то можна згадати висловлення Майкла Фарадея. На питання – *яка користь від електрики?*, від відповів: *“Коли-небудь ви будете мати можливість обкласти її податком”.*

Використана література

1. Цена персональных данных (Рыночная цена конфиденциальности, или буря в стакане воды). – 2000 // www.i2r.ru/article.shtml?id=1384.

2. В. Михеев. Проблема правовой защиты персональных данных // www.kiev-security.org. ua/box /4/136.shtml.

3. В.М.Брижко Правовий механізм захисту персональних даних: монографія ; за ред. доктора економічних наук, професора М.Я. Швеця та доктора юридичних наук, професора Р.А. Калюжного – К.: Парламентське видавництво, 2003. – 120 стор.

4. Берд Киви. Анонимность в Сети как залог свободы //www.sdteam.com/articles/hack058. shtml

5. Баранов А.А., Брыжко В.М., Базанов Ю.К. Права человека и защита персональных данных. – Харьков: ХПГ-Фолио, 2000. – 280 с.

6. Закон України “Про інформацію” // Відомості Верховної Ради України . – 1992. – № 48.

7. В.Михайлов Информация и собственность / Компьютерра от 18.06.2001 г. //www. computerra.ru/offline/2001/400/10524.

8. В.Брижко. До питання застосування у правотворчості понять “інформація” та “дані” // Правова інформатика. – 2005. – № 8. – С. 31-37.

9. Постанова Верховної Ради України “Про прийняття за основу проекту Закону України “Про захист персональних даних” від 15 травня 2003 року № 784-IV.

10. Кирилов В.И., Старченко А.А. Логика: учеб. для юридич. вузов и фак. ун-тов. – 2-е изд., испр. и доп. – М.: Высш. Шк., 1987. – 271 с.

11. Конвенція № 108 Ради Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” від 28.01.1981 р. // www.convention.coe.int/treaty/en/Treaties/Html/ 108.htm.

12. И.Л. Бачило О праве собственности на информационные ресурсы // Информационные ресурсы России. – 1997. – № 4. – С.19-23.

13. С.В. Вихорев. Информация как объект вещного права //www.infotecs.ru/gtc/New_ publications /FILOSOF.html.

14. В.А. Копылов. Информация и собственность / Информационные ресурсы России. – 1996. – №3. – С. 10-12.

15. Е.А. Суханов. Объекты права собственности / Закон. – 1995. – № 4. – С. 94-98.

УДК 004:681.3

М. ГУЦАЛЮК, *кандидат юридичних наук, доцент*

ДО ПИТАННЯ ІДЕНТИФІКАЦІЇ ОСОБИ ЗА ДОПОМОГОЮ БІОМЕТРИЧНИХ ДАНИХ

Анотація. *Щодо впровадження мікрочипів у паспорт громадянина*

Глобалізація світової економіки призводить до прискорення міграційних процесів в усьому світі. За оцінкою ООН, понад 175 млн. чоловік (3 % населення планети) нині постійно проживають за межами держав, у яких народилися. У 2000 році вони становили 8,7 % населення розвинутих країн і лише 1,5 % населення “бідних” держав. Причому з кожним роком ця тенденція підсилюється: якщо 1965 року країни Заходу прийняли 36,5% міжнародних мігрантів, то в 2000 році – 43,4 %. З 1970 по 2000 рік число міжнародних мігрантів подвоїлося.

Ідеологія вільної торгівлі, вільного обміну інформацією і бізнесу без кордонів неминуче зменшує значення окремих держав. Водночас глобалізація призвела до появи феномену міжнародного тероризму. Міжнародні терористи можуть жити в одній країні, збирати гроші – в іншій, купувати зброю – у третій, а здійснювати атаки – у четвертій.

Щодо масштабу міграційних процесів в Україні, то, за повідомленням виконуючого обов’язки начальника Державного департаменту у справах громадянства, імміграції та реєстрації фізичних осіб МВС України С.Радутного, на сьогодні державний кордон України в обох напрямках перетинають понад 30 мільйонів людей. Приблизно 60 тисяч осіб виїжджають з України на постійне місце перебування за кордон. Кожного року до органів внутрішніх справ звертаються за наданням паспортно-візових послуг майже 15 мільйонів осіб [1].

За висновками дослідницького центру Nixon Center, ріст міграції супроводжується збільшенням числа терористичних атак. Після терактів 11 вересня 2001 року більшість індустріально розвинутих країн світу сконцентрувалися на вирішенні трьох головних задач (англійською мовою зазвичай використовується термін 3P – preventing/запобігання, prosecuting/покарання, protecting/захист): по-перше, на запобіганні в'їзду терористів у країну і надання їм права на постійне проживання, по-друге, на покаранні терористів за вчинені ними злочини, і по-третє, на захисті громадян. Для цього створюються особливі бази даних, правоохоронні органи обмінюються інформацією один з одним, активно використовують ідентифікацію осіб, використовуючи при цьому сучасні досягнення науки і техніки [2].

Останнім часом у найрізноманітніших сферах для ідентифікації особи все частіше використовують унікальні характеристики людини – сітківку ока, відбитки пальців, почерк, голос і навіть запах. Галузь наукових знань, що охоплює планування й аналіз результатів кількісних біологічних експериментів і спостережень методами математичної статистики, називають біометрією.

Досягнення біометрії, які використовують в прикладних цілях, сьогодні перетворилися на могутню індустрію. Експерти аналітичної компанії Cajmers In-Stat прогнозують, що в 2005 р. обсяг ринку біометричних пристроїв зросте до 520 млн. дол. порівняно з
227,9 млн. дол. у 2000 р. На їхню думку, через чотири роки устаткування, що забезпечує

ідентифікацію людей по унікальних фізичних ознаках, стане частиною стандартного набору засобів безпеки [3].

Використання біометричних даних користувачів найбільш поширене в комплексних системах доступу, а також для захисту комп'ютерної інформації, у тому числі і електронних трансакцій. Цікаве застосування пропонується й у сфері торгівлі. Так в одній з мереж супермаркетів Німеччини відвідувачі незабаром зможуть оплачувати покупки по відбитку пальця. Як стверджують розробники нової системи оплати, дана технологія дозволить заощаджувати до 40 секунд часу, затрачуваного в середньому кожним покупцем на оплату готівкою або пластиковою карткою [4].

Але особливо гострі дискусії сьогодні проходять під час обговорення проблеми впровадження біометричних технологій в основний документ, який сам підтверджує особу громадянина, – паспорт.

Упровадження складних захисних елементів пояснюється тим, що паспорт, розроблений з використанням традиційних технологій, не витримує ніякої критики з погляду його підробки з використанням офісної техніки, яка сьогодні стала доступна широким верствам населення.

Тому 25 вересня 2000 року в м. Брюсселі представниками урядів держав – членів Європейського Союзу була прийнята Резолюція з питань безпеки паспортних документів і інших дорожніх документів. Резолюцією ухвалено, що з 1 січня 2005 року в країнах Євросоюзу вводяться загальнообов'язкові мінімальні стандарти безпеки в сфері виробництва паспортних і проїзних документів, спрямовані на захист паспортів від підробок. І хоча правоохоронці досить часто зіштовхуються з підробкою паспортів – адже це явище супроводжує такі види правопорушень, як торгівля людьми, нелегальна міграція, торгівля зброєю тощо, проблема набула надзвичайної актуальності після терористичних актів 11 вересня 2001 року в США і вибухів у Лондоні у 2005 році. Тому біометричні паспорти в найближчі 2-3 роки повинні стати звичайним явищем в усьому світі.

Зокрема, як повідомляє Державний департамент США, вони будуть оснащені мікрочипом, здатним зберігати такі дані, як ім'я, дату народження, стать, місце народження, дату видачі паспорта, номер паспорта і фото його власника. Цифровий підпис захищає ці дані від підробки і зменшує небезпеку підміни фотографії [5]. Разом з цим, Сполучені Штати Америки, вводячи в себе паспорти нового зразка, вимагають відповідної заміни і паспортів країн Євросоюзу. З 2006 року без віз відвідати США зможуть тільки власники паспортів нового зразка, які практично неможливо підробити [6].

Першою вимогу США виконала Бельгія. З 1 листопада 2005 року паспорта з вмонтованим чипом, у якому містяться біометричні дані обличчя власника, впроваджуються у Німеччині. Цікаво, що при фотографуванні на паспорт суворо заборонено посміхатися, адже це може суттєво змінити дані. Наступним кроком з 2007 року планується вносити інформацію з відбитками пальців.

У Латвії видача подібних паспортів почнеться з другої половини 2006 року, а з 2008 року планується запис також і відбитків пальців.

З 2008 року паспорти, що містять відомості про відбиток пальця і сітківку ока, впроваджує Великобританія. При цьому міністр внутрішніх справ Великобританії Чарльз Кларк підкреслив, що: *“Надійна ідентифікаційна схема допоможе запобігти діяльності терористів, більше третини з яких користуються фальшивими паспортами. Вона дозволить значно ефективніше боротися з торгівлею людьми”* [7].

Активно обговорюється дана проблема і у країнах колишнього СРСР. У серпні 2005 року в м. Мінську Міжнародна організація по міграції проводила семінар для фахівців із країн СНД. На ньому зазначалося, яку саме інформацію буде зберігати мікрочип, який міститиметься у паспортах громадян країн СНД. Зокрема, розглядалась можливість проводити ідентифікацію особи на митницях або в аеропортах по голосу, великому або вказівному пальцеві, а також по райдужній оболонці ока.

У Росії подібні паспорти одержать широке поширення в 2006 році, а перші 150 тисяч закордонних паспортів нового зразка, за словами генерального директора “Госзнака” Аркадія Ткачука, будуть виготовлені до кінця 2005 року [8].

Технології завтрашнього дня обіцяють набагато ефективніше проводити паспортний контроль, здійснювати фінансові операції тощо. Але, як правило, за кожен крок вперед необхідно заплатити вторгненням у приватне життя звичайних громадян. Схоже, сьогодні громадськість вважає такий компроміс прийнятним, і вчені активізують роботу по ідентифікації осіб, сподіваючись навчитися затримувати злочинців, перш ніж ті завдадуть удару.

Проте, одне з найбільш дискусійних питань, які виникають при введенні електронних паспортів, – співвідношення між правами людини і захистом її життя, а також національної безпеки. Щоденна англійська газета “Independent” пише, що за людьми, які ніколи не вчиняли злочини, *можуть “встановити електронне спостереження без їхньої згоди”*, адже результати біометричного сканування особи, вмонтовані у посвідчення особи, будуть розміщені в загальнонаціональній базі даних, з якої згодом можна співвідносити зйомки, зроблені камерами зовнішнього спостереження.

База даних дасть поліції і спецслужбам можливість стежити за людьми незалежно від того, чи є вони правопорушниками. Зйомки, зроблені камерами зовнішнього спостереження на вулицях, у магазинах і навіть у торгових центрах, можна буде співвідносити з фотографіями дорослих жителів після того, як закон про посвідчення особи набере сили. На думку правозахисних організацій, це надає “небезпечну” загрозу праву громадян на особисту таємницю.

Через події в Лондоні правоохоронці все більше сходяться на думці, що найбільшим надбанням людини є її життя. При цьому МВС Великобританії заявило, що поліція буде користуватися базою даних виключно при розслідуванні конкретних злочинів. Поліція може зажадати інформацію з Національного реєстру без відому і згоди громадянина, якщо вона необхідна для запобігання нових злочинів або з'ясування, хто вчинив злочин, що розслідується.

Що ж стосується України, то паспорти для виїзду за кордон, у які можливе впровадження мікрочипа, могли вже випускатися з початку 2005 року. Ці паспорти були схвалені Міжнародною організацією цивільної авіації (ІСАО), яка підтвердила, що новий паспорт цілком відповідає міжнародним стандартам і сертифікаційним вимогам. Це особливо важливо в зв'язку з тим, що ІСАО належить провідна роль у розробці вимог до паспортів і інших проїзних документів, а з 11 липня 2005 року рекомендації ІСАО в даній сфері є офіційним міжнародним стандартом.

Однак Указом Президента України № 457 від 10 березня 2005 року були внесені зміни в попередні укази, у тому числі скасовано Указ № 500 “Про створення Єдиного реєстру фізичних осіб”. І виробництво документа було припинено [9].

Надалі в пресі з'явилися публікації про випуск електронних паспортів до Дня Незалежності у 2005 р. Однак, уповноважені особи МВС України повідомили

громадськість про те, що випуск нових паспортів буде здійснено тільки після парламентських виборів 2006 р., щоб їх видача ніяк не вплинула на виборчу кампанію.

Тому залишається тільки чекати на прийняття відповідного закону, у якому були б викладені всі основні вимоги до головного документа громадянина – паспорта. Кілька законопроектів, зокрема поданих народним депутатом М.Оніщуком – “Про паспорт громадянина України” і народним депутатом О.Зарубінським – “Про паспорт громадянина України та інші документи, що посвідчують особу і підтверджують громадянство України” знаходяться на розгляді у Верховній Раді України. І тільки після їхнього прийняття можлива підготовка підзаконних нормативних актів, відповідно до яких і будуть виготовлятися вітчизняні ідентифікаційні документи, які відповідають світовому рівню.

Використана література

1. Операція “Мігрант” завершилась. Що далі? / Урядовий кур’єр. – 2005. – № 190. – С. 11.
2. http://www.washprofile.org.
3. http://itware.com.ua.
4. http://www.marketing.web-standart.net.
5. Водяной знак 2005, 17 августа.
6. High-tech passports coming; complaints already in // USA TODAY. Monday, April 4, 2005, 13A.
7. http://www.korrespondent.net.
8. http://government.e-rus.ru/site.shtml.
9. http://edaps.biz.

УДК 342.721:681.3.02

Д. СОПІЛЬНЯК, молодший науковий співробітник
Науково-дослідного інституту приватного права
і підприємництва Академії правових наук України

ДО ПИТАННЯ ЗАСОБІВ ІНДИВІДУАЛІЗАЦІЇ НАЙМАНОГО ПРАЦІВНИКА

Анотація. *Про необхідність прийняття міжгалузевого закону для врегулювання відносин у сфері охорони та захисту персональних даних*

Впровадження в усі сфери діяльності особи, суспільства та держави інформаційних технологій та мереж передачі даних зумовлює поширення великих масивів інформації на значних територіях. За таких умов, з одного боку, інформація, як найважливіший ресурс суспільства здобуває все більшого значення, а з другого, – виникає необхідність чіткої регламентації порядку поширення і використання окремих видів інформації.

Досвід розвинених країн свідчить про те, що правовою базою, фундаментом інформаційного суспільства є інформаційне законодавство. Права людини і громадянина в Україні на інформацію, її вільне отримання, використання, поширення та зберігання в обсягах, необхідних для реалізації кожним своїх прав, свобод і законних інтересів, закріплюються і гарантуються чинним законодавством. Нормативна основа інформаційних правовідносин у державі визначена у статтях 32 і 34 Конституції України [1], Законах України “Про інформацію” [6], “Про друковані засоби масової інформації (пресу) в Україні” [7], “Про телебачення і радіомовлення” [8], відповідними нормами Цивільного [2] та Кримінального [3] кодексів України, Кодексу України про адміністративні правопорушення [4], а також низкою ратифікованих Україною міжнародних нормативних документів(*, спрямованих на захист честі, гідності та ділової репутації особи внаслідок поширення неправдивої інформації, відшкодування матеріальної і моральної шкоди, завданої збиранням, збереженням, використанням та розголошенням відомостей про особу. Отже, необхідно враховувати комплексний характер інформаційного законодавства, що включає в себе конституційно-правові, адміністративно-правові, міжнародно-правові, цивільно-правові й кримінально-правові норми. Віддаючи пріоритет публічно-правовому регулюванню інформаційних правовідносин, не слід забувати й про приватноправові аспекти даних правовідносин.

Практично всі дії людини в сучасному світі фіксуються в різних базах даних (рахунки, чеки, медичні карти, трудові книжки тощо). На особливу увагу заслуговує питання визначення правового статусу інформації про особу (персональних даних) у сфері трудових правовідносин, оскільки саме в ный акумулюється найповніша база

(* Останнім часом у сфері захисту інформації законами України ратифіковано угоди між Кабінетом Міністрів України та Урядом Російської Федерації про взаємну охорону секретної інформації (15 листопада 2001 р.); Урядом Французької Республіки про взаємну охорону таємної інформації та матеріалів (5 липня 2001 р.); Урядом Італійської Республіки про взаємну охорону секретної інформації (10.01.2002 р.); Урядом Республіки Таджикистан про взаємну охорону секретної інформації (4 червня 2004 р.); Урядом Республіки Вірменія про взаємну охорону секретної інформації (19 червня 2003 р.); Урядом Туркменистану про взаємну охорону секретної інформації (10 січня 2002 р.); Урядом Республіки Польща про взаємну охорону секретної інформації (26 вересня 2002 р.); Урядом Чеської Республіки про охорону секретної інформації (8 вересня 2004 року); Урядом Латвійської Республіки про взаємну охорону секретної інформації (22 жовтня 2004 р.) тощо.

зазначених даних. Так, відповідно до частини другої статті 32 Конституції України не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Це конституційне положення деталізується низкою нормативних актів у сфері збирання, зберігання, використання та поширення інформації, в тому числі і про особу. Стаття 23 Закону України “Про інформацію” визначає інформацію про особу як сукупність документованих або публічно оголошених відомостей про особу. Джерелами документованої інформації про особу є видані на її ім’я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень. Інформація, яку працівник надає роботодавцю, повинна мати форму документа. Основними даними про особу (персональними даними) зазначена стаття Закону України “Про інформацію” визначає такі: національність, освіта, сімейний стан, релігійність, стан здоров’я, а також адреса, дата і місце народження.

За правилом, встановленим статтею 25 Кодексу законів про працю України [5], при укладанні трудового договору забороняється вимагати від осіб, які поступають на роботу, відомості про їх партійну і національну приналежність, походження, прописку та документи, подання яких не передбачено законодавством. У той же час, при укладанні трудового договору відповідно до частини другої статті 24 КЗпП України громадянин подає паспорт або інший документ, що посвідчує особу, трудову книжку, а у випадках, передбачених законодавством, – також документи про освіту (спеціальність, кваліфікацію), про стан здоров’я та інші.

