НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА ТА ПСИХОЛОГІЇ

ГРОМАДСЬКА ОРГАНІЗАЦІЯ
«АСОЦІАЦІЯ ДОКТОРІВ ФІЛОСОФІЇ УКРАЇНИ»

ІТ ПРАВО:
ПРОБЛЕМИ І ПЕРСПЕКТИВИ РОЗВИТКУ В УКРАЇНІ

Збірник матеріалів науково-практичної конференції

18 листопада 2016 р.

Львів – 2016

УДК 347.77:004](477)
ББК Х621.152 (4Укр)
І-92

Розглянуто і рекомендовано до друку
Вченою радою Навчально-наукового Інституту права та психології
Національного університету
«Львівська політехніка» (протокол № 4 від 24 жовтня 2016 р.)

Упорядники:

Бачинський Т.В. – асистент кафедри цивільного права та процесу Навчально-наукового інституту права та психології Національного університету «Львівська політехніка», кандидат юридичних наук

Лозовицький Д.С. – докторант кафедри Інформаційних систем в менеджменті Львівського торговельно-економічного університету, кандидат економічних наук, доцент

Радейко Р.І. – асистент кафедри адміністративного та інформаційного права Навчально-наукового інституту права та психології Національного університету «Львівська політехніка», кандидат юридичних наук

Відповідальний за випуск:

Бортник Н.П. – завідувач кафедри адміністративного та інформаційного права Навчально-наукового інституту права та психології Національного університету «Львівська політехніка», доктор юридичних наук, професор

І-92 **ІТ право: проблеми і перспективи розвитку в Україні:** збірник матеріалів науково-практичної конференції. – Львів: НУ «Львівська політехніка», 2016. – 396 с.

У збірнику опубліковано матеріали науково-практичної конференції «ІТ право: проблеми і перспективи розвитку в Україні» (Львів, 18 листопада 2016 р.). Статті присвячені публічно-правовим проблемам сфери ІТ (адміністративно-кримінальні аспекти), приватно-правові проблеми сфери ІТ, управління ефективністю діяльності, рекрутинг, психологічна підготовка фахівців у ІТ сфері.

Для науковців, представників органів державної влади, міжнародних організацій, громадських об'єднань, аспірантів, здобувачів, фахівців у сфері ІТ-права, які практично займаються ІТ-питаннями.

Матеріали конфренції подаються в авторській редакції.

ISSN 2519-1837

УДК 347.77:004](477)
ББК Х621.152 (4Укр)

ЗМІСТ

ВСТУПНЕ СЛОВО

Вже більше двох десятиліть світ живе в інформаційній ері свого розвитку. Інформаційні технології у наш час є ключем до технічного та технологічного прогресу практично у всіх сферах, а також є концентрованим відображенням загальних тенденцій інформаційної революції кінця XX – початку XXI століть.

Стає очевидним, що інформаційні технології інтегрують не тільки комунікаційні та технологічні ресурси, але й матеріальні, фінансові, інтелектуальні, гуманітарні, політичні та інші, формують і диверсифікують процеси соціальної регуляції.

Глобалізація світової економіки була б не можливою без розвитку IT-індустрії. Останні кілька років стали періодом надзвичайно швидких і масштабних змін у галузі інформаційних технологій та обумовлених ними трансформацій світової політики. IT-корпорації та компанії стали флагманами прогресу та еталоном орієнтування у питаннях реалізації глобальних та великих проектів. В умовах інтеграції світової економіки з надшвидкими темпами розвитку IT-індустрії, надзвичайно актуальними для IT-компаній і наукових установ, які готують спеціалістів для IT-галузі, є питання нормативно-правової, психологічної, управлінської підготовки IT-фахівців.

Правове поле діяльності IT-галузі України потребує напрацювання комплексного нормативно-правового забезпечення процесу функціонування IT-сфери. Актуальними питаннями залишаються: забезпечення прав і свобод людини і громадянина, законних інтересів суспільства і держави у сфері IT-права; організації та діяльності суб'єктів забезпечення інформаційної безпеки; запобігання, виявлення і припинення правопорушень (злочинів) в IT-сфері; правові проблеми віртуального середовища; захист прав споживачів при он-лайн купівлі; договірні відносини у сфері передачі прав інтелектуальної власності та захисту прав інтелектуальної

власності в Інтернеті; відповідальність за порушення умов використання контенту; створення правового поля у сфері трудових відносин в IT-галузі, проблеми конвергенції вітчизняного правового поля з нормами міжнародного права для IT-індустрії тощо.