Пункт 6 Положення про паспорт громадянина України [12], встановлює вимоги до інформаційного змісту паспортної книжечки громадянина України: на першу і другу сторінки паспортної книжечки заносяться прізвище, ім’я та по батькові, дата і місце народження. На десятій сторінці робляться відмітки про сімейний стан власника паспорта, на одинадцятій–шістнадцятій – про реєстрацію постійного місця проживання громадянина. На прохання громадянина до паспорта може бути внесено (сьома, восьма і дев’ята сторінки) на підставі відповідних документів дані про дітей, групу крові і резус-фактор.

Особа, яка претендує на зайняття посади державного службовця третьої – сьомої категорій, згідно із статтею 13 Закону України “Про державну службу” [9] подає за місцем майбутньої служби відомості про доходи та зобов’язання фінансового характеру, в тому числі і за кордоном, щодо себе і членів своєї сім’ї. Особа, яка претендує на зайняття посади державного службовця першої і другої категорій, повинна подати також відомості про належні їй та членам її сім’ї нерухоме та рухоме майно, вклади у банках і цінні папери.

У процесі трудових правовідносин роботодавцю згідно з чинним законодавством може знадобитися також інша інформація про працівників деяких категорій: про наявність у сімейних двох і більше утриманців при вирішенні питання про переважне право на залишення на роботі при звільненні працівників у зв’язку із змінами в організації виробництва і праці (пункт1 частини другої статті 42 КЗпП); про стан здоров’я осіб молодше вісімнадцяти років (стаття 191 КЗпП) та працівників, зайнятих на важких роботах, роботах із шкідливими чи небезпечними умовами праці або таких, де є потреба у професійному доборі (стаття 169 КЗпП) та в інших випадках, передбачених законодавством.

За загальним правилом (стаття 25 КЗпП, ст. 23 Закону України “Про інформацію”), роботодавцю заборонено вимагати персональні дані про політичні, релігійні, інші переконання і сімейне (приватне) життя працівника. Разом з тим, для працівників певних категорій встановлене інше. Так, відповідно до статті 5 Закону України “Про

статус суддів” [10], суддя не може належати до політичних партій та профспілок, брати участь у будь-якій політичній діяльності, мати представницький мандат, обіймати будь-які інші оплачувані посади, виконувати іншу оплачувану роботу, крім наукової, викладацької та творчої. Отже, отримання такої інформації є правомірним.

Дані про сімейне (приватне) життя працівника (інформація про життєдіяльність у сфері сімейних, побутових, особистих відносин), пов’язані з питаннями трудових відносин, можуть бути одержані роботодавцем від самого працівника, тобто тільки за його письмової згоди. Наприклад, чи є жінка одинокою матір’ю, чи має дитину-інваліда тощо (Глава XII КЗпП).

Під терміном “інші документи” мається на увазі, наприклад, ідентифікаційний номер фізичних осіб-платників податків та інших обов’язкових платежів, який відповідно до статті 7 Закону України “Про Державний реєстр фізичних осіб-платників податків та інших обов’язкових платежів” [11] є обов’язковим для використання підприємствами, установами, організаціями всіх форм власності, включаючи установи Національного банку України, комерційні банки та інші фінансово-кредитні установи, в разі: виплати доходів, з яких утримуються податки та інші обов’язкові платежі згідно з чинним законодавством України (оплата праці на підставі трудового договору); укладання цивільно-правових угод, предметом яких є об’єкти оподаткування та щодо яких виникають обов’язки сплати платежів (у тому числі договорів підряду); відкриття рахунків в установах банків.

Таким чином на підприємстві, в установі, організації, з якою громадянин укладає трудовий договір, формується певна база даних, яка згідно із Законом “Про інформацію” містить повний обсяг персональних даних про нього. Враховуючи викладене, під терміном “персональні дані працівника”, слід розуміти певний обсяг відомостей про дії та події в житті працівника за допомогою яких можна ідентифікувати його особу.

Виникає питання про режим зберігання, використання та поширення такої інформації. На превеликий жаль, аналіз чинного законодавства та правозастосовної практики дає підстави констатувати наявність у нормативно-правовій базі в частині інформаційних правовідносин нечітко визначених, колізійних положень і прогалин, що негативно впливає на забезпечення конституційних прав і свобод людини і громадянина. Частина друга статті 32 Конституції України вказує на особливості передбаченого правовими нормами порядку збирання, зберігання, використання і поширення конфіденційної інформації про особу – режим доступу до такої інформації. Але чинним законодавством України не повністю визначено режим збирання, зберігання, використання та поширення інформації, зокрема щодо персональних даних працівника. Закон України “Про інформацію” закріплює лише загальні принципи доступу до інформації, що стосується громадян, які перебувають у трудових відносинах з роботодавцем. Механізм реалізації зазначеної процедури належним чином не визначений. Відсутнє й регулювання використання конфіденційних даних у сфері трудових правовідносин. Так, відповідно до Закону України “Про інформацію” (статей 28 та 30) за режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну. Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. У той же час інформація про особу охороняється законом (стаття 23 Закону України “Про інформацію”).

Відповідно до частини четвертої статті 23 Закону України “Про інформацію” забороняється збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених законом. Згідно з Рішенням Конституційного Суду України від 30.10.1997 № 5-зп у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону

України “Про інформацію” та статті 12 Закону України “Про прокуратуру” (справа К.Г. Устименка) [13] частину четверту статті 23 Закону України “Про інформацію” треба розуміти так, що забороняється не лише збирання, а й зберігання, використання та поширення конфіденційної інформації про особу без її попередньої згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту, прав та свобод людини. До конфіденційної інформації, зокрема, належать свідчення про особу (освіта, сімейний стан, релігійність, стан здоров’я, дата і місце народження, майновий стан та інші персональні дані).

Висновки

Аналіз чинного законодавства дозволяє зробити висновок, що персональні дані працівника – певний обсяг відомостей про дії та події в житті працівника, за допомогою яких можна ідентифікувати його особу та які є особливим видом конфіденційної інформації, що охороняється законом, збирання, зберігання, використання та поширення якої без попередньої згоди працівника заборонено.

Для усунення суперечностей у визначенні та розмежування поняття “персональні дані” з іншими видами інформації, зокрема конфіденційної, а також правового регулювання порядку зберігання, використання та поширення персональних даних різними нормами та галузями права слід прийняти міжгалузевий нормативний документ на рівні закону “Про охорону та захист прав на персональні дані”.

Слід звернути увагу науковців, дослідників на необхідність активізувати діяльність для вироблення адекватних правових понять (дефініцій), в тому числі й суміжних із поняттям “персональні дані”.

Використана література

1. Конституція України від 28.06.1996 № 254к/96-ВР
2. Цивільний кодекс України від 16.01.2003 // “Голос України”, 12.03.2003.
3. Кримінальний кодекс України від 05.04.2001 № 2341-III // Відомості Верховної Ради України від 29.06.2001, № 25, ст. 131.
4. Кодекс України про адміністративні правопорушення від 7 грудня 1984 року № 8073-X.
5. Кодекс законів про працю України від 10.12.1971 № 322-VIII // Відомості Верховної Ради УРСР, 17.12.1971, № 50, ст. 375.
6. Закон України “Про інформацію” від 2 жовтня 1992 року № 2657-XII // Відомості Верховної Ради України, 1992, № 48, ст.650.
7. Закон України “Про друковані засоби масової інформації (пресу) в Україні” від 16.11.1992 № 2782-XII // Відомості Верховної Ради України від 05.01.1993, № 1, ст. 1.
8. Закон України “Про телебачення і радіомовлення” від 21.12.1993 № 3759-XII // Відомості Верховної Ради України від 09.03.1994, № 10, ст. 43.
9. Закон України “Про державну службу” від 16.12.1993 № 3723-XII // Відомості Верховної Ради України, 1993, № 52, ст. 490.
10. Закон України “Про статус суддів” від 15.12.1992 № 2862-XII // Відомості Верховної Ради України від 23.02.1993 - 1993 р., № 8, ст. 56.
11. Закон України “Про Державний реєстр фізичних осіб-платників податків та інших обов’язкових платежів” від 22.12.1994 № 320/94-ВР // Відомості Верховної Ради України, 10.01.1995, № 2, ст. 10.
12. Положення про паспорт громадянина України, затверджене постановою Верховної Ради України від 26 червня 1992 року № 2503-XII.
13. Рішення Конституційного Суду України від 30.10.1997 № 5-зп у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України “Про інформацію” та статті 12 Закону України “Про прокуратуру” (справа К.Г. Устименка).

УДК 351.713:336.225.64

С. ПОЗНЯКОВ, провідний науковий співробітник
НДЦ ПО Національної академії ДПС України

ІНФОРМАТИЗАЦІЯ КОМПЛЕКСНОЇ СИСТЕМИ ДЕТІНІЗАЦІЇ ВІДНОСИН У СФЕРІ ПОГАШЕННЯ ПОДАТКОВОГО БОРГУ ПЛАТНИКІВ ПОДАТКІВ

Анотація. *У статті розкривається мета, завдання та основні напрями інформатизації комплексної системи детінізації відносин у сфері погашення податкового боргу, а також визначено поняття та зміст системи превентивного адміністративного контролю.*

Реалізація адміністративної реформи в Україні і розвиток адміністративного законодавства; новелізація фінансового і податкового законодавства України та його адаптація до європейських правових стандартів; інформаційне забезпечення законотворчої, нормотворчої і правозастосовної діяльності визначено одними із пріоритетних напрямів розвитку правової науки на 2005 – 2010 рр. Для їх впровадження в життя необхідно розв’язання проблемної ситуації, пов’язаної з інформаційним забезпеченням управління, створенням злагодженої системи органів фінансового контролю, адаптацією вітчизняного фінансового та податкового законодавства до європейських стандартів, створенням теоретичної бази системної інформатизації правових інформаційних систем [1].

Євроінтеграційна стратегія розвитку України, реформування державного управління, стратегія розвитку державної податкової служби потребують спрямування зусиль податкової служби на збільшення дохідної частини бюджету шляхом вдосконалення та лібералізації податкового законодавства, розширення бази оподаткування, створення сприятливих умов для розвитку виробництва, приватного підприємництва, детінізацію економічних відносин, а також скорочення витрат на адміністрування податків шляхом спрощення системи податкового адміністрування, автоматизації адміністративних процесів у сфері оподаткування, реформування організаційно-функціональної структури органів державної податкової служби (далі – ОДПС) [2].

Аналіз досліджень і публікацій, в яких започатковано розв’язання даних проблем [3-6], свідчить лише про початок формування загальних та спеціальних (галузевих) напрямів теоретико-прикладних досліджень проблем інформатизації у сфері оподаткування. В цілому, проблеми правової інформатики у фінансовій сфері є досить різними за сутністю та змістом. Проте, з урахуванням результатів нашого дослідження є необхідність наукового напрацювання положень щодо *практичного створення спеціалізованих інтегрованих комп’ютеризованих систем фінансово-правової та адміністративно-правової інформації у сфері оподаткування*, які не лише б мали можливість одночасного адміністративного використання відповідної інформації як податківцями, так і підприємцями з метою зниження конфліктних ситуацій між ними, удосконалення процедур податкового адміністрування, але й ефективного забезпечення досягнення цілей, виконання завдань, функцій, передбачених податковим законодавством щодо попередження вчинення платниками податків податкових правопорушень, тіньової економічної діяльності.

Не вирішеною раніше частиною вищезазначених проблем є формування теоретико-прикладних засад інформаційно-аналітичного забезпечення комплексної системи детінізації відносин у сфері погашення податкового боргу платників податків, функціонування превентивного адміністративного контролю з метою попередження податкових

правопорушень, тіньової економічної діяльності.

Ціллю статті є започаткування дискусії науковців та практиків щодо запровадження в межах інформатизації сфери оподаткування нового напряму теоретико-прикладних досліджень – інформатизації комплексних систем детінізації відносин у сфері оподаткування і, зокрема, сфери погашення податкового боргу, визначення поняття та змісту системи превентивного адміністративного контролю у сфері погашення податкового боргу.

*Виклад основного матеріалу дослідження з обґрунтуванням отриманих результатів.*Метою інформатизації комплексної системи детінізації відносин у сфері погашення податкового боргу (далі – КСД) є інформаційно-аналітичне забезпечення створення сприятливого економіко-правового клімату для здійснення легальних фінансово-господарських операцій податкових боржників, а також створення оптимальної організаційної та функціональної інфраструктури суб’єктів управління у сфері погашення податкового боргу.

Одним із **основних завдань** інформаційно-аналітичного забезпечення комплексної системи детінізації відносин у сфері погашення податкового боргу є інформаційне забезпечення реалізації загальних груп заходів КСД-відносин у сфері погашення податкового боргу, а саме:

I. Організації створення умов органами державної влади для реалізації конституційного права громадян на здійснення легальної, економічно вигідної підприємницької діяльності.

II. Організації системи превентивного адміністративного контролю у сфері погашення податкового боргу як форми соціального контролю.

III. Заходів внутрішньоорганізаційної оптимізації адміністративно-правового режиму детінізації відносин у сфері погашення податкового боргу.

Інфраструктура інформаційно-аналітичного забезпечення КСД у сфері погашення податкового боргу платників податків повинна створюватися, *по-перше*, на основі базових інформаційних моделей, що розробляються на даний час в ОДПС у рамках проекту “Програма модернізації державної податкової служби України-1” [7], в т.ч. у таких напрямах , як:

- забезпечення внутрішньокорпоративної структурно-функціональної системи органів управління (контролю) – спеціальних підрозділів ОДПС щодо адміністрування податкового боргу;
- забезпечення зовнішнього середовища (системи функціональної та інформаційної взаємодії органів державної влади, контролюючих органів, установ та організацій щодо вирішення питань, пов’язаних із погашенням податкового боргу та детінізацією фінансово-господарської діяльності податкових боржників).

По-друге, інфраструктура інформаційно-аналітичного забезпечення стосовно до завдань нашого дослідження, повинна бути побудована *виходячи із вище визначених* загальних груп заходів КСД-відносин у сфері погашення податкового боргу щодо створення сприятливого економічного клімату для здійснення легальних фінансово-господарських операцій податкових боржників, а також створення оптимальної організаційної і функціональної інфраструктури суб’єктів управління у сфері погашення податкового боргу та їх інформаційного супроводження.

Інформаційно-аналітичне забезпечення у сфері погашення податкового боргу системно здійснюється на загальному та спеціальному рівнях інформаційної системи ОДПС.

1. *Загальний (внутрішньоорганізаційний та зовнішній) рівень інформаційно-аналітичного забезпечення КСД у сфері погашення податкового боргу* забезпечується функціонуванням загальної системи податкового адміністрування – функціонального та інформаційного забезпечення ОДПС.

2. *Спеціальний* (внутрішньоорганізаційний та зовнішній) рівень інформаційно-аналітичного забезпечення пов'язаний із специфічним завданнями *КСД у сфері погашення податкового боргу* – усунення факторів відтворення тіньових відносин та створення на цій основі економічних передумов зацікавленого ініціативного повернення відносин у сфері погашення податкового боргу з тіньового, тобто з різних причин неврахованого, у врахований державою капіталообіг, а також побудову на цій основі організаційно-правової інфраструктури превентивної протидії вчиненню тіньових проявів.

Центральним напрямом заходів забезпечення функціонування КСД у сфері погашення податкового боргу є організація функціонування системи превентивного адміністративного контролю.

Превентивний адміністративний контроль у сфері погашення податкового боргу – це комплекс превентивно-адміністративних заходів, які системно проводяться спеціально уповноваженими суб’єктами управління з метою забезпечення функціонування адміністративного контролю за своєчасністю виконання платниками податків своїх податкових зобов’язань, погашення податкового боргу, попередження податкових правопорушень, превентивної протидії вчиненню тіньових проявів, а також створення адміністративно-правових, фінансово-правових, інформаційно-правових засад для здійснення податковими боржниками легальної фінансово-господарської діяльності, забезпечення реалізації принципу публічності в розкритті необхідної інформації про податкових боржників для зацікавлених осіб.

До комплексу заходів із інформаційного забезпечення превентивного адміністративного контролю у сфері погашення податкового боргу включаються такі групи заходів.

1. Формування уповноваженими державними органами автоматизованих інформаційних баз даних про фінансово-господарську діяльність платників податків, а також адміністративно-правове забезпечення функціонування державної автоматизованої реєстрації визначених державою найбільш ризикових правочинів, які ними здійснюються.

Формування компетентним державним органом документальної справи на кожного платника податків (компанію), а також інтегрованих автоматизованих інформаційних баз даних (електронних накопичувальних справ) повинно відбуватися на стадії їх створення (державної реєстрації). У зазначених справах повинна формуватися інформація про їх діяльність, злиття, розподіл та ліквідацію. Найбільш ризикові правочини, які здійснюються платниками податків – податковими боржниками, повинні реєструватися у державному автоматизованому реєстрі правочинів. Зокрема, до найбільш ризикових правочинів у сфері погашення податкового боргу необхідно віднести:

- укладання та реалізація договорів купівлі-продажу, предметом яких є “устаткування”, “обладнання”, інше майно підприємств, що не підлягає приватизації;
- укладання та реалізація договорів купівлі-продажу цінних паперів акціонерних товариств, які є стратегічними для держави;
- укладання та реалізація договорів відчуження, використання, ліквідації (оренда, лізинг, сублізинг тощо) активів підприємств;
- операції щодо взаємозаліків, переуступки права вимоги, ін. фінансових договорів.

Обов’язковій державній реєстрації також повинні підлягати *протоколи загальних зборів* стратегічних для держави господарських товариств щодо їх рішень про

проведення операцій відчуження, використання, ліквідації (оренда, лізинг, сублізинг, тощо) активів зазначених підприємств, а також експортних контрактів (договорів) для контролю за погашенням їх податкового боргу (використання баз даних податкових та митних органів) під час експорту активів податкових боржників.

2. Створення та здійснення уповноваженими державними органами автоматизованого моніторингу фінансово-господарської діяльності податкових боржників на основі автоматизованих систем реєстрації правочинів та методу непрямого збору необхідної інформації із зовнішніх та внутрішніх (корпоративних) інформаційних джерел. У зазначений напрям входять такі заходи.

Здійснення моніторингу фінансово-господарської діяльності податкових боржників:

на основі:

2.1. автоматизованих інформаційних систем декларування: 1) виконання податкових зобов’язань; 2) проведення податковим боржником визначених державою ризикових фінансово-господарських операцій;

засобами:

2.2. автоматизованого робочого місця (АРМ) “Податковий керуючий” з автоматизованою інформаційно-аналітичною підсистемою непрямого збору необхідної інформації із зовнішніх та внутрішніх (корпоративних) інформаційних джерел із використанням триєдиної ролі документообігу у сфері погашення податкового боргу.

Від організації створення та функціонування АРМ “Податковий керуючий” та відповідних облікових автоматизованих інформаційних систем суб’єкта господарювання буде залежати ефективність інформаційно-аналітичного забезпечення функціонування КСД-відносин у сфері погашення податкового боргу. У зв’язку з цим, *податковий керуючий* повинен мати функціональну можливість адміністрування внутрішніх інформаційних ресурсів корпоративної системи податкових органів: автоматизованої інформаційної системи (АІС) “Облік платників та податків”, її підсистеми автоматизованої системи (АС) “Боржники”, використання АІС “Режимно-облікові бланки та їх користувачі” (у перспективі), АІС контрольно-попереджувального моніторингу (КПМ) у сфері виробництва та обігу підакцизних товарів (у перспективі), а також інформаційними ресурсами зовнішніх інформаційних джерел – баз даних щодо діяльності підприємств податкових боржників (на адміністративно-договірній основі) із митної служби, Пенсійного фонду України, органів управління щодо вирішення питань платоспроможності та фінансового оздоровлення податкових боржників, органів статистики, тощо.

Крім цього, створення АРМ “Податковий керуючий” має значення для досягнення цілей і завдань КСД-відносин у сфері погашення податкового боргу із наступними функціональними можливостями:

а) видача довідок засобами АРМу про наявність податкового боргу у платника податків на *бланках суворої звітності із електронною, автоматизованою реєстрацією інформації про даний факт* (дата видачі, посади службової особи, що видала, ПІБ);

б) ведення електронного реєстру видачі **копій документів**: 1) взяття на облік суб’єктів господарювання (з метою відстеження відкриття банківських рахунків податковими боржниками); 2) як платників податків (довідки про надання ідентифікаційного коду платника податків, свідоцтва);

в) формування та аналіз податкових ризиків у сфері погашення податкового боргу шляхом використання максимально можливого спектра наявної інформації про податкового боржника.

Однією із найголовніших превентивних функцій АРМу “Податковий керуючий” є організація створення автоматизованого обміну інформацією між АРМом і АБД суб’єктів управління у сфері погашення податкового боргу, а також державними реєстраційними базами даних. Зокрема, інфраструктуру обміну інформацією можливо визначити таким чином:

- системи “Реєстрація платників податків” (необхідність об'єднання з реєстром новостворених суб’єктів господарювання) – АРМ “Податковий керуючий”;
- АРМ “Податковий керуючий” – Державний автоматизований реєстр правочинів;
- АРМ “Податковий керуючий” – АБД митних органів;
- АРМ “Податковий керуючий” – Державний автоматизований реєстр обтяжень;
- АРМ “Податковий керуючий” – Національний банк України;
- АРМ “Податковий керуючий” – Державний комітет статистики України;
- АРМ “Податковий керуючий” – Національна комісія регулювання електроенергетики України;
- АРМ “Податковий керуючий” – Державна комісія з цінних паперів та фондового ринку.

Для вирішення питання неплатоспроможності, попередження невиконання своїх податкових зобов’язань, вчинення дій щодо незаконного банкрутства та усунення факторів тінізації фінансово-господарської діяльності підприємств податкових боржників у процедурах відновлення платоспроможності боржника та визнання його банкрутом інфраструктура обміну інформацією пропонується таким чином:

- АРМ “Податковий керуючий” – державний уповноважений орган з питань банкрутства;
- АРМ “Податковий керуючий” – Український центр реструктуризації підприємств та розвитку приватного сектору.

2.3. Триєдина роль документообігу у сфері погашення податкового боргу полягає в документальній фіксації юридично значущих фактів (правочинів), пов’язаних із різноманітними адміністративними аспектами організації цілеспрямованої діяльності суб’єктів та об’єктів у досліджуваній сфері. Насамперед, документальна фіксація відбувається за такими напрямами документування:

- загальна система зовнішнього та внутрішнього адміністративно-правового документообігу між податковим боржником та контролюючим органом як засобу здійснення превентивного адміністративного контролю у сфері погашення податкового боргу;
- системи обміну інформацією (документообіг) між суб’єктами управління для здійснення превентивного адміністративного контролю за проведенням визначених у законодавстві ризикових фінансово-господарських операцій податкового боржника (відчуження, використання, ліквідації активів) з метою попередження тіньового вимивання активів боржника та інших його правопорушень;
- системи документального моніторингу (поточного, ретроспективного спостереження) та аналізу щодо тіньових проявів податкових боржників, попередження фальсифікації та підробки облікової, звітної, адміністративної документації.

3. Система адміністративних запобіжно-припинювальних заходів забезпечення погашення податкових зобов’язань платників податків та вчинення тіньових проявів.

Система адміністративних запобіжно-припинювальних заходів щодо погашення податкових зобов’язань платників податків та попередження вчинення тіньових проявів повинна діяти з моменту порушення таким платником податків норм податкового закону. В основі превентивного функціонального механізму адміністративного

контролю повинен діяти правовий механізм **попереднього затримання активів платника податків** за рішенням податкового керуючого, який є відповідальним за виконання податкових зобов’язань закріпленим за ним платником податків, із складанням відповідного протоколу на строк 48 годин, протягом якого адміністративним судом вирішується питання щодо застосування адміністративного арешту активів (функція судового контролю над власністю). Також, повинно допускатися застосування **затримання активів** третьої сторони (дебітора) в частині, що належить податковому боржнику, на строк до 48 годин з послідуючим їх арештом за рішенням адміністративного суду.

Виходячи з цього основним функціональним правовим інститутом адміністративних запобіжно-припинювальних заходів пропонується визначити *удосконалений правовий механізм адміністративного арешту активів платника податків* (далі – арешт активів) як запобіжний, забезпечувальний та припинювальний захід (спосіб) щодо ухилення від виконання податкових зобов’язань, погашення податкового боргу платників податків, тіньової економічної діяльності, попередження порушень норм податкового закону. Арешт активів повинен застосовуватися в комплексі з іншими заходами інформаційно-аналітичного забезпечення, а саме:

1. Для забезпечення повноти обліку платників податків податковий орган повинний щомісячно проводити звірку районного рівня Єдиного банку даних платників податків (юридичних осіб) – Реєстру фізичних осіб з даними відповідних органів державної реєстрації та органів статистики з обов’язковим складанням актів звірок [8].

2. Створення **автоматизованої інформаційної системи** (АІС) **“Арешт активів”** для накопичення інформації, обліку дій, узгодження реєстрацій застосування обтяжень (за видами арештів), історії платника податків (правопорушника), щодо активів якого застосовувався або застосовано арешт активів, у яких банках заблоковано рахунки платника податків, стан рахунків у режимі арешту активів, у яких банках відкриті, закриті рахунки платника податків. Адміністраторами АІС “Арешт активів” повинні бути працівники спеціального правоохоронного підрозділу. Обмін інформацією повинен здійснюватися за такою схемою:

- АІС “Арешт активів” – Єдина інформаційна система з обліку, зберігання та оцінки майна, що реалізується за рішеннями органів виконавчої влади [9];
- АІС “Арешт активів” – Інформаційно-аналітична система обліку та контролю за реалізацією арештованого державними виконавцями майна [10];
- АРМ “Податковий керуючий” - АІС “Арешт активів” – Автоматизована інформаційна система контрольно-попереджувального моніторингу (АІС КПМ) (в стадії розробки) [11].

Висновки

Раціональна побудова інфраструктури інформаційного забезпечення КСД у сфері погашення податкового боргу, в т.ч. превентивного адміністративного контролю, надасть можливість розв’язати низку найбільш актуальних проблем не лише сфери оподаткування, а й інших сфер соціально-економічної діяльності.

Результатом інформатизації КСД у сфері погашення податкового боргу платників податків повинно бути:

1. Систематизація та уніфікація систем зовнішнього та внутрішнього електронного документообігу (за схемою суб’єкт господарювання – контролюючий орган – суб’єкт господарювання). На основі уніфікації та автоматизації системи документообігу у сфері погашення податкового боргу може бути створена оптимальна схема передачі, накопичення, аналізу, оцінки та прогнозування інформації про діяльність суб’єктів та об’єктів сфери погашення податкового боргу.

2. Налагодження оперативного обміну необхідною управлінською інформацією (документами) для прийняття ефективних та оптимальних управлінських рішень й забезпечення прискорення адміністративних процесів управління у сфері погашення податкового боргу.

3. Ефективне оперативне (поточне) спостереження, контроль та формування найбільш повної інформації за проведенням фінансово-господарської діяльності податкового боржника (відчуження, використання, ліквідації та ін.).

4. Проведення поточної роботи щодо попередження фальсифікації та підробки облікової, звітної, адміністративної документації.

5. Виявлення та попередження розвитку негативних факторів тіньової економічної діяльності податкового боржника без відповідного збільшення числа працівників контролюючого органу, витрат на проведення перевірки, а також *отримання додаткової можливості для контролюючого органу без зайвого втручання в роботу суб’єкта господарювання зберегти його прибуткову діяльність та забезпечити погашення його заборгованості перед бюджетом.*

Використана література

1. Пріоритетні напрями розвитку правової науки на 2005-2010 рр., рекомендовані відділеннями Академії правових наук України, затверджені Загальними зборами АПрН України 09.04.2004 р. // http://www.aprnu.kharkiv. org/nd/prioritet_n_2005-2010.htm

2. Про внесення змін до Стратегічного плану розвитку державної податкової служби України на період до 2013 року: Наказ ДПА України, від 29.09.2005 № 420 // http://www.liga.net/ zakon/ligazakon.html.

3. Мельник П., Попович В., Цимбалюк В. Щодо проблем правової інформатики у фінансовій сфері // Правова інформатика. – 2004. – № 2. – С. 11-15.

4. Мельник П., Попович В., Цимбалюк В. Становлення фінансово-правової інформатики у сфері оподаткування // Правова інформатика. – 2004. – № 3. – С. 9.

5. Безрученко В., Мойсюк О., Цимбалюк В. Комп’ютерні технології як засіб моделювання в діяльності податкової служби (у контексті проблем фінансово-правової інформатики) // Правова інформатика. – 2004. – № 4. – С. 11-20.

6. Новицький А. Інтеграція інформаційних систем як чинник підвищення ефективності контрольної діяльності // Правова інформатика. – 2004. – № 4. – С. 62-67.

7. Угода про позику (Проект “Модернізація державної податкової служби України – 1”) між Україною та Міжнародним банком реконструкції та розвитку, від 04.09.2003 // http://www.liga.net/ zakon/ligazakon.html.

8. http://www.sta.gov.ua/news.php3?7094.

9. Положення про Єдину інформаційну систему з обліку, зберігання та оцінки майна, що реалізується за рішеннями органів виконавчої влади: Наказ Фонду державного майна України від 26.03.2004 № 598, зареєстрований в Міністерстві юстиції України 25.05.2004 за № 651/9250 // http://www.liga.net/ zakon/ligazakon.html.

10. Положення про функціонування Інформаційно-аналітичної системи обліку та контролю за реалізацією арештованого державними виконавцями майна: Наказ Міністерства юстиції України від 21.01.2005 № 10/5, зареєстрований в Міністерстві юстиції України 24.01.2005 за № 88/10368 // http://www.liga.net/ zakon/ligazakon.html.

11. Гаркуша В.С., Мойсюк О.М., Позняков С.П. Спеціальне декларування господарських операцій та ідентифікація продукції як засоби попередження правопорушень у сфері обігу підакцизних товарів // Вісник податкової служби України. – 2003. – № 31.

УДК 656.13:625.712.63

О. ЗАГОРУЙ, аспірант Національного транспортного університету
Б. РАЦІБОРИНСЬКИЙ, *кандидат економічних наук,*
старший науковий співробітник

ОЦІНКА УМОВ БЕЗПЕКИ РУХУ В ЗОНІ ВПЛИВУ АВТОМОБІЛЬНОЇ СТОЯНКИ

(правові аспекти боротьби з порушниками Правил дорожнього руху)

Анотація. *У статті досліджуються питання впливу автомобільних стоянок та автомобілів, що припарковані уздовж проїжджої частини дороги на режим руху транзитних автомобілів та вносяться пропозиції щодо внесення змін до законодавства України про евакуацію транспортних засобів за порушення правил стоянки.*

Як елемент дорожніх умов автомобільні стоянки справляють певний формуючий вплив на режим руху автомобілів, які рухаються по основній дорозі, що поширюється на ділянці, довжина якої перевищує довжину проїзду території стоянки уздовж основної дороги. У зв’язку з цим, зону її впливу можна характеризувати як ділянку основної дороги, у межах якої транспортний потік має незручності, викликані наявністю стоянки та автомобілів, які залишені власниками на дорозі в місцях, заборонених для стоянки. Рух автомобілів у зоні впливу стоянки має ряд особливостей, обумовлених наявністю декількох взаємодіючих потоків автомобілів: транзитного, що рухається повз стоянку, заїжджаючих на її територію і виїжджаючих з неї. Таким чином, у зоні впливу, поряд з рухом транзитних автомобілів прямого ходу, яким надане переважне право проїзду, здійснюються маневри поділу і сполучення транспортних потоків.

Вплив стоянки на режим руху транзитних автомобілів проявляється зниженням їх швидкості і зміною траєкторії руху, обумовлених як наявністю спорудженої стоянки, так і впливом автомобілів, що з’їжджають і виїжджають з її території. Втрати часу, що виникають при цьому, є тим об’єктивним фактором, що зумовлює вибір оптимальних проектних рішень щодо організації руху автомобілів у зоні впливу автомобільної стоянки.

Втрати часу транзитних автомобілів у зоні впливу стоянок мають незначні розміри і питання про доцільність застосування стандартних пристроїв на з’їзді і виїзді з їх території вимагає теоретичних досліджень й експериментальної перевірки.

Під безпекою руху в зоні впливу автомобільної стоянки ми розуміємо усунення різкого порушення режиму руху автомобілів у тій частині дорожньо-транспортної інфраструктури, в якій можуть мати місце дорожньо-транспортні пригоди (далі – ДТП), зумовлені наявністю автомобільних стоянок. Для їх попередження і зведення нанівець ймовірності ДТП необхідно здійснити ряд інженерних заходів які забезпечать необхідну безпеку і зручність руху як для транзитного потоку автомобілів на основній дорозі, так і автомобілів, які заїжджають на територію стоянки чи виїжджають з неї на дорогу [1-3]. Вимоги щодо забезпечення безпеки руху є основним критерієм оцінки для функціонування і розміщення автомобільної стоянки, оскільки в даному випадку вони є необхідною умовою для дотримання двох інших критеріїв – економічності і зручності експлуатації.

Метою роботи є дослідження впливу автомобільних стоянок на безпеку дорожнього руху.

У ході натурних спостережень установлено, що при достатній площі стоянки і наявності упорядкованих під’їздів до неї відсутні небажані скупчення автомобілів (наявність черг), а отже, немає і простоїв, що, як правило мають місце на перетинаннях і примиканнях доріг. Таким чином, планувальні параметри під’їздів до автостоянок впливають тільки на режим руху транзитних автомобілів, що проявляються в зниженні їх швидкості і зміні траєкторії руху.

Облік умов безпеки руху впливає на результати технічно-економічного обґрунтування місткості, параметри розміщення стоянки відносно основної дороги; вибір ємності стоянки, кількості і планування під’їздів до неї; методи організації руху автомобілів і пішоходів на території стоянки і в зоні її впливу – на основну дорогу.

Вплив стоянок на безпеку руху автомобілів, які рухаються по основній дорозі і під’їздах, можна оцінити за допомогою статистичних даних щодо кількості і видів дорожньо-транспортних пригод, а також за величиною коефіцієнта безпеки ($K_б$), який характеризує умови забезпечення безпеки руху на даній ділянці дороги за величиною коливання швидкості автомобілів при в’їзді на неї [3, 4]. Значною мірою умови руху поблизу стоянок визначаються співвідношенням інтенсивності руху автомобілів на під’їздах і по основній дорозі. У зв’язку з цим, можна визначити поняття зони впливу стоянки як ділянці дороги, на довжину якої поширюється її вплив на режим і безпеку руху автомобілів.

У загальному випадку умови безпеки руху в зоні впливу стоянки можуть бути визначені шляхом аналізу взаємного впливу транспортно-експлуатаційних характеристик дороги, потоку автомобілів і технічно-експлуатаційних параметрів стоянки.

Для оцінки впливу стоянок на безпеку руху були зібрані звітні дані про види і кількість ДТП на обстежуваних дорогах за шість років (рис. 1). Для забезпечення порівняння отриманих результатів у якості оцінного використовувався показник відносної аварійності (K) – приведена кількість ДТП на 8,5 мільйона автомобілів [4]:

$$K = \frac{z \cdot k \cdot 10^7}{(N + N_1) \cdot 25} \quad , \tag{1.1}$$

де: z – середня кількість подій, зареєстрованих у зоні впливу стоянок за рік;

N – інтенсивність руху транзитних автомобілів по основній дорозі, авт./добу;

N_1 – інтенсивність руху автомобілів на під’їздах до стоянки, авт./добу;

k – коефіцієнт річної нерівномірності руху;

25 – коефіцієнт, що враховує середню кількість робочих днів на місяць, протягом яких завантаження доріг різко перевищує завантаження в неробочі дні.