Основну мету конференції «IT-право: проблеми і перспективи розвитку», організатори вбачають у започаткуванні нової традиції академічної дискусії щодо перспектив, проблем і нових бачень в IT-сфері.

Залучення до роботи конференції не лише теоретиків, але й представників органів державної влади України, громадських об'єднань, фахівці у сфері IT-права, які на практиці займаються IT-питаннями, дає змогу визначити та проаналізувати проблеми і перспективи розвитку IT-права.

Ортинський В.Л.
Директор Навчально-наукового інституту права та психології Національного університету «Львівська політехніка», доктор юридичних наук, професор, заслужений юрист України

ПУБЛІЧНО-ПРАВОВІ ПРОБЛЕМИ СФЕРИ ІТ (АДМІНІСТРАТИВНО-КРИМІНАЛЬНІ АСПЕКТИ). КІБЕРБЕЗПЕКА

Арістова І.В. –
завідувач кафедри адміністративного та інформаційного права Сумського національного аграрного університет, доктор юридичних наук, професор

МЕТОДОЛОГІЯ НАУКИ «ІНФОРМАЦІЙНЕ ПРАВО»

Звертаючись до стислої характеристики сучасного стану науки «інформаційне право», слід зазначити, що вона лише зароджується, і майже не має у своєму арсеналі фундаментальних теоретичних досліджень, що визнані усією науковою юридичною спільнотою. Водночас, вчені все частіше звертаються до інформаційно-правових та близьких до них проблем, відкриваючи крок за кроком нові горизонти науки «інформаційне право», у тому числі ІТ-права. На сьогодні вже існує низка досліджень, в яких здійснено спробу усвідомлення феномена «інформаційне право», зокрема його методології. Серед вітчизняних вчених слід передусім назвати О. А. Баранова, К. І. Бєлякова, В. М. Брижка, Р. А. Калюжного, Л. П. Коваленко, Б. А. Кормича, В. А. Ліпкана, А. І. Марущака, А. М. Новицького, В. Г. Пилипчука, О. М. Селезньової, І. М. Сопілко, В. С. Цимбалюка та ін.

Узагальнюючи позиції вчених, які досліджують та вирішують проблеми у сфері інформаційного права, вважаємо, що існують відповідні підстави стверджувати наступне. У

переважній більшості робіт (наприклад, [1-4]) поняття «методологія» визначається як сукупність методів та прийомів наукового пізнання, у тому числі у сфері суспільних інформаційних відносин. Відмічаючи позитивну роль авторів зазначених робіт у становленні науки «інформаційне право», водночас, вважаємо за необхідне відмітити існування в інформаційному праві недостатнього розуміння поняття «методологія», розгляду методології лише як інструментарію. Вважаємо за доцільне викласти та обґрунтувати власну точку зору щодо визначення поняття «методологія науки «інформаційне право»«.

У роботі відстоюється позиція, що необхідною умовою становлення будь-якої науки (у тому числі науки «інформаційне право») постає формування її методології. До того ж, вихідним положенням нашого дослідження постає те, що загальна теорія права та держави має бути фундаментом науки «інформаційне право» [5]. Виходячи із зазначеного вище, було з'ясовано точки зору фахівців у галузі загальної теорії права та держави (зокрема, М. І. Матузова, О. В. Малька, О. Ф. Скакун, Л. А. Луць, О. В. Зайчука, Н.М. Оніщенко) щодо розуміння поняття «методологія». Встановлено, що у філософському словнику методологія розуміється як наука, яка вивчає пізнання і наукову діяльність [6, с. 278]. Погоджуючись з позицією авторів роботи [7, с. 41], що методологія як теорія має не тільки загальносоціальний, а й універсальний характер, водночас, вважаємо, що у зазначеній роботі не було розвинуте положення стосовно того, що методологія – це організація наукової діяльності [7,с. 36]. На нашу думку, яскравим прикладом розвитку цього положення постають дослідження, що знайшли своє ґрунтовне висвітлення у роботі [8].