Інтенсивність руху на під’їздах до стоянки (N_1) являє собою кількість автомобілів, що побували на території стоянки за добу, і визначається як:

$$N_1 = \frac{U_1}{a_n} \quad , \tag{1.2}$$

де: U_1 – число людей які скористувались послугами стоянки за добовий період її роботи;

a_n – середнє число людей в одному автомобілі з урахуванням складу потоку.

$$U_1 = m \cdot T \cdot \alpha \cdot \eta \text{, вод./год.,} \tag{1.3}$$

де: m – число місць на стоянці;

T – час роботи стоянки;

α – коефіцієнт обертання одиниці місткості стоянки;

η – коефіцієнт нерівномірності завантаження стоянки за час її роботи.

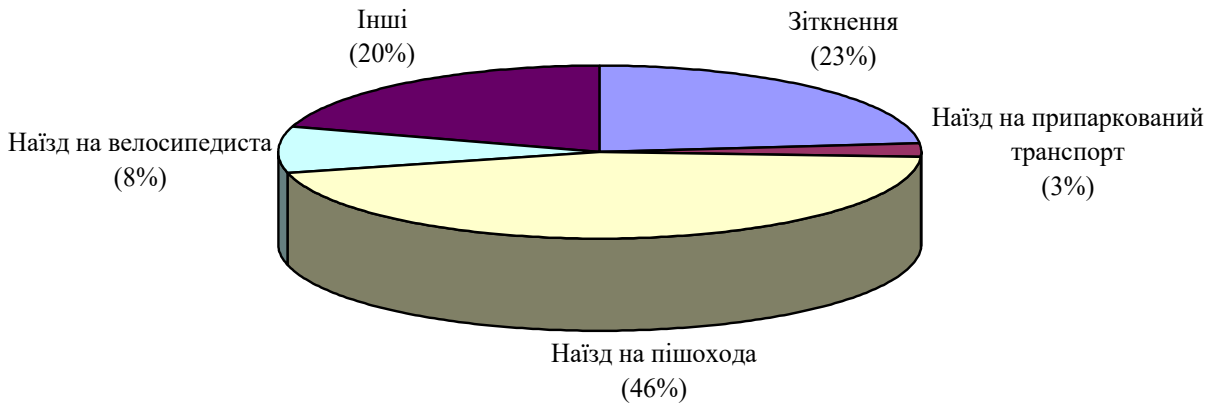


Рис. 1. Діаграма кількості і видів ДТП у зоні впливу автомобільних стоянок

Коефіцієнт обертання одиниці місткості (α) дорівнює максимальній кількості обслуговуючих водіїв за одиницю часу (1 год.). Величина α змінюється від долі одиниці (для стоянок з тривалим паркуванням) до 3-4 (для стоянок з короткочасним паркуванням) і визначається типом стоянки, режимом і тривалістю її роботи, організацією і формою обслуговування, удосконаленням технологічного облаштування.

Як свідчать отримані дані, ділянки доріг у зоні впливу стоянок можна віднести до: “дуже небезпечні” ($K > 12$), “небезпечні” ($6 < K < 12$), “мало небезпечні” ($3 < K < 8$) і “безпечні” ($K < 3$). Питома вага дорожньо-транспортних пригод у зоні впливу обстежених стоянок у загальному числі ДТП на дорогах із середньорічною інтенсивністю руху автомобілів у межах 2000 - 2500 авт./добу становила близько 20 %, а на дорогах, де інтенсивність перевищує 4000 авт./добу, до 25 % дорожньо-транспортних випадків.

Основна частина зіткнень автомобілів у зоні впливу стоянок відбувається в результаті помилок водіїв при здійсненні в’їзду з дороги на територію стоянки – 36 %, через стоянку автомобілів на проїжджій частині дороги (частково чи повністю) – 30 %, при здійсненні маневру розвертання – 21 %.

Наявність стоянки, її розміри і параметри розміщення суттєво впливають на безпеку руху. Це підтверджують встановлені залежності відносної аварійності (K) від місткості стоянки ($\boldsymbol{n}$) (рис. 2, табл. 1).

Таблиця 1

Значення коефіцієнтів залежності відносної аварійності від місткості стоянки

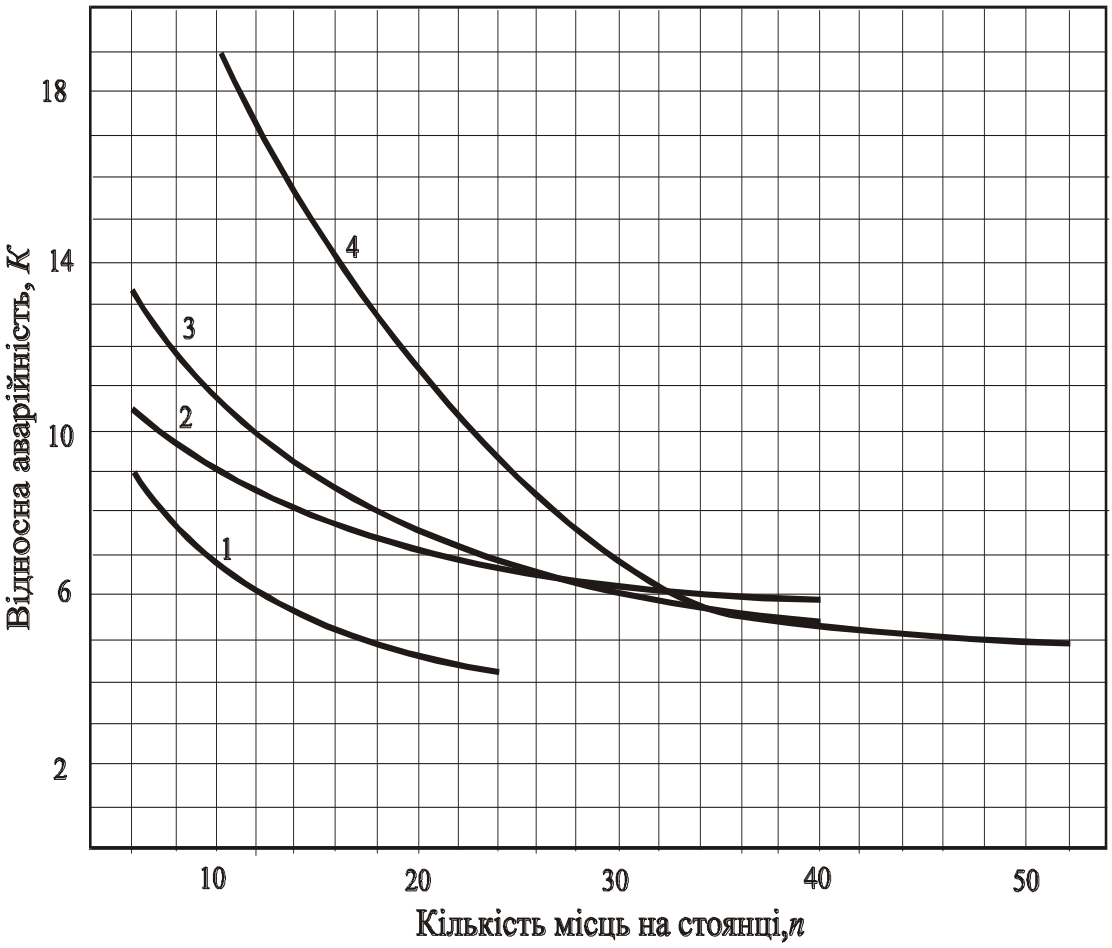
№ граф.	Вид залежності $K = f(n)$	Коефіцієнти		
		r	***t***	**F**
1.	K = 15,154-1,164+0,030 n^2	0,721	2,079	1,387
2.	K = 14,786+0,040-0,008 n^2	0,828	3,302	2,272
3.	K = 11,776-0,349+0,005 n^2	0,532	1,255	0,929
4.	K = 30,385-1,279+0,016 n^2	0,804	2,706	1,888
5.	K = 10,635-0,838+0,020 n^2	0,856	2,867	2,244
6.	K = 28,459-0,861+0,011 n^2	0,987	0,818	24,008
7.	K = 15,510-0,163+0,008 n^2	0,971	7,010	10,428
8.	K = 35,341-1,037+0,009 n^2	0,637	1,432	1,010

Загальний вигляд отриманих залежностей свідчить про згасаючі характери впливу місткості стоянки (n) на величину торгової виручки підприємства в день (C_T) і відносну аварійність (K). Відповідно, якщо таке граничне значення n, після якого зміна C_T і K стає незначним, то виходячи з умов економічності і забезпечення безпеки руху дослідження залежностей $C_T = f(n)$ і $K = f(n)$ встановлюють раціональні значення місткості стоянки у підприємств громадського харчування (табл. 1.2)

Таблиця 1.2

Раціональне значення місткості стоянки поблизу підприємств громадського харчування

Назва підприємства	Місткість, посадк. місць	Ємність стоянки, авт. місць		
		за наявних умов		Рекомендовані значення
		$C_T = f(n)$	$K = f(n)$	
Кафе	20 - 30	14	12	15
	31 - 40	30	32	25
	41 - 50	30	30	30
	51 - 60	32	30	35
Ресторани	40 - 50	10	6	10
	51 - 60	15	20	20



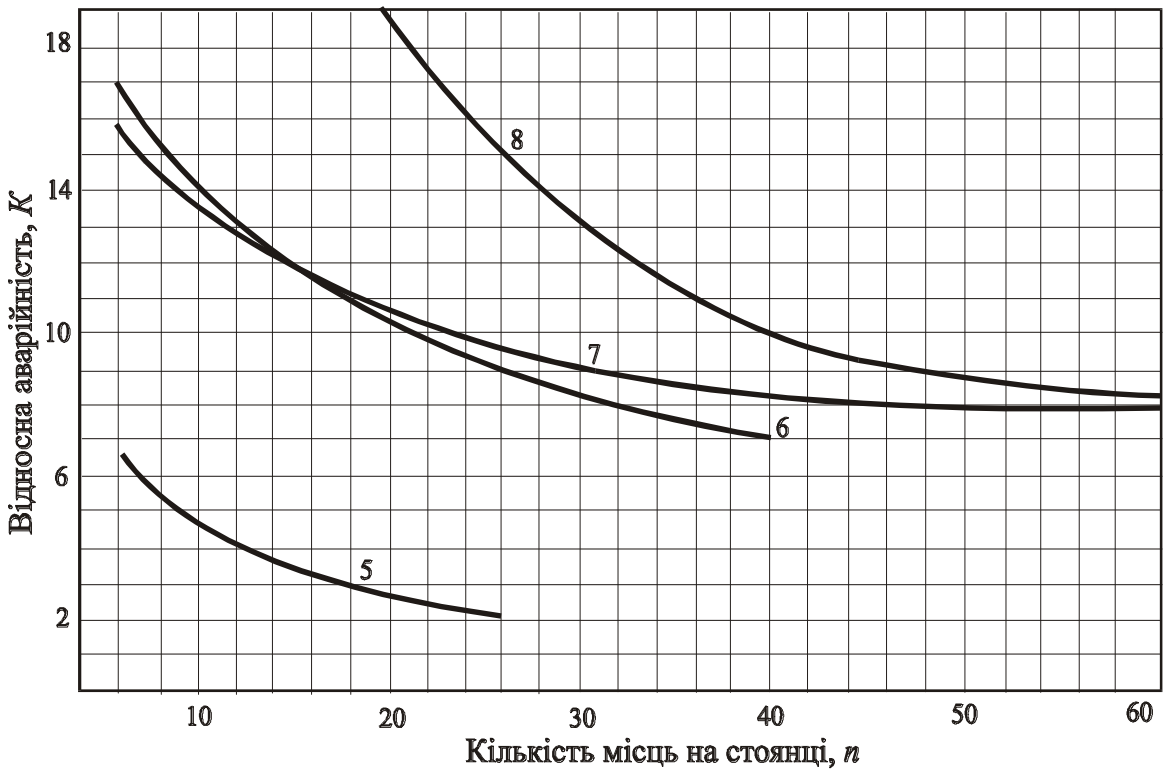


Рис. 2. Залежність відносної аварійності (К) від розміру стоянки у підприємств харчування: а) кафе; б) ресторани.

Таким чином, раціональна місткість автостоянки для кафе, ресторанів, дорожньої інфраструктури становитиме відповідно $n = 0,6\ m$ і $n = 0,3\ m$.

Проблема неправильного паркування транспорту існує досить давно. З метою її вирішення в Україні запроваджені Правила благоустрою території, паркування транспортних засобів, що передбачають примусову доставку на спеціальні майданчики транспортних засобів, які неправильно поставлені на стоянку чи з порушенням Правил дорожнього руху. Останнім часом знайдено досить ефективний спосіб боротьби з порушниками правил стоянки: евакуація транспортних засобів, залишених у неналежному місці. Автомобілі, які припарковано з порушеннями Правил дорожнього руху, вилучаються на штраф-майданчик спеціальними автомобілями – евакуаторами. Працює евакуатор разом із спеціальними мобільними групами ДАІ. Насамперед, вилучаються автомобілі не просто залишені там, де заборонена зупинка, а ті, котрі, крім всього іншого, заважають руху: на зупинках громадського транспорту, на трамвайних шляхах, на перехрестях, на пішохідних переходах, у місцях в’їздів і виїздів, у другому ряді. Повертається автомобіль власнику лише після оплати штрафу за порушення Правил дорожнього руху та “послуг” евакуатора. Але слід зазначити, що дана система не набула ще ефективного застосування в Україні, оскільки дії евакуаторів досконально не захищені законом.

Висновки

1. Проаналізовано звітні дорожньо-транспортні пригоди (ДТП) на автомобільних дорогах України за шість років. Питома вага дорожньо-транспортних випадків у зоні впливу обстежених стоянок у загальному числі ДТП на дорогах у середньому становить близько 20 %.

2. Основними причинами високої аварійності в існуючій мережі автостоянок є:

– невідповідність попиту місткості і частоти розміщення стоянок;

– недостатні розміри стоянок;

– невірне, з погляду забезпечення безпеки руху, розміщення стоянок;

– відсутність чи невдала геометрія під’їздів до стоянок;

– недоліки в організації руху автомобілів і пішоходів у зоні впливу стоянок на основній дорозі і на їх території.

3. Для ефективного застосування різних способів боротьби з порушниками правил стоянки необхідно внести зміни та доповнення в законодавство України. На наш погляд, необхідно максимально захистити законом вищенаведений спосіб боротьби з порушниками правил паркування транспортних засобів, одночасно передбачивши створення цивілізованих умов для їх паркування у спеціально відведених місцях.

Використана література

1. Автомобильные перевозки и организация дорожного движения: сСправочник ; пер. с англ. / В. Рэнкин, П. Клафи, С. Халберт и др. – М.: Транспорт, 1981. – 592 с.

2. Безопасность движения автомобильного транспорта: справочник / Талицкий И.И. – М.: Росагропромиздат, 1988. – 312 с.

3. Бородина С.Г. Проектирование сооружений обслуживания на автомобильных дорогах с учетом обеспечения безопасности движения: дис… к-та техн. наук / МАДИ. – М., 1982. – 186 с.

4. Романов А.Г. Дорожное движение в городах: закономерности и тенденции. – М.: Транспорт, 1984. – С. 52-79.

ВІД РЕДАКЦІЙНОЇ КОЛЕГІЇ

Неофіційний переклад

Рекомендації Ради Європи № R(87)15 від 17.09.1987 р.

“ПРО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ДАНИХ У СЕКТОРІ ПОЛІЦІЇ”

(Схвалено Комітетом Міністрів держав-членів Ради Європи 17 вересня 1987 року на 410-й зустрічі заступників Міністрів)

Комітет Міністрів Ради Європи згідно зі Статтею 15б Статуту Ради Європи,

враховуючи, що мета Ради Європи – досягнення більшої єдності між її членами,

зважаючи на зростаюче використання персональних даних у зв’язку з їх автоматизованою обробкою у секторі поліції та майбутньою користю від застосування комп’ютерів та інших технічних засобів у цій сфері,

беручи до уваги стурбованість можливою загрозою правам особи, що виникає внаслідок неправильного застосування методів автоматизованої обробки її даних,

визнаючи необхідність збалансування інтересів суспільства щодо прав та основних свобод людини, з одного боку, та запобігання й припинення кримінальних правопорушень і підтримання громадського порядку, з іншого боку,

пам’ятаючи про положення Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних від 28 січня 1981 року, і зокрема про винятки, що дозволені на підставі Статті 9,

враховуючи положення Статті 8 Конвенції про захист прав людини та основних свобод,

р е к о м е н д у є урядам держав-членів:

керуватися в їх внутрішньому законодавстві та практиці принципами, що надані у Додатку, та забезпечувати інформування громадськості щодо виконання положень цих Рекомендацій, зокрема що стосуються прав, які надаються індивідам через їх застосування.

Д о д а т о к

Сфера застосування і визначення

Принципи, що містяться в цих Рекомендаціях, стосуються збирання, зберігання, використання та передачі персональних даних, які є об’єктом автоматизованої обробки, в цілях поліції.

Термін “персональні дані” означає будь-яку інформацію, що стосується ідентифікованої чи не ідентифікованої особи. Особа не повинна розглядатися як така, що ідентифікується, якщо ідентифікація вимагає невиправданих витрат часу, коштів або людських ресурсів.

Термін “у цілях поліції” означає всі завдання, які можуть розв’язувати органи поліції для запобігання чи припинення кримінальних правопорушень та досягнення громадського порядку.

Термін “відповідальний орган” (контролер файла) означає орган, службу чи будь-яку іншу організацію, уповноважену згідно з національним законом вирішувати питання про цілі обробки файлу, категорії персональних даних, що мають зберігатися, та операції, які можуть застосовуватися до них.

Держави-члени можуть застосовувати принципи, що містяться в цих Рекомендаціях, до персональних даних, що не підлягають автоматизованій обробці. Ручна обробка даних не повинна проводитись, якщо її метою є невиконання положень цих Рекомендацій.

Держави-члени можуть поширювати принципи, що містяться в цих Рекомендаціях, на дані, що стосуються груп людей, асоціацій, фундацій, компаній або будь-якої іншої організації, що складається безпосередньо або опосередковано з індивідів, незалежно від того, чи такі організації мають статус юридичної особи.

Положення цих Рекомендацій не повинні витлумачуватися як такі, що обмежують або перешкоджають можливості держав-членів поширювати при потребі окремі з цих принципів на збирання, зберігання та використання персональних даних у цілях державної безпеки.

Основні принципи

Принцип 1 – Контроль та повідомлення

1.1.Кожна держава-член повинна мати незалежний наглядовий орган за межами поліцейського сектору, який би відповідав за забезпечення поваги до принципів, викладених у цій Рекомендації.

1.2. Нові технічні засоби обробки даних можуть запроваджуватися лише в разі, коли вжито всіх розумних заходів, щоб їх використання відповідало духові існуючого законодавства про захист даних.

1.3. Відповідальний орган повинен радитись із наглядовим органом заздалегідь у будь-якому випадку, коли застосування методів автоматизованої обробки породжує проблему із втіленням цієї Рекомендації.

1.4. Постійні автоматизовані файли повинні повідомлятися наглядовому органу. Повідомлення повинно вказувати на характер кожного задекларованого файла, установу, відповідальну за його обробку, її цілі, тип даних, що містяться у файлі, а також осіб, яким ці дані передаються.

Тимчасові файли, які були створені під час конкретного розслідування, також повинні повідомлятися контролюючому органу у відповідності з умовами, встановленими останнім, або згідно з національним законодавством.

Принцип 2 – Збір даних

2.1. Збір персональних даних у цілях поліції повинен обмежуватись мірою, необхідною для відвернення реальної небезпеки чи припинення кримінального правопорушення особливого характеру. Будь-який виняток з цього положення повинен бути предметом спеціального національного законодавства.

2.2. Якщо дані про індивіда були зібрані і зберігаються без його відома і якщо дані не знищені, він повинен бути поінформований, у разі доцільності, що інформація про нього тримається як тільки предмет діяльності поліції більше не цікавить її.

2.3. Збір даних за допомогою технічних чи інших автоматизованих засобів може здійснюватися лише відповідно до особливих положень.

2.4. Збір даних про осіб лише на тій підставі, що вони мають особливе расове походження, особливі релігійні переконання, сексуальну поведінку чи політичні погляди або належать до особливих рухів чи організацій, які не оголошені поза законом (“вразливі” дані), повинен заборонятися. Збір даних, що торкаються цих питань, може здійснюватися у разі виняткової потреби для цілей конкретного розслідування.

Принцип 3 – Зберігання даних

3.1. Наскільки можливо, зберігання персональних даних для цілей поліції має обмежуватися точними даними, які необхідні поліції для виконання її підрозділами правомірних завдань у межах внутрішнього законодавства та обов’язків, визначених міжнародним правом.

3.2. Наскільки можливо, різні категорії даних мають розрізнятися при зберіганні за ступенем їх точності або надійності, а саме: дані, що ґрунтуються на фактах, мають відрізнятися від тих, що основані на міркуваннях чи особистих оцінках.

3.3. Якщо дані, зібрані для адміністративних цілей, зберігатимуться постійно, їх слід тримати в окремому файлі. В будь-якому разі, слід вжити заходів, щоб адміністративні дані не підпадали під привила, що застосовуються для поліцейських даних.

Принцип 4 – Використання даних поліцією

Згідно з Принципом 5 особливі дані, зібрані й збережені поліцією для цілей поліції, мають використовуватися виключно в цих цілях.

Принцип 5 – Передача даних

5.1. Повідомлення у межах сектору поліції. Передача даних між підрозділами поліції для використання їх у цілях поліції повинна дозволятися, якщо існує законна підстава для їх передачі у межах законних повноважень цих підрозділів.

5.2 (i). Повідомлення іншим державним органам. Передача даних іншим державним органам дозволяється в окремих випадках, якщо:

а) існує чіткий законний обов’язок або дозвіл чи з санкції наглядового органу, або якщо

б) дані необхідні одержувачу для виконання ним його правомірного завдання, при цьому, ціль збирання чи обробки, яка здійснюватиметься одержувачем, повинна бути сумісною з первинною обробкою, а правові зобов’язання органу, що передає, мають не суперечити цьому.

5.2 (ii). Передача іншим державним органам дозволяється винятково в таких випадках:

а) коли повідомлення, поза всяким сумнівом, здійснюється в інтересах суб’єкта даних або коли останній дав на це згоду чи коли обставини вказують на явну презумпцію такої згоди;

б) коли передача даних необхідна для відвернення серйозної небезпеки.

5.3 (i). Повідомлення приватним структурам. Повідомлення даних приватним структурам дозволяється, зокрема, коли існує інше законне зобов’язання або дозвіл чи санкція наглядового органу.

5.3 (ii). Повідомлення приватним структурам дозволяється як виняток у таких випадках:

а) в інтересах суб’єкта даних або коли останній дав на це згоду чи коли обставини вказують на наявність такої згоди;

б) повідомлення необхідне для відвернення серйозної навислої загрози.

5.4 Міжнародна передача. Повідомлення даних органам влади іноземних держав повинно обмежуватися органами поліції. Воно дозволяється лише:

а) коли існує чітке правове забезпечення за внутрішнім чи міжнародним правом;

б) за умови відсутності такого забезпечення, якщо передача необхідна для запобігання серйозної навислої небезпеки або потрібна для припинення серйозного кримінального правопорушення відповідно до звичайного права і забезпечується, щоб національне регулювання захисту особи не було під загрозою порушення.

5.5 (i). Запити про повідомлення. Згідно зі спеціальними положеннями внутрішнього законодавства чи міжнародних угод у запитах про передачу інформації повинна вказуватись організація чи особа, що робить запит, а також причина запиту та її правомірність.

5.5 (ii). Умови повідомлення. Якість даних повинна, за можливістю, перевірятися щонайпізніше в час їх повідомлення. При всіх повідомленнях даних, за можливістю, зазначається юридичне рішення щодо цього, а також рішення не робити передачу і дані, що спираються на точку зору або особисте враження, перевіряються, перш ніж бути переданими, при цьому зазначається міра достовірності й надійності повідомленого.

Якщо виявиться, що дані вже не точні на даний момент, їх не слід передавати. Якщо дані, що не є точними або актуальними передано, то організація, яка здійснила передачу, повинна за можливістю, інформувати одержувача даних про їх невідповідність.

5.5 (iii).Захист передачі. Дані, повідомлені іншим державним органам, приватним структурам чи іноземним органам, не повинні використовуватися в інших цілях, окрім тих, що зазначені в запиті.

Використання даних в інших цілях, що не передбачені в параграфах 5.2 чи 5.4 цього принципу, повинне бути узгоджене з організацією, що здійснює передачу.

5.6 Взаємопов’язування файлів і доступ до файлів у діалоговому режимі. Пов’язування файлів до файлів, здійснюване в різних цілях, підлягає одній з умов:

(а) згода наглядового органу для цілей розслідування щодо правопорушення або

(б) згідно з чітким правовим положенням.

Прямий доступ (доступ у діалоговому режимі) до файла може дозволятися лише, якщо це узгоджується із внутрішнім законодавством, яке повинне враховувати Принципи 3 – 6 цієї Рекомендації.

Принцип 6 – Доступність для громадськості, право доступу до файлів поліції, право на виправлення даних і право на оскарження

6.1 Наглядовий орган повинен вживати заходів, щоб громадськість була поінформована про існування файлів, які є об’єктом повідомлення, а також про її права стосовно цих файлів. Втілення цього принципу передбачає врахування особливого характеру тимчасових файлів, зокрема потребу уникати перешкод щодо виконання законних завдань органами поліції.

6.2 Суб’єкт даних повинен мати змогу доступу до поліцейського файла в розумних інтервалах часу і без надмірного зволікання згідно з положеннями внутрішнього законодавства.

6.3 Суб’єкт даних повинен мати змогу зробити, де це необхідно, виправлення його даних, що містяться у файлі.

Персональні дані, які через реалізацію права доступу виявились неточними або надмірними чи невідповідними будь-якому з інших принципів цієї Рекомендації, повинні знищуватися, виправлятися або супроводжуватися уточнюючою запискою, доданою до файла.

Таке знищення або корегування повинні поширюватися, наскільки це можливо, на всі документи, що супроводжують поліцейський файл, і здійснюватися негайно або принаймні під час подальшої обробки даних або їх наступної передачі.

6.4 Застосування прав доступу, виправлення та знищення може обмежуватись лише тією мірою, наскільки це обмеження є необхідним для виконання законного завдання поліції або необхідне для захисту суб’єкта даних чи прав і свобод інших осіб.

В інтересах суб’єкта даних письмовий коментар повинен не допускатися законом у специфічних справах.

6.5 Відмова в цих правах чи їх обмеження повинне пояснюватися письмово із зазначенням причин. Єдиним випадком, коли відмовляють в ознайомленні з цими причинами, є необхідність виконання правомірного завдання поліції або необхідність захисту інших осіб.

6.6 Якщо в доступі відмовлено, суб’єкт даних повинен мати можливість оскаржити це до наглядового органу або іншого незалежного органу, який має підтвердити, що відмова належно обґрунтована.

Принцип 7 – Тривалість зберігання і поновлення даних

7.1. Повинно забезпечуватися, щоб персональні дані, які зберігалися для поліцейських цілей, знищувалися, якщо вони більше не потрібні для цілей, заради яких вони зберігалися.

З цією метою особлива увага звертається на такі критерії необхідності зберігання даних: у світлі висновку слідства в особливому випадку; остаточного судового рішення, зокрема у випадку виправдання, реабілітації, амністії.

7.2. Правила націлені на зазначення терміну зберігання персональних даних різних категорій, так само як і регулярні перевірки їх якості мають визначатися за погодженням з наглядовим органом або згідно з внутрішнім законодавством.

Принцип 8 – Безпека даних

Відповідальний орган повинен вжити всіх заходів, щоб забезпечити належну фізичну і логічну схоронність даних і запобігти їх несанкціонованому доступу, передачі чи зміні.

При цьому має враховуватися зміст файлів.

****

П О Я С Н Ю В А Л Ь Н И Й М Е М О Р А Н Д У М

до Рекомендації РЄ № R(87) від 15 від 17.09.1987 р.

Вступ

1. Незважаючи на те, що принципи захисту даних, викладені в Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних (відома як Конвенція РЄ № 108 про захист даних) від 28 січня 1981 року, широко застосовуються при збиранні, зберіганні, використання тощо персональних даних як у приватному, так і державному секторах, відчувається необхідність пристосувати їх до специфічних вимог особливих секторів.

2. “Секторний підхід” до захисту даних зумовив прийняття Комітетом Міністрів Ради Європи чотирьох рекомендацій, вироблених її Міжурядовим Комітетом експертів із захисту даних: Рекомендація № R(81)1 про правила для автоматизованих банків медичних даних (від 23 січня 1981р.), Рекомендація № R(83)10 із захисту персональних даних, використовуваних у наукових дослідженнях та статистиці (від 23 вересня 1983р.), Рекомендація №R(85)20 із захисту персональних даних, використовуваних в цілях прямого маркетингу (від 25 жовтня 1985р.) і Рекомендації № R(86)1 із захисту персональних даних, використовуваних у секторі соціального забезпечення (від 23 січня 1986 р.).

3. У зв’язку з таким секторним підходом, Комітет експертів із захисту даних дійшов висновку про доцільність реагування на проблеми захисту даних, породжених використанням персональних даних у секторі поліції, також про підготовку законодавчого інструменту провадження низки принципів, створених для врегулювання збирання, зберігання, використання, передачі і консервації персональних даних поліцією, який був би витлумачений у межах норм, викладених у Конвенції про захист даних.

4. Враховуючи зростання ролі поліції в житті людей, зумовлену новими загрозами суспільству у вигляді тероризму, наркобізнесу тощо, а також загальним зростанням злочинності, було визнане за необхідне виробити чинні керівні принципи для сектору поліції, які б підкреслювали таке необхідне в наших суспільствах збалансування прав особи та правомірної діяльності поліції, коли остання звертається за допомогою до технологій обробки даних.

5. Беручи до уваги, що параграф другий Статті 9 цієї Конвенції дозволяє державам-членам відхилятися від принципів захисту даних Конвенції з метою “припинення кримінальних правопорушень”, комітет експертів уповноважив робочу групу окреслити проблеми, що виникають при використанні персональних даних у секторі поліції, й виробити чіткі пропозиції щодо їх вирішення. Робочу групу склали експерти з Бельгії, Франції, Італії, Нідерландів, Португалії, Швеції, Швейцарії та Об’єднаного Королівства. Під головуванням д-ра Р.Швейзера (Швейцарія) робоча група провела п’ять зустрічей.

6. Протягом першої зустрічі (19 і 20 грудня 1983 р.) робоча група спробувала визначити, якою мірою законодавства держав-членів забезпечені спеціальними положеннями, що регулюють використання персональних даних у секторі поліції. Крім того, було зроблено широкий огляд проблем цього сектору щодо захисту даних. У зв’язку з цими завданнями робоча група була забезпечена дослідженням, проведеним консультантом, професором Х.Маісл (Франція).

7. Під час другої зустрічі (18-20 червня 1984 р.) члени робочої групи поглибили вивчення питань, врахувавши відповіді, отримані від держав-членів на запитання. Крім того, робоча група проаналізувала відповідні судові прецеденти Європейського Суду та Європейської Комісії з прав людини у контексті Статті 8 Європейської Конвенції з прав людини, яка є основоположною для збирання, використання, зберігання тощо персональних даних поліцією.

В процесі обговорення було вироблено проект, який відображає бачення робочою групою шляхів урегулювання використання персональних даних у сфері поліції.

8. На третій зустрічі (17-19 грудня 1984 р.) робоча група переглянула попередній проект. Уважному розгляду було піддано, зокрема, перелік обмежень, викладених у 2 параграфі Статті 9 Конвенції про захисту даних. Робоча група дійшла згоди про доцільність заснування спеціальних принципів захисту даних для класичних завдань поліції, пристосувавши їх до особливих вимог, особливо по відношенню до завдання “припинення кримінальних правопорушень”.

9. Спираючись на коментарі та огляди, представлені пленарним комітетом, робоча група поширила свій аналіз під час подальших зустрічей (5-7 червня 1985 р., 27-29 листопада 1985 р.), щоб вирішити такі питання, як повідомлення даних поліцією третім сторонам і особливо щодо транскордонних потоків даних. Пленарному комітету було представлено остаточний текст проекту пояснювального меморандуму, підготовленого секретаріатом.

10. Комітет експертів схвалив проект Рекомендацій і проект пояснювального меморандуму на 13-й зустрічі (4-7 листопада 1986 р.) після докладного ознайомлення і вирішив надати ці тексти Європейському Комітету з правового співробітництва для ознайомлення і схвалення.

11. Проект Рекомендацій і проект пояснювального меморандуму були схвалені Європейським Комітетом з правового співробітництва 22 травня 1987 року.

Докладні коментарі

Преамбула

Техніка все ширше застосовується в роботі поліції. У секторі, де збирання, зберігання величезної кількості персональної інформації необхідне з урахуванням різнопланової й важливої ролі поліції в суспільстві, переваги від використання технічних засобів незаперечні. Різноманітна злочинність вимагає вироблення таких же витончених методів боротьби з правопорушеннями. Комп’ютери дозволили поліції піднести її ефективність у збиранні персональних даних та сприяти швидкому прийняттю рішень у посиленні законності на користь суспільства.

Разом з тим, проблеми посиленого використання засобів автоматизації в усіх сферах, що спричинили прийняття Конвенції № 108 про захист осіб у зв’язку з автоматизованою обробкою персональних даних від 28 січня 1981 року, особливо гостро відчуваються у сфері поліції. Саме в цій сфері наслідки порушення основоположних принципів, викладених у цій Конвенції, особливо тяжко позначаються на індивіді.

Преамбула визначає необхідність досягнення збалансованості між інтересами зацікавлених сторін: інтересами особи і його правом на приватність та інтересами суспільства в запобіганні й припиненні кримінальних правопорушень та підтримані громадського порядку.

Не дивно, що збалансування важливо досягти в поліцейському секторі. Стаття 8, параграф 2 Європейської Конвенції з прав людини та Стаття 9 Конвенції про захист даних дозволяють робити винятки з прав, які вони пропонують.

Незважаючи та те, що преамбула застерігає щодо можливої загрози приватності особи внаслідок неправильного застосування методів автоматизованої обробки, варто мати на увазі, що приватність не можна витлумачувати лише як захист чиєїсь приватної сфери від настирливості. З цієї причини преамбула звертає увагу на Статтю 8 Конвенції про захисту прав людини та основних свобод, на законність застосування певних технічних засобів стеження для отримання даних про людей, і на те, щоб ті узгоджувалися з положеннями Статті 8 та відповідними висновками Європейського Суду з прав людини.

Звернення до підслуховування телефонних розмов та перехоплення кореспонденції – приклади зневажання приватного життя у строгому розумінні. Європейський Суд з прав людини ухвалив таке рішення у двох справах (Справа Класа [Klass] та ін., судове рішення від 6.9.1978 р., серія А, № 28; справа Мелоуна [Malone], судове рішення від 2.9.1984 р., серія А, № 82). Принципи 2.2 та 2.3 мають тлумачитися у світлі судових прецедентів цього Суду.

Проте преамбула також посилається на положення Конвенції РЄ № 108 від 28 січня 1981 року, які виходять за рамки традиційного визначення приватності, і встановлює низку захисних принципів, розроблених з метою врегулювання збирання, зберігання, використання та передачі персональних даних.

Спеціальна увага в преамбулі приділена обмеженням, дозволеним згідно зі Статтею 9 Конвенції про захист даних. Проте, винятки з положень Статті 5 (“якість даних”), Статті 6 (правила про “спеціальні категорії даних”) та Статті 8 (“додаткові гарантії для суб’єкта даних”) санкціонуються лише тоді, коли вони передбачаються законом і є необхідним заходом у демократичному суспільстві виключно в інтересах, серед іншого, “припинення кримінальних правопорушень”. Пам’ятаючи, що Європейський Суд з прав людини своїм рішення у справі Мелоуна визначив чіткі критерії (точність, переконливість, передбачуваність тощо), можна сподіватися, що принципи, викладені в цьому рекомендаційному правовому документі, повинні служити корисними порадами законодавцю у справі тлумачення обмежень параграфа 2 Статті 9 Конвенції Ради Європи № 108 про захист персональних даних при обробки персональних даних у сфері поліції. Це слід мати на увазі в контексті, наприклад, параграфа 2.1.