Перед тим, як визначитися із власною позицією щодо розуміння поняття «методологія», «методологія науки» (у тому числі науки «інформаційне право»), вважаємо за необхідне з'ясувати визначення поняття «наука». Поділяючи думку щодо пріоритетності використання структурного аналізу у процесі дослідження науки [9, с. 90], і водночас, розуміючи науку як багатоаспектне явище, у роботі вважається, що основними її аспектами (які слід чітко розрізняти у кожному конкретному

випадку) є наступні: 1) наука як результат (наукові знання); 2) наука як процес (наукова діяльність); 3) наука як соціальний інститут (спільнота вчених, сукупність наукових установ і структур наукового обслуговування) [8, с. 28]. Вважалося за доцільне передусім акцентувати увагу на перших двох аспектах науки.

На основі проведених досліджень було встановлено, що становлення науки «інформаційне право» вимагає розробки якісних пізнавальних моделей. З цією метою у роботі сформовано модель дослідження науки «інформаційне право» (пізнавальну модель) як системну цілісність двох взаємодіючих моделей: 1) перша модель – модель дослідження науки «інформаційне право» (як результат, наукові знання); 2) друга модель – модель дослідження науки «інформаційне право» (як процес, наукова діяльність) [10].

З'ясовано, що наукова діяльність (у тому числі у сфері інформаційного права), за умови її грамотного здійснення, спрямована на новий науковий результат, що зумовлює необхідність її організації. На нашу думку, у зв'язку з цим, свого уточнення буде потребувати друга модель дослідження науки «інформаційне право» («як процесу», «як наукової діяльності»). Встановлено, що концепція уточнення другої моделі має включати положення щодо ефективної форми організації діяльності (у тому числі наукової). Аналіз різноманітних форм організації діяльності [8, с. 14-22] дозволив дійти висновку, що в умовах розвитку інформаційного суспільства доцільно досліджувати організацію наукової діяльності у сфері інформаційного права в проектній формі.

Аналіз положень запропонованої концепції уточнення другої моделі (моделі дослідження науки «інформаційне право» як наукової діяльності) дозволив усвідомити необхідність включення до цієї концепції положення щодо створення третьої моделі (моделі організації наукової діяльності у сфері інформаційного права). У роботі запропоновано відповідну модель, особливістю якою є те, що вона комплексно враховує: 1) статику (результат): це система, невід'ємними складовими якої є: а) суб'єкт (наприклад, вчений); б) об'єкт (наука «інформаційне право»); в) прямі та зворотні зв'язки між

суб’єктом та об’єктом (за допомогою форм, засобів, методів, результатів). Системоутворюючим чинником постає ціль (мета), яка має узгоджуватися з метою, що задається надсистемою – юридичною наукою; 2) динаміку (процес): це система, складовими якої (критерій – «за часом») є наступні: фази, стадії, етапи наукової діяльності.

Водночас, аналіз, зокрема роботи [8, с. 6], дозволяє переконатися, що організацію діяльності розглядає методологія, яка визначається як вчення про організацію діяльності. Виходячи із того, що наукова діяльність у сфері інформаційного права є творчим процесом, який потребує організації, є підстави стверджувати, що організація наукової діяльності у сфері інформаційного права постає предметом методології науки «інформаційне право» (як наукової діяльності). Ґрунтуючись на розширеному розумінні методології як вчення про організацію наукової діяльності (у тому числі, наукових знань) та системній цілісності науки «інформаційне право» (як результату та як наукової діяльності), обґрунтовано визначення поняття «методологія науки «інформаційне право» як вчення про організацію наукової діяльності (у тому числі, наукових знань) у сфері інформаційного права.

Встановлено, що методологія науки «інформаційне право» має обов’язково враховувати існування суб’єкта, об’єкта, мети, методів наукової діяльності у сфері інформаційного права. Тобто, розгляд методології науки «інформаційне право» лише як сукупності методів та засобів дослідження виявляється не повним. Таким чином, вважаємо, що адекватною моделлю предмета методології науки «інформаційне право» (і як наукової діяльності, і як результату) можна вважати третю модель (модель організації наукової діяльності у сфері інформаційного права), у якій організації потребує як процес (наукова діяльність), так і результат наукової діяльності (отримані наукові знання про об’єкт – «науку «інформаційне право»).