Зрозуміло, що перелік обмежень вужчий, ніж суспільні інтереси, окреслені у параграфі 5 преамбули. Проте мета цих Рекомендацій полягає в тому, щоб установити спеціальні принципи захисту даних для класичних та вирішальних завдань поліції, а також пристосувати ці

принципи до особливих вимог, зокрема заходів з “припинення кримінальних правопорушень”. Проте, персональні дані, зібрані й використовувані в цілях, що не підпадають під діяльність поліції, наприклад, в адміністративних цілях, підлягають загальним нормам захисту даних.

Сфера застосування та визначення понять

Ці принципи покликані врегульовувати всі критичні моменти, коли виникає питання про захист даних при збиранні, зберіганні, використані й передачі персональних даних. Всі ці дані певним чином пов’язані з “цілями поліції”. Останній термін витлумачується з точки зору інтересів суспільства, про які йшлося у параграфі 5 Преамбули. Зауважимо, що в цьому документі цей термін в подальшому уточнюватиметься по тексту, що забезпечуватиме різне витлумачення завдань поліції по боротьбі з кримінальними правопорушеннями і завдань, які вона повинна виконувати по їх запобіганню й підтриманню громадського порядку.

Рекомендації стосуються просто “органів поліції”. Слід пам’ятати, що відповідно до конкретної законодавчої системи можуть співіснувати різні поліцейські органи. Можливо, не завжди легко їх розрізнити з точки зору розподілу функцій. Проте, незважаючи на номенклатуру, ці принципи повинні застосовуватись до будь-якого органу з функціями поліції, що займаються збиранням, зберіганням, використанням та передачею персональних даних у цілях, викладених у параграфі 3 цього розділу.

Рекомендації торкаються в першу чергу автоматизованої обробки персональних даних; термін “персональні дані” визначається в попередніх рекомендаціях Ради Європи у сфері захисту даних. Варто нагадати, що незалежно від того, вважається особа ідентифікованою чи ні, вона мусить визначатися ідентифікованою, враховуючи вишукані методи ідентифікації, наприклад, техніку відбитків пальців, систему розпізнавання голосів, службу банків даних тощо.

“Відповідальний орган”, згадуваний у цьому розділі, є в дійсності, за термінологією Конвенції, контролером файлів. Цей орган має нести максимальну відповідальність за файли. У Принципі 1.4 буде з’ясовано, що назва відповідального органу для конкретного файла повинна бути повідомлена наглядовому органу.

Хоча цей документ присвячується автоматизованій обробці персональних даних, відомо, що деяка частина держав-членів Ради Європи все ще більшою мірою покладається на ручну обробку даних. В інших країнах, де комп’ютеризація поліції поставлена добре, дані, що зберігаються в комп’ютерах, можуть бути зрозумілими лише тоді, якщо робиться посилання на ручні файли. Тому не бажано вилучати ручні файли, з цієї причини цим документом визнається, що держави-члени вільні поширювати ці принципи на дані, утримувані в ручній формі. Параграф 38, як буде видно далі, забезпечує вказівки щодо того, як держави-члени повинні трактувати питання ручного утримання даних.

З часом, все більше даних, утримуваних сьогодні в ручній формі, будуть автоматизовані, а тому принципи, що містяться у цьому документі, будуть поширюватися й на них. Проте не слід допускати, щоб держава-член навмисно обходила гарантії, викладені в цьому документі, перетворюючи персональні дані з автоматизованих файлів на ручні файли. Проте, слід визнати, що визначити, чи мав місце навмисний обхід, буває важко, якщо дані знищуються згідно з Принципом 7, а роздруковані дані залишаються.

Згідно з параграфом 2 Статті 3 Конвенції про захист даних цей документ також визнає, що держави-члени мають можливість застосовувати ці принципи до юридичних осіб.

Нарешті, стосовно питань державної безпеки, які пояснювальна записка до Конвенції про захист даних подає як “захист державного суверенітету від внутрішньої чи зовнішньої загрози, включаючи захист міжнародних відносин держави”, бажано визнавати право держав-членів поширити деякі з гарантій, передбачених цим документом, на сферу держаної безпеки, де їх використання можливе й принагідне.

У контексті питання державної безпеки та юридичних осіб слід пам’ятати, що принципи, викладені в цій Рекомендації, були визнані розробниками як мінімальні гарантії і що державам-членам залишено право посилювати заходи захисту.

Принцип 1 – Контроль та повідомлення

Органи захисту даних або уповноважені виконують головну функцію за внутрішнім законодавством у захисті даних. Там, де такі органи існують, їм мають бути передані функції, викладені в цих Рекомендаціях. Не бажано створювати ще один окремий орган у цілях цієї Рекомендації. Проте, будь-який новий орган, що створюється, повинен бути незалежним від контролю поліції; суттєву якісну можливість містять Рекомендації, уповноважуючи на певних етапах цей орган приймати рішення, оцінюючи межі обмеження діяльності поліції щодо використання персональних даних.

Конституційна структура певних держав-членів може вимагати створення кількох незалежних наглядових органів, де органи захисту даних чи уповноваженні ще не існують. Орган не обов’язково має бути колегіальним. Допустимо, що якась особа виконуватиме функцію “забезпечення поваги до принципів, викладених у цих Рекомендаціях”. Проте, віддаючи належне важливості цієї ролі, бажано, щоб наглядовий орган, незалежно від його форми, мав достатньо ресурсів, щоб бути ефективним.

Слід також наголосити, що відсутність загального законодавства про захист даних не є перешкодою для створення незалежного наглядового органу у сфері поліції. Принципи, викладені в Рекомендаціях, адресовано всім державам-членам і можуть використовуватись країнами, яким ще належить прийняти загальні норми із захисту даних.

Цією преамбулою визнається, що, крім комп’ютерів, інші нові технічні засоби обробки даних також підносять ефективність роботи поліції, наприклад, системи розпізнавання голосів, розпізнані машиною ідентифікаційні картки, технології стеження з використання комп’ютера, електронні системи стеження. Проте, враховуючи можливість їх неправильного використання, важливо, щоб їх запровадження й використання супроводжувалися усвідомленням їх впливу на індивіда. З цією метою Принцип 1.2 рекомендує зважливо підходити до їх запровадження, не вступаючи в конфлікт духом існуючого законодавства із захисту даних. Крім того, потрібні будуть широкі обговорення доцільності впровадження нових технологій, які можуть становити загрозу приватності, якщо це не буде взято до уваги законодавцями під час прийняття норм захисту даних.

У зв’язку з цим незалежний наглядовий орган покликаний виконувати важливу роль. Згідно з Принципом 1.3 він має бути посилений у повноваженнях, щоб здійснювати моніторинг за клопотанням відповідального органу, коли останній має намір запроваджувати методи автоматизованої обробки даних, що можуть породити проблеми із застосуванням цих рекомендацій. Принцип 1.3 не передбачає застосування права вето на запровадження таких методів. Проте, вони дозволяють наглядовому органові перевіряти запропоновані методи, щоб переконатися, що ті не обходять принципи, наприклад, що стосуються передачі даних (Принцип 5). Він може порадити відповідальному органові вжити певних заходів, щоб забезпечити дотримання принципів Рекомендацій.

У цілях цього документа “файли поліції” – це всі структуровані/упорядковані персональні дані, які відповідають вимогам служб поліції з точки зору запобігання чи припинення кримінальних правопорушень або забезпечення громадського порядку. Файли поліції, як це визначається, сприяють поліції отримувати інформацію, що стосується ідентифікованих чи неідентифікованих осіб. Принцип 1.4 зобов’язує поліцію або, можливо, якийсь інший орган, призначений національним законодавством, повідомити про свої автоматизовані файли наглядовий орган і охарактеризувати певні деталі, що стосуються кожного автоматизованого файла.

Зауважимо, що це загальна вимога повідомлення. Жодних винятків не робиться щодо файлів, що стосуються винятково припинення кримінальних правопорушень. Як зазначалося раніше, Рекомендації призначені для вироблення спеціальних правил для типових завдань поліції, єдиним винятком з яких, коли це необхідно, є врахування особливостей вимог поліції в контексті “припинення кримінальних правопорушень”.

Незважаючи на те, що правила повідомлення обмежуються автоматизованими поліцейськими файлами, може бути випадок, що якісь держави-члени скористаються їх правом поширити принципи, викладені в цьому документі, на ручні файли.

Якщо таке станеться, держава-член може зобов’язати поліцію зробити позначення кожного типу утримуваного файла, контролера файла, його ціль, характер даних, що містяться в ньому, та осіб, яким ці дані повідомляються. Таке загальне позначення повинно повідомлятися наглядовому органу. Як альтернатива, потребу в повідомлені кожного опису можна уникнути, якщо кожен підрозділ поліції зобов’яжуть забезпечити, щоб його ручні файли узгоджувалися з відповідним описом, розробленим на центральному рівні. Якщо поліцейський підрозділ не дотримується цього загального опису, він буде зобов’язаний зробити власний опис і повідомити його наглядовому органу.

Можливі, звичайно, й інші шляхи поширення цих принципів на ручні файли.

Другий підпараграф Принципу 1.4 стосується питання тимчасових файлів, які були заведені під час окремого розслідування.

Позначення кожного тимчасового файла породжує неприйнятну бюрократію. Проте такі файли не повинні уникати певного виду повідомлення. Національне законодавство може передбачити обставини, за яких на них має бути звернена увага наглядового органу. Можливо, що внутрішнє право вимагатиме лише повідомлення про існування таких файлів або “загального” повідомлення тимчасових файлів певного типу, що дозволить наглядовому органові перевіряти їх, з тим щоб переконатися, що вони відповідають принципам захисту даних.

Як альтернатива, у разі відсутності відповідних положень у внутрішньому законодавстві наглядовий орган разом з відповідальним органом, зазначеним раніше, може виробити керівні принципи для повідомлення тимчасових файлів. Наприклад, з діалогу між наглядовим органом та відповідальною організацією з’ясовується, що такі файли повинні повідомлятися після того, як вони вже проіснували прийнятний час або, якщо можна передбачати, що проіснують протягом прийнятного часу. Буде знайдено й інші критерії для повідомлення.

Файли, заведенні в цілях окремого розслідування, що швидко надається, не потребують повідомлення.

Принцип 2 – Збір даних

Принцип 2.1 виключає необмежений, нерозбірливий збір даних поліцією. Він окреслює якісний і кількісний підхода до Статті 5(c) Конвенції про захист даних, у якій зазначається, що персональні дані мають бути адекватними, відповідними і не надмірними стосовно цілей, задля яких зберігаються. Враховуючи, що стаття 9(a) Конвенції дозволяє обмеження цього принципу з огляду на “припинення кримінальних правопорушень”, Принцип 2.1 цих Рекомендацій намагається окреслити межі цих винятків, обмежуючи збирання персональних даних такою мірою, яка необхідна для запобігання реальній небезпеці або припинення певного кримінального правопорушення, якщо тільки внутрішній закон чітко не дозволяє ширші повноваження поліції у зборі інформації. Під “реальною небезпекою” слід розуміти не таку, що пов’язана з особливим кримінальним порушенням, а таку, що включає будь-які обставини, за яких виникає обґрунтована підозра, що серйозні кримінальні правопорушення скоєні чи могли б бути скоєними до зняття непідтверджених теоретичних припущень. В якості прикладу можна навести таке: обґрунтована підозра, що невизначені наркотики повинні нелегально завезти в країну через порт на неідентифікованій приватній яхті, виправдовуватиме збір даних про всі такі яхти, що обслуговуються цим портом, але не про всі яхти, їх власників та пасажирів, що використовують всі порти цієї країни.

Принцип 2.2 стосується збирання й зберігання даних без відома суб’єкта даних і намагається запропонувати регулюючий механізм на випадок, коли дані, зібрані в такий спосіб, вирішено зберегти, але, якщо це не шкодитиме поліції в досягненні поставлених цілей, особу інформують про наявність даних на неї. Звичайно, ця процедура не потрібна, якщо поліція вирішила знищити дані, зібрані на особу без її відома.

Слід погодитись, що принцип 2.2 може виявитись складним для втілення, якщо йдеться про вуличні відео чи подібні засоби масового стеження, що надають інформацію про велику кількість людей. З цієї причини цей принцип рекомендує інформувати тих осіб, що підлягали негласному стеженню, про те, що дані ці ще утримуються на них “якщо доцільно”. Поліція сама повинна прийняти таке рішення.

Сподіваємось, що держави-члени оцінять цей принцип як корисний, розглядаючи сучасний прецедент Європейської Комісії з прав людини, в якому у контексті Статті 8 Європейської Конвенції з прав людини визнано, що збирання й зберігання даних про особу без повідомлення їй про це може зачіпати питання захисту даних (звернення № 8170/78, X проти Австрії; звернення № 9248/81, Лідер проти Швеції).

У той час, як Принцип 2.2 робить наголос на збереженні персональних даних, зібраних без відома суб’єкта даних негласними засобами чи нетаємними (наприклад, шляхом постановки питань сусідам суб’єкта даних), Принцип 2.3 зосереджує увагу на збиранні даних технічними засобами стеження або іншими автоматизованими засобами. Спеціальні положення національного законодавства повинні врегульовувати збирання даних такими методами. Так, слід пам’ятати про судові прецеденти Європейського Суду з прав людини, коли вирішується питання щодо прослуховування телефонних розмов. Рішення у справі Мелоуні показує, що така форма технічного стеження може застосовуватися санкціоновано з урахуванням доступних законних правил, які достатньою мірою визначають межі й спосіб застосування повноважень “на розсуд” покладених на органи влади, і супроводжуються адекватними гарантіями захисту від зловживання.

Правоохоронні органи діють у рамках встановлених законом, і їх діяльність по збиранню даних регламентується так само. Відповідно, положення внутрішнього законодавства, які повинні брати за їх мінімальну основу положення Конвенції про захист прав людини та основних свобод (1950 р.), повинні поважатись. У зв’язку з цим варто враховувати також судові прецеденти Європейської Комісії та Європейського Суду з прав людини у питаннях арешту або утримання під арештом для допиту, обшуку та конфіскації, методів допиту, взяття проб тіла, відбитків пальців та фотографування тощо. Зрозуміло, що відповідні внутрішні законодавства повинні відповідати положенням Конвенції як вони розтлумачені Європейським Судом з прав людини.

Принцип 2.4 розглядає питання “вразливих” даних і відображає рекомендацію Статті 6 Конвенції із захисту даних про обмеження збирання й зберігання особливої категорії даних. Це може бути випадок, коли збирання певних “вразливих” даних необхідно в цілях, викладених у Принципі 2.1. Проте, в кожному разі збирання таких даних не повинно здійснюватися просто для того, щоб дозволити поліції скласти файл на якусь групу меншин, чиї звички чи поведінка відповідають закону. Збирання таких даних повинно здійснюватися лише з дозволу, якщо це “абсолютно необхідно в цілях конкретного розслідування”. Вираз “конкретне розслідування” повинен розглядатися як загальне обмеження; таке розслідування повинно ґрунтуватися на міцній законодавчій основі, щоб переконати в тому, що серйозне кримінальне правопорушення було вчинено чи могло статись. Збирання “вразливих” даних за таких обставин повинно бути “абсолютно необхідним” для потреб таких розслідувань.

Посилання на сексуальну поведінку (як підставу для збирання даних) не застосовується щодо вже скоєних правопорушень.

Принцип 3 – Зберігання даних

Персональні дані, після того як були зібрані, підлягають рішенню щодо їх зберігання в поліцейських файлах. Принцип 3.1 звертається до вимог точності і обмежень у зберіганні. Дані, що зберігаються, мають бути точними й обмеженими такою мірою, якою це необхідно, щоб забезпечити виконання поліцією її законних завдань. Принцип 3.1 визначає, що, крім національного законодавства, джерелом законної діяльності поліції, яке узаконює збирання даних, може бути міжнародне право, яке у цілях цих Рекомендацій взято до уваги, щоб включити міжнародне співробітництво в межах Інтерполу (наприклад, міжнародні правові угоди про співробітництво між силами національних поліцій).

Цей принцип важливий з огляду на те, що звертає увагу на факт, коли включення персональних даних до поліцейського файла може спричинитися до поліцейського запису, а нерозбірливе зберігання даних може зашкодити правам і свободам особи. Поліція також має бути зацікавленою в тому, щоб мати в розпорядженні лише точні й надійні дані.

Слід відзначити, що принцип 3 в цілому є загальною вимогою, що стосується всіх типів даних, зібраних у цілях поліції, як позначалося вище.

Принцип 3.2 спрямований на застосування системи класифікації даних. Гадаємо, слід розрізняти підтверджені й непідтверджені дані, що включають оцінку людської поведінки, факти й погляди на них, надійну інформацію (і різні відтінки цього) і здогади; справжню причину віри в те, що інформація точна, і безпідставну віру в її точність.

Дані, зібрані й збереженні поліцією для адміністративних цілей (наприклад, інформація про страхування від пожежі, втрати майна тощо), також є предметом загальних принципів зберігання даних. Принцип 3.3 рекомендує, щоб такі дані зберігалися окремо від тих даних, що зібрані в цілях поліції згідно з цим документом, якщо вирішено зберігати їх необмежено. Принципово неправильно було б поширювати на них спеціальний режим поліцейських даних із запровадженням особливого підходу до захисту даних у сфері поліції.

Проте не завжди буває можливим забезпечити чіткий поділ даних на дві категорії. І все ж, у такому разі держави-члени повинні вивчити всі підходи, щоб уникнути змішування даних, забезпечуючи, щоб адміністративні дані залишалися об’єктом загальних правил захисту даних.

Принцип 4 – Використання даних поліцією

Принцип 4 формулює заключне положення: персональні дані, зібрані з метою запобігання й припинення кримінальних правопорушень, або для підтримання громадського порядку (“поліцейські цілі”), повинні використовуватись лише в цих цілях. Проте, абсолютний характер цього правила визначається частково Принципом 5.

Принцип 5 – Передача даних

Принцип 5 побудовано так, щоб врегульовувати різні форми передачі даних, що може на законних підставах мати місце, а також забезпечувати принципи, що торкаються всіх передбачуваних передач.

Передача даних у поліцейській сфері обумовлюється наявністю у поліцейського органу, який одержує дані, правомірного інтересу на це, наприклад, як необхідна одержувачу для запобігання чи боротьби з кримінальними правопорушеннями або підтримання громадського порядку. Встановлюється, що поліцейський підрозділ, що запитує інформацію в іншого поліцейського підрозділу, може повідомити певні дані, щоб його запит про інформацію було виконано, причому обидві сторони повинні виконувати вимогу щодо законного інтересу, викладену в Принципі 5.1.

При передачі за межі поліцейського сектору умови, що визначають передачу, більш суворі: оскільки комунікація може бути і не в цілях поліції у прямому розумінні. Наголошується винятковий характер обставин, викладених у Принципах 5.2 та 5.3, за яких дозволяється передавати дані. Буде визначено, що обставини (а) та (б) у Принципах 5.2 (ii) та 5.3 (ii) спеціально позначаються як “виняткові”.

Публічними установами, яких стосується Принцип 5.2, можуть бути, наприклад, органи соціального забезпечення, органи внутрішньої перевірки за сплатою річних податків, імміграційного контролю, органи митної служби тощо.

Загальні умови передачі даних таким органам, визначені Принципом 5.2 (i), підпараграфи (а) та (б). Зазначимо, що Принцип 5.2 (i, а) розглядає можливість наглядового органу санкціонувати передачу даних. Пам’ятаючи про цю функцію, підкреслену в Принципі 1, наголошуємо на необхідності незалежності наглядового органу від поліцейського сектору.

“Чітке законне санкціонування”, про яке йдеться в Принципі 5.2 (i, а) може забезпечуватися: 1) суддею; 2) членом магістрату; 3) посадовою особою.

Взаємодопомога між органами поліції і публічними установами, зазначеними вище, також можлива за відсутності обставин, викладених у Принципі 5.2 (i, а). Принцип 5.2 (i, б) дозволятиме, наприклад, органам соціального захисту, що розслідують порушення у секторі соціального захисту, мати доступ до відповідних даних поліції, якщо дані є суттєвими для його розслідування. Визнано, що публічні установи, про які йшлося у параграфі 59, займаються діяльністю, подібною якимось чином до поліцейської, а тому інформація, утримувана поліцією, може бути корисною для їх діяльності. Поняття сумісності, згадуване в Принципі 5.2 (i, б),

відображає Статтю 5(б) Конвенції про захист даних. Отже, дані можуть передаватися для спорідненої діяльності. “Законні обов’язки” поліції слід трактувати відповідно до внутрішнього законодавства.

Принцип 5.2 (ii) викладає дві додаткові обставини, що виправдовують повідомлення; нагадаємо, що дозволятимуть вони повідомлення лише як “виняткове”. Для ілюстрації положення наведемо приклад, коли установа з соціального захисту, зіткнувшись з вимогою мігранта про пільги, повинна перевірити легальний статус останнього в цій країні, звернувшись до поліцейського файлу. Це буде і на користь заявника. Зазначимо, що небезпека, про яку йдеться в (б), повинна буди серйозною і вже навислою. Було вирішено кваліфікувати небезпеку в такий спосіб, як і в Принципі 5.2 (ii), якщо стосується лише виняткових випадків допущення комунікації. Якщо ж існує серйозна, але не термінова загроза, то комунікація має здійснюватися згідно з положеннями Принципу 5.2 (ii, а).

Інколи для поліції буває необхідним передати дані приватним організаціям, хоча й не того рівня, що розглядається у випадку взаємодопомоги між органами поліції та іншими публічними установами. Інколи поліція робить доступними конфіденційні дані про відомих шахраїв, що обкрадають крамниці та банки, чи інформації про викрадені кредитні картки та чеки. Знов-таки, Принцип 5.3 розглядає їх як виняткові випадки, вимагаючи чітких правових зобов’язань чи санкцій (наприклад, згоди члена магістрату) або згоди наглядового органу. За відсутності цих факторів Принцип 5.3 повторює ці ж умови, що викладені в Принципі 5.2 (ii).

Слід мати на увазі, що положення Принципі 5.2 та 5.3 стосуються поширення чи повідомлення через радіомовлення публічним установам чи приватним особам ідентифікуючих знімків чи фотографій підозрюваних осіб, що отримані з автоматизованих обробок даних.

Принцип 5.4 торкається міжнародної передачі поліцейських даних у суворому розумінні між органами поліції. Звернення до міжнародного права передбачає не лише міжнародні угоди про взаємодопомогу в кримінальних справах, але й співробітництво в межах Інтерполу. Крім того, цей принцип враховує наявність (або намір) угод між сусідніми державами, підписаний з метою поліпшення транскордонної передачі даних між поліцейськими відділами.

Стосовно терміну “поліцейські органи”, погоджено, що у деяких державах-членах певні види поліцейської роботи можуть виконуватися організаціями, які не є в суворому розумінні “поліцейськими органами”. Отже, може бути прецедент, що певні функції, які мисляться як такі, що є в компетенції поліції, в окремих державах-членах можуть бути фактично перекладені на неполіцейські установи в інших державах-членах.

У цілях Принципу 5.4 термін “поліцейські органи” слід розуміти в широкому смислі. Питання повинно ставитись лише таким чином: орган виконує функцію, пов’язану з припиненням кримінальних правопорушень чи досягненням громадського порядку. Нарешті, Принцип 5.4 не слід витлумачувати як такий, що виключає можливість передачі даних іноземним юридичним органам де такі органи виконують функції, пов’язані із запобіганням і припиненням кримінальних правопорушень. Вимоги, викладені в Принципі 5.4, мають поважатись.

Міжнародний обмін персональними даними між поліцейськими установами повинен відбуватися лише за умов, викладених або в (а) чи (б). Принцип 5.4 буде корисним, якщо держава-одержувач не є членом Інтерполу, або якщо договору, що санкціонує передачу даних реципієнту, не існує.

Текст Принципу 5.4 відображає до певної міри положення Статті 12 Конвенції про захист даних, яка розглядає питання транскордонних потоків даних. Речення “і передбачає, щоб внутрішні закони захисту особи не порушувались” доповнює концепцію “еквівалентного захисту”. Отже, орган, що надсилає, сам повинен задовольняти рівень захисту даних для поліції, що існує в державі, яка одержує. При вирішенні питання, чи повинен наглядовий орган ставити умови щодо використання даних в державі, яка їх отримує, слід розуміти, що ці умови слід поважати. Обидва Принципи 5.4 (а) та (б) підпадають під застереження.

Принцип 5.5 зв’язує низку правил, що врегульовують різні форми повідомлення даних, про які йшлося вище.

Звертаючись до правил, які регулюють передачу даних, розробники керувалися певною мірою положеннями, викладеними в “Правилах про співробітництво поліції та внутрішній контроль за архівами Інтерполу”. Крім них відображено положення “Європейської Конвенції про взаємодопомогу у кримінальних справах” від 20 квітня 1959 року.

Критерії, сформульовані в Принципі 5.5, спрямовані на забезпечення того, щоб повідомлення даних здійснювалося на законних підставах. Нагадаємо, що Принцип 5.1 зобов’язує орган поліції, що просить дані у іншого органу поліції в межах поліцейського сектору, мати законні підстави для отримання цих даних. Проте, Принцип 5.5 (i) розглядає як внутрішній, так і зовнішній обмін даними, що стали предметом правомірних вимог.

Встановлюється, що внутрішнє право чи положення міжнародних угод можуть вирішувати питання про виправданість запиту.

Принцип 5.5 (ii) не абсолютний за своєю природою. Умови, сформульовані в ньому – “наскільки це можливо” мають задовольнятись. Наприклад, відомо, що в деяких країнах судові рішення не завжди надсилаються до поліції.

Як зазначалося, і в інтересах поліції, і в інтересах особи дані повинні бути точними.

Принцип 5.5 (ii) зважає також на те, що в різних країнах існують різні періоди моніторингу. З цієї причини здійснення перевірки якості даних дозволяється до моменту їх передачі.

Принцип 5.5 (iii) дозволяє використання даних винятково в цілях, що відрізняються від цілей доведення правомірності першого запиту про повідомлення. Важливо, щоб орган який повідомляє було поінформовано про використання даних. Слід пам’ятати, що різні цілі повинні стосуватися одного чи більше факторів, що розглядаються в Принципах 5.2 – 5.4.

Принципи 5.5 (ii) не застосовуються до передачі в середині поліцейського сектору. Правила, викладені в Принципах 4.1 та 5.1, застосовуються в такому випадку.

У той час, коли Принцип 2 формулює загальне положення про збирання даних поліцією, Принцип 5.6 торкається особливої ситуації, коли поліція в пошуках інформації може підключати свої файли до файлів, що утримуються для відмінних цілей, наприклад, органів соціального захисту, списки пасажирів, що зберігаються авіалініями, файли членства в профспілках тощо. Отже, може вестись пошук таких файлів, які б надавали чіткий опис типу правопорушення або осіб, які, можливо, причетні до такого правопорушення.

Легітимність такої практики залежить від гарантованості підстави санкції, зазначеної в (a) чи (б). “Чіткі правові забезпечення”, на які є посилання в Принципі 5.6 (б), повинні зазначити умови, за яких може відбутися підключення (поєднання) файлів.

Можливість поліції, що має прямий комп’ютеризований доступ до файлів, що робиться різними органами поліції чи іншими органами, обговорюється в заключному під-параграфі Принципу 5.6. Прямий доступ за таких обставин повинен узгоджуватися з внутрішнім законодавством, яке має відображати відповідно основі принципи цієї Рекомендації.

Принцип 6 – Доступність для громадськості, право доступу до файлів поліції, право на виправлення і право на апеляцію

Вимога прозорості для існуючих поліцейських файлів з огляду на права осіб стосовно поліцейських файлів є особливо важливою. Принцип 6.1 покладає завдання з прозорості на наглядовий орган, хоча держави-члени, без сумніву, знайдуть додаткові шляхи втілення цієї вимоги.

Вимога прозорості повинна стосуватися в принципі всіх автоматизованих файлів. Проте зрозуміло, що обсяг інформації, що може бути надана для поліцейських файлів, буде залежати від особливих обставин.

Наприклад, більш загальний опис слід надавати тимчасовому файла, що стосується делікатного розслідування, яке проводиться.

Особа в першу чергу повинна мати право направляти звернення про доступ до поліцейського файла контролерові цього файла. Це право принаймні повинно задовольнятися через посередницький чи наглядовий орган. Внутрішнє законодавство повинне вживати відповідні заходи, щоб існувало таке право. Крім того, Принцип 6.2 гарантує доступ суб’єкта даних у розумних проміжках часу і без невиправданої затримки.

У принципі, звернення про доступ до даних не повинно реєструватися, оскільки це може обмежувати реалізацію права. Проте, якщо держава-член має систему реєстрації, слід потурбуватися, щоб реєстрація утримувалася окремо від кримінальних файлів, утримуваних поліцією. Слід також подумати про знищення реєстру через розумний проміжок часу.

У зв’язку з тим, що дані виявляються не точними в результаті застосування права доступу або вважаються неточними, невідповідними чи надмірними в наслідок застосування інших принципів, Принцип 6.3 передбачає, що поліція дбатиме про приведення відповідного файла в належний порядок. Це може бути зроблено через знищення неточних даних чи виправлення інформації, щоб вона відповідала істинній ситуації. Альтернативою стиранню, як це передбачено Принципом 6.3, є зберігання даних у файлі, але з поміткою про їх дійсний стан. Це може стосуватися заяв, зроблених свідками, які виявились неточними. Доцільніше буде не усувати таку заяву з файла, а залишити її, додавши правильну версію подій.

Другий підпараграф принципу 6.3 викладає графік знищення чи виправлення даних. Зауважимо, що ці заходи застереження стосуються не самого файлу, а повинні застосовуватися до кожного документу, залученого до файлу.

Досвід принаймні в одній державі-члені показав, що в принципі можливий санкціонований доступ у переважній більшості випадків. Принцип 6.4 визначає, що у праві доступу (а отже й праві на виправлення та знищення) може бути й відмовлено у викладених випадках.

Відзначимо, що обмеження в інтересах суб’єкта даних прав і свобод інших було взято зі Статті 9, підпараграф 2(б) Конвенції про захист даних. У контексті поліцейського сектору це формулювання повинно поширюватися на захист свідчень чи поліцейських інформаторів.

Альтернативне виправдання обмеженого доступу – “обов’язкового для виконання законного завдання поліцією” – не має чіткого відбиття у Статті 9 зазначеної Конвенції. Проте є переконання, що в контексті обмежень права на доступ, застереження Конвенції для “припинення кримінальних правопорушень” є кращим формулюванням.

Особа може мати необхідність в отриманні копії її поліцейського файла, наприклад, у зв’язку з наймом на роботу. Причому, не в її інтересах буде отримання письмової копії чи констатації про те, що міститься у файлі. В такому разі внутрішнє законодавство може санкціонувати усну передачу змісту файла.

Принципи 6.5 та 6.6 формулює певні процедурні гарантії у випадку відмови чи обмеження права доступу, виправлення чи знищення. По-перше, відмова чи обмеження вмотивовуються письмово. Важливо показати, що обов’язок покладений на поліцію принципом 6.4 підпорядковувати права суб’єкта даних вищим інтересам, викладеним тут, виконується.

Буде зауважено, що зазначення причин може не вимагатися лише з тих же причин, що виправдовують відмову чи обмеження прав доступу, виправлення чи стирання. Об’єкт даних інформується про його право на апеляцію у зв’язку з відмовою в доступі. Це право має формулюватися у вигляді обґрунтованого рішення, передбаченого положенням 6.5. Якщо причини відмови не зазначаються, бо поліція переслідує вищі інтереси, однак особі повідомляють, як вона може оскаржити це рішення.

Принцип 6.6 розроблено з урахуванням практики різних держав-членів у наданні права доступу. У деяких країнах можуть трапитися випадки, коли особа не матиме прямого права доступу до файла поліції і буде зобов’язана домагатися доступу через вищій наглядовий орган.

Згадуваний “інший незалежний орган” означає, що в деяких країнах суд чи трибунал може розглядати апеляції, а не вищій наглядовий орган. Але незалежно від цього суб’єкт даних користуватиметься правом звернутися до суду чи трибуналу, щоб домогтися виправлення, доповнення файла тощо, якщо йому у цьому було відмовлено.

Внутрішнє законодавство визначає посередницькі органи чи наглядовий орган для перевірки поліцейського файла, з приводу якого виникла суперечка. Може статися, що наглядовий орган не буде зобов’язаний повідомляти дані особі, якщо навіть і не має підстав для відмови у доступі. Суб’єктові даних просто повідомляють, що перевірку поліцейського файлу зроблено і що файл - в порядку. В іншому разі, контролюючий орган може прийняти рішення про повідомлення даних, що містяться у файлі, суб’єкту даних.

Принцип 7 – Тривалість зберігання і поновлення даних

Важливо, щоб робилися періодичні перегляди поліцейських файлів з тим, щоб вилучити з них зайву чи неточну інформацію, а також поновити її. Принцип 7.1 перераховує чинники, які слід мати на увазі, коли вирішується питання, чи продовжене зберігання даних залишатиметься необхідними для запобігання чи припинення злочину або підтримання громадського порядку.

Принцип 7.2 містить побажання, щоб якість даних перевірялась регулярно відповідно до встановлених правил, і щоб вони консервувалися також на підставі, визначеній правилами. Застосування цього принципу поліпшить виконання завдань, покладених на поліцію Принципом 5.5, підпараграф (ii).

Внутрішнє право може санкціонувати заходи по виробленню таких правил. В іншому разі, правила ці могли б формулюватися самім наглядовим органом в консультаціях з поліцією. Якщо поліція сама виробляє правила, вона повинна консультуватися з наглядовим органом стосовно їх змісту та застосування.

Зрозуміло, що поліцейські дані становлять цінність з точки зору дослідницьких та статистичних даних. Внутрішнє законодавство про архіви забезпечує шляхи вирішення всіх проблем, які виникають у цьому зв’язку. Якщо необхідно, мають робитися посилання на положення Рекомендації №R(83)10 про захист персональних даних, використовуваних у наукових та статистичних цілях.

Принцип 8 – Безпека даних

Принцип 8 відображає вимоги фізичної безпеки та конфіденційності. Відповідальний орган, зазначений вище, повинен дбати, щоб лише уповноважений персонал мав доступ до терміналів і щоб повідомлення даних виконувалося відповідно до вимог, які, за Принципом 5, є законними. З цією метою відповідальний орган міг би завести журнал, в якому записувалась би інформація, що розглядається в принципі 5.5 (i).

<META> – Украинская поисковая система
http://www.internetrights.org.ua/books/do/2_3_3.doc

ШАНОВНІ ЧИТАЧІ !

Науково-дослідний центр правової інформатики АПрН (НДЦПІ) України разом з Апаратом Верховної Ради України, Верховним Судом України, МВС України та іншими органами державної влади і місцевого самоврядування здійснює планові науково-дослідні роботи та розробки за господарськими договорами й зовнішньоекономічними контрактами правових проблем щодо сфери інформації, інформатики та інформатизації, які спрямовані на побудову в Україні е-середовища.

За результатами робіт за 2001–2005 роки НДЦПІ України на базі аналізу й узагальнень, систематизації міжнародної та вітчизняної практики, оцінки тенденцій, що намітилися, розробив та видав ряд матеріалів, які мають теоретичне та практичне значення у зв’язку з проблемами нормативного та організаційного упорядкування суспільних інформаційних відносин щодо політичної, економічної, фінансової, банківської, технологічної, екологічної, медичної, освітянської, культурної, виробничої, інформаційної, правоохоронної та іншої діяльності.

Результати досліджень призначені для науковців і практиків для подальшого опрацювання загальних і спеціальних питань інформаційного законодавства та підтримки інформаційної безпеки держави. Вони будуть корисними також для студентів, аспірантів юридичних та інших навчальних закладів при вивченні проблем в галузі інформації, інформатики, інформатизації та інформаційного права, а також при розробці науково-практичних посібників та рекомендацій щодо боротьби з комп’ютерними правопорушеннями в умовах формування е-середовища та просування країни до інформаційного суспільства.

Перелік результатів науково-дослідної роботи та видань Науково-дослідного центру правової інформатики Академії правових наук України у 2001–2005 роках

№ п/п	Автор (колектив авторів), найменування, назва джерела	Проблематика дослідження	Тип видання
1	Правова інформатика / Швець М.Я., Брижко В.М, Калюжний Р.А., Саницький В.А., Клімашевська Ю.А., Задорожня Л.М. та ін. ; за ред. Швеця М.Я. та Калюжного Р.А. – К.: ІВА, 2003	Системна інформаизація законотворчої, правоохоронної, судочинної діяльності в Україні	Монографія, 168 с.
2	Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики / Калюжний Р.А., Швець М.Я., Шамрай В.О. та ін. ; за ред. Калюжного Р.А., Шамрая В.О. Академія державної податкової служби України. – К.: КВІЦ, 2002	Організаційно-правові питання інформаційного забезпечення управлінської діяльності	Монографія, 296 с.
3	Інформатизація, право, управління: організаційно-правові питання / Калюжний Р.А., Крупчан О.Д., Гавловський В.Д., Гуцалюк М.В., Цимбалюк В.С., Швець М.Я. ; за ред. Швеця М.Я., Крупчана О.Д. – К.: Академія правових наук України, 2002	Про інтегровану систему інформаційно-аналітичного забезпечення	Монографія, 191 с.
4	е–будущее и информационное право / В.М. Брыжко, А.А. Орехов и др. ; под. ред. Калюжного Р.А., Швеца Н.Я. – К: “Интеграл”, 2002	Стан та перспективи технологічного та правового майбутнього	Монографія, 264 с.
5	Інформаційне суспільство. Дефініції… / В.М. Брижко, А.А.Орєхов та ін. ; за ред. М.Я. Швеця, Р.А. Калюжного. – К: “Інтеграл”, 2002	Терміни та поняття у сфері інформатизації	Довідник-посібник, 220 с.

6	Інформаційно-пошукова система “Термінологія законодавства” / Швець М.Я., Севастьянов В.Ф., Дорогих С.О. та ін. – К.: НДЦПІ АПрН України, 2002	Про ІПС	Посібник, 25 с.
7	Інформаційно-пошукова система “Законодавство” / Севастьянов В., Швець М., Слюсар В., Дорогих С. – К.: ІВА, 2002	Про ІПС	Посібник, 103 с.
8	Комп’ютерна злочинність / Романюк Б.В., Цимбалюк В.С., Гавловський В.Д. та ін. – К.: АТІКА, 2002	Щодо інформаційної безпеки	Посібник, 240 с.
9	Основи захисту інформації від несанкціонованого доступу / Ільніцький А.Ю., Саницький В.А., Шорошев В.В., Близнюк І.Л. – К.: Національна академія внутрішніх справ України, 2002	Про концептуальні основи захисту інформації	Посібник, 208 с.
10	Вступ до інформаційної культури та інформаційного права / Калюжний Р.А, Швець М.Я. Цимбалюк В.С. та ін. – К.: ІВА, 2003	Щодо теорії інформаційної культури	Монографія, 240 с.
11	Правовий механізм захисту персональних даних. / В.М. Брижко ; за ред. Швеця М.Я., Калюжного Р.А. – К.: Парламентське видавництво, 2003	Про упорядкування інформаційних відносин в сфері персональних даних	Монографія, 124 с.
12	Інформаційно-пошукова система “Законодавство”. – К: НДЦПІ АПрН України, 2003	База даних на CD, понад 120 тис. документів	
13	Інформаційно-пошукова система “Термінологія законодавства”. – К: НДЦПІ АПрН України, 2003	База даних на CD, понад 16 тис. термінів	
14	Інформаційно-пошукова система “Дисертаційні дослідження”. – К: НДЦПІ АПрН України, 2003	База даних на CD	
15	Автоматизоване робоче місце “Кримінолога-аналітика”. – К: НДЦПІ АПрН України, 2003	База даних на CD	
Видання 2004 року			
16	Науково-дослідний центр правової інформатики Академії правових наук України. – К.: НДЦПІ АПрН України, 2004 // *www.bod.kiev.ua*	Історія, діяльність, впроваджені проек-ти тощо	Презентаційний буклет, 4 арк.
17	Тезаурус EUROVOC: **а**втоматизована інформаційно-аналітична система порівняння законодавства України із законодавством країн ЄС: посібник ; за ред. академіка НАН України В.Я. Тація та академіка АПН України В.О. Зайчука. – К.: Парламентське видавництво, 2004.	Українська версія багатомовного тезауруса EUROVOC Європейського Парламенту.	Посібник, 383 с.
18	Організаційно-правові питання захисту персональних даних: дис. ... канд. юрид. наук: 12.00.07 – теорія управління; адміністративне право і процес; фінансове право; інформаційне право / В.М. Брижко. – (Науково-дослідний центр правової інформатики АПрН України). – К., 2004	Упорядкування суспільних інформаційних відносин у сфері захисту персональних даних в Україні	Дисертація, 251 с.
19	Системна інформатизація законотворчої та право-охоронної діяльності: монографія ; під науковим керівництвом та редакцією В.В. Дурдинця та В.О. Зайчука. – К.: Парлам. вид-во, 2004	Теоретичні і прак-тичні питання щодо інформаційних систем і технологій	Монографія, 520 с.

20	Системна інформатизація виборчих і референдумних процесів в Україні: монографія / Фурашев В.М., Коваль М.І., Маглюй С.А. – К.: Парлам. вид-во, 2004	Побудова, впровадження та використання інформаційних систем і технологій у практиці	Монографія, 608 с.
21	Основи інформаційного права України: навч. посіб. / Гавловський В.Д., Гриценко В.В., Мельник П.В., Попович В.М., Ріпа С.П., Цимбалюк В.С., Швець М.Я. ; за ред. М.Я.Швеця, Р.А.Калюжного та П.В.Мельника. – К.: Знання, 2004.	Про зміст, сутність та особливости інформаційного права	Посібник, 274 с.
Видання 2005 року			
22	Правова інформатика: підручник : у 2-х т. – Т. 1 / М.Я. Швець, В.М. Брижко, Л.М. Задорожня, Ю.А. Клімашевська, М.І. Коваль, В.М. Фурашев, В.Г. Хахановський та ін. – К.: Парлам. вид-во, 2005.	Побудова, впровадження та використання інформаційних систем і технологій у законотворчій, правозастосовній, правоохоронній, судовій та правоосвітній діяльності	Підручник, 416 с.
23	Проблеми інформаційного права та правової інформатики / В. Брижко, М. Швець, Ю. Базанов ; за ред. члена-кореспондента АПрН України М. Швеця. – [2-е вид., доп.]. – К., 2005 р.	Стан і перспективи державної інформаційної політики та системної інформатизації	Наукове видання, 302 с.

Якщо Вас, шановні читачі, зацікавило те або інше видання НДЦПІ АПрН України, звертайтеся за адресою:

01032, м. Київ, вул. Саксаганського, 110–В.
Науково-дослідний центр правової інформатики
Академії правових наук України

Тел.: 234–94–56
Тел./факс: 234–55–60

РЕЦЕНЗІЯ на монографію:

В. Брижко, М. Швець, М. Коваль, Ю. Базанов.

*“**е-майбутнє та інформаційне право”.*** – [2-е вид., доп.];
за ред. члена-кореспондента АПрН України М.Швеця.
– К.: НДЦПІ АПрН України. – 2005 р. – 303 с. //www.bod.kiev.ua.

Подана на рецензію монографія підготовлена до публікації авторським колективом у складі В. Брижка, М. Швеця, М. Коваля, Ю. Базанова обсягом 303 сторінки.

Монографія є результатом закінченої науково-дослідної роботи авторів з чіткою постановкою проблематики в загальному вигляді у контексті завдань формування теорії та практики інформаційного права і правової інформатики як нових комплексних, міжгалузевих дисциплін у складі юридичної науки.

Авторами монографії проведено глибокий аналіз досліджень, відображених у публікаціях, зокрема, у Інтернеті, в яких започатковано розв’язання проблем теорії і практики інформатизації правотворчості, правозастосування та правової освіти, забезпечення формування інформаційного суспільства як в Україні, так і у світі.

З урахуванням досвіду європейських країн досліджуються проблеми інформатизації та інформаційного права як новий напрям законодавства України, складовою частиною якого є правова інформатика. Оцінюються галузі інформаційного законодавства, в яких можливі найбільш радикальні зміни. Запропоновано концептуальні підходи до формування електронно-цифрового законодавства і кодифікації норм, що регулюють суспільні інформаційні відносини. Наведено складові стратегічних завдань інформатизації, що вимагають нормативно-правового упорядкування на шляху до побудови в Україні інформаційного суспільства.

Видання містить матеріали про принципи державної інформаційної політики щодо вирішення проблем “е-документообігу” та “е-підпису”, про конфіденційну інформацію, що є власністю держави, про інформаційну культуру і злочинність, про окремі аспекти державної програми “е-Україна”, про модулі системи “е-уряд”, про необхідність розвитку законодавства щодо системної інформатизації виборчих і референдумних процесів в Україні та ін. Зроблено історичний екскурс щодо розвитку індустріалізації і комп’ютеризації на пострадянському просторі.

Дослідниками чітко визначено не вирішені раніше частини загальної проблематики, яким присвячена монографія, сформовано ціль та здійснено постановку завдань дослідження. Виклад основного матеріалу дослідної роботи відповідним чином структурований з повним обґрунтуванням отриманих наукових результатів, наведені загальні висновки та перспективи подальшого розвитку інформаційного права та правової інформатики як напрямів наукових досліджень у складі юридичної науки.

Авторами не тільки опрацьовано значна кількість джерел, але й здійснено аналітично-синтетичне дослідження та логічну структуризацію матеріалу, що дозволяє мати наочне та досить повне уявлення щодо стану та перспектив електронно-інформаційного майбутнього та інформаційного права.

Практична значимість розкритих у дослідженні положень та пропозицій полягає у тому, що вони можуть бути корисними у законодавчій, судовій та правозастосовній діяльності для широкого кола науковців, яких цікавлять проблеми правового

упорядкування суспільних інформаційних відносин у сфері інформаційного права та правової інформатики в умовах формування електронно-інформаційного середовища та просування країни до інформаційного суспільства.

Монографія відповідає вимогам до підготовки наукових видань, написана літературною науковою мовою, структура її логічно узгоджена. За змістом вона може бути використана у подальших наукових дослідженнях, а також як навчально-практичне видання при викладенні навчальних дисциплін “Інформаційне право”, “Правова інформатика”, “Інформаційна культура”, “Інформаційна безпека”.

Висновки: монографічне дослідження під назвою “е-майбутнє та інформаційне право” є досить актуальним за сучасних умов активного розвитку та поширення інформаційно-комп’ютерних технологій та телекомунікаційних мереж у всіх сферах діяльності суспільства.

Виходячи із зазначеного, можна рекомендувати монографію “е-майбутнє та інформаційне право” до публікації з метою поширення її серед фахівців у законодавчій, судовій та правозастосовній діяльності, а також для широкого кола науковців, аспірантів та студентів.

Доктор юридичних наук, професор,
начальник кафедри адміністративного права
та адміністративної й кримінально-процесуальної діяльності
Національної академії державної податкової служби України

В.К. ШКАРУПА

РЕЦЕНЗІЯ на монографію

В.Брижко. ***Правовий механізм захисту персональних даних*** ; за ред. члена-кореспондента АПрН України М. Швеця. – 2-е вид., допов. – К.: НДЦПІ АПрН України. – 2005. – 294 с.

У зв’язку із завданнями, що визначені Програмою інтеграції України до Європейського Союзу від 14.09.2000 р., у даний час важливого значення набуває нормативно-правове та організаційно-правове регулювання суспільних інформаційних відносин, пов’язаних із захистом персональних даних, у плані загальної гармонізації вітчизняного законодавства з європейськими стандартами захисту прав людини та основних свобод як необхідної передумови входження України у світовий інформаційний простір.

Актуальність. Проблеми, що висвітлені у монографії, безпосередньо пов’язані із питаннями адаптації законодавства України до законодавства Європейських Співтовариств, початок якої було надано Угодою про партнерство і співробітництво між Україною і ЄС та його державами-членами від 14.06.1994 р., переліком першочергових завдань, що окреслені Постановою Верховної Ради України “Про Заходи державної політики України в галузі прав людини” від 17.06.1999 р. та Програмою інтеграції України до Європейського Союзу від 14.09.2000 р.

Зміст поданої на рецензію монографії свідчить про те, що тематика та проблеми, які у ній висвітлюються, відповідають вищезазначеному, а також є актуальними для теорії і практики становлення нової наукової дисципліни – інформаційного права, що покликане вирішувати питання регулювання суспільних інформаційних відносин та боротьби з правопорушеннями в інформаційній сфері, за умов широкого впровадження інформаційно-комп’ютерних технологій та телекомунікаційних мереж.

Виходячи із завдань, які поставлені у монографії, автором означене правове поле щодо механізмів управління у сфері захисту персональних даних, дослідження яких отримало систематизований зміст, якій спрямований на створення та удосконалення загальнодержавної системи управління в країні. Викладений матеріал має єдиний методичний підхід до розгляду різнорідних питань щодо захисту персональних даних.

Новизна вкладеного у монографії матеріалу полягає в тому, що вперше у вітчизняній науці здійснена спроба поставити питання та аргументувати можливість захисту даних про особу з точки зору її права власності на свої персональні дані. Це дає можливість приступити до подальшого дослідження та формування нових підходів і нових механізмів управління щодо захисту прав та боротьби із злочинністю за умов поширення інформаційно-комп’ютерних технологій та телекомунікаційних мереж.

Аргументовані у монографії теоретичні положення спираються на положення статті 11 Конвенції № 108 Ради Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” від 28.01.1981 р. та чинне законодавство України, зокрема, статті 3 і 22 Конституції України та статтю 54 Закону України “Про інформацію”.

Наукова цінність результатів, отриманих у результаті дослідження різнорідних проблем та питань щодо інформаційного права у сфері захисту персональних даних полягає у тому, що в роботі здійснено досить глибокий огляд та аналіз стану нормативних актів ЄС, а також – національної нормативно-правової бази, практики її реалізації в окремих країнах світу та пострадянських державах, сформульовані

теоретичні висновки і пропозиції, які розвивають засади наукового регулювання зазначеної сфери суспільних інформаційних відносин.

Пропозиції, викладені у монографії, можуть бути використані в законодавчій діяльності, у юридичних та інших навчальних закладах при вивченні дисциплін, пов’язаних із інформацією, інформатикою, інформатизацією, а також при розробці науково-практичних посібників та рекомендацій з питань удосконалення методів боротьби з комп’ютерними правопорушеннями.

Монографія викладена науковою мовою з урахуванням вимог формальної та діалектичної логіки, має детальний, структурований зміст, відповідає викладенню матеріалів щодо наукових досліджень та юриспруденції.

Висновки. Виходячи із зазначеного, монографія може бути рекомендованою до видання, в тому числі в електронному вигляді, та розповсюдження серед широкого кола науковців і практиків з метою подальшого опрацювання загальних і спеціальних питань нормативно-правового та організаційно-правового упорядкування суспільних інформаційних відносин у сфері захисту персональних даних.

Доктор юридичних наук, професор,
заслужений юрист України,
член-кореспондент Академії правових наук України,
перший проректор Української академії державного управління
при Президентові України **Н. НИЖНИК**

Про редакційну колегію:

==========

==========

Адреса редакції: 01032, м. Київ-32, вул. Саксаганського, 110-В.
Тел.: 234-94-56, 246-48-58; тел./факс: 234-55-60; e-mail: *bib_rada@i.kiev.ua.*
Розрахунковий рахунок: № 35224002002155, банк: УДК у м. Києві,
МФО 820019, код ЄДРПОУ 25959933.
Свідоцтво про державну реєстрацію журналу: серія КВ № 8254 від 22.12.2003 р., видане Державним комітетом телебачення і радіомовлення України.

Виготовлено з оригінал-макета НДЦПІ АПрН України в друкарні Київської філії державного підприємства Науково-дослідного економічного інституту Міністерства економіки України.
01103, м. Київ, бул. Др. Народів, 28.

==========

ШАНОВНІ ДРУЗІ !

Журнал “Правова інформатика” видається у двох варіантах – паперовому та електронному.

Зі змістом матеріалів, що розміщені в журналі, Ви маєте можливість ознайомитися наступним чином:

1) зі скороченим змістом матеріалів можна ознайомитися, відвідавши сайт Науково-дослідного центру правової інформатики Академії правових наук України: ***//www.bod.kiev.ua***
або безпосередньо – електронну версію журналу: //***www.bod.kiev.ua/jurnal***;

2) електронний варіант на CD-ROM, крім повного варіанта журналу “Правова інформатика”, містить додатки: бази даних “Законодавство”, “Законопроект”, “Київ”, “Крим” (160000 документів), “Термінологія законодавства України” (22000 термінів), багатомовний тезаурус “EUROVOC” та інформацію про дослідження з проблем держави і права.

Тираж електронного видання: 1000 прим.

Замовити передплату на електронний варіант журналу “Правова інформатика” та вказані бази даних можна за телефоном: **234-55-60.**

Для передплатників журналу встановлення та обслуговування баз даних “Законодавство”, “Законопроект”, “Київ”, “Крим” з активованим щоденним поновленням по e-mail або FTP – за пільговими цінами;

3) паперовий варіант журналу “Правова інформатика” тиражується в обмеженому обсязі. Телефон для довідок: **234-94-56**.