Виходячи із важливої ролі та місця суб'єкта наукової діяльності у методології науки «інформаційне право», у роботі вважалося за необхідне акцентувати увагу на дослідженні якісних стандартів, які мають бути у будь-якого суб'єкта. Такі стандарти передусім виробляються наукознавством. У роботі

відстоюється позиція, що дослідник в сфері інформаційного права повинен достатньо чітко та свідомо: 1) уявляти, що таке наука, як вона організовується; 2) знати закономірності розвитку науки, структуру наукового знання, критерії науковості нового знання, форми наукового знання, якими він користується і в яких він хоче відобразити результати свого наукового дослідження і т. ін. [8, с. 26]. Тобто, у дослідника (суб'єкта) обов'язково має бути підґрунтя для наукової діяльності у сфері інформаційного права для того, щоб ця діяльність була свідома та організована. Враховуючи те, що наукознавство, як галузь науки, включає гносеологію, яка, у свою чергу, включає, як компонент своєї структури, методологію науки, з'ясовано деякі гносеологічні засади методології науки «інформаційне право» [11].

Перша гносеологічна засада: вчений, який займається дослідженнями у сфері інформаційного права, має враховувати, зокрема, існування однієї із закономірностей розвитку науки в цілому – взаємодію та взаємопов'язаність усіх галузей науки. Звертаємо увагу на важливість взаємодії усіх галузей юридичної науки, оскільки це дозволяє досліджувати предмет однієї із галузей юридичної науки (наприклад, науки «інформаційне право») за допомогою прийомів і методів інших юридичних наук.

Друга гносеологічна засада: для формування у суб'єкта якісного стандарту під час проведення наукових досліджень вельми важливо актуалізувати здійснення спеціальних досліджень у напряму вибору критеріїв науковості знання, а також їх використання у сфері інформаційного права. Було виділено групи критеріїв науковості: 1) історичні критерії науковості (формально-логічна непротирічність знання; перевірка досвідом та емпірична обґрунтованість; інтерсуб'єктивність та універсальність та ін.); 2) функціонально-орієнтовані критерії науковості (логічні критерії – непротирічність, повнота, незалежність вихідних аксіом та ін.; прагматичні критерії – простота, інструментальна ефективність та ін.); 3) об'єктивно-предметні критерії науковості (системність, доказуємість та обґрунтованість, достовірність та об'єктивна істинність).

Третя гносеологічна засада: однією із складових стандарту дослідника у сфері інформаційного права, має бути інформація про форми організації наукових знань. Встановлено, що на сьогодні у літературі практично відсутнє систематичне викладення зазначеного питання. Аналіз багатьох наукових праць у сфері інформаційного права засвідчив, що науковці: 1) вводять у науковий обіг різноманітні поняття, категорії; 2) висувають гіпотези; 3) розробляють концепції, теорії; 4) формують ідеї; 5) порушують проблему і т. ін. З одного боку, у роботі підтримується у цілому намагання дослідників щодо розбудови науки «інформаційне право», з іншого боку, вважаємо, що науковий рівень цих досліджень не завжди «дотягує» до існуючих стандартів, зокрема, щодо правильного розуміння та коректного використання таких конструкцій, як концепція, теорія, категорія та ін. Наприклад, немає чіткого розуміння загального та вузького тлумачення терміну «теорія», основних компонентів теорії, типів теорії, центрального системоутворюючого елемента теорії тощо. Така ситуація зумовлює потребу у проведенні досліджень форм організації наукових знань у сфері інформаційного права.

Акцентовано увагу на одній із форм організації наукових знань у сфері інформаційного права – понятті. Виходячи із того, що процес утворення та розвитку понять вивчає логіка (формальна та діалектична), необхідно активізувати використання логіки для правильного визначення понять науки «інформаційне право». Встановлено способи визначення понять. Аналіз багатьох наукових досліджень у сфері інформаційного права (передусім дисертаційних досліджень) переконливо доводить, що використання логіко-семантичного методу для визначення понятійної бази лише анонсується, і насправді є суттєві підстави для активізації наукової дискусії щодо правильного мислення, яке має бути підпорядковано вимогам чотирьох його законів. Звертаємо увагу науковців на необхідність спільного вирішення цього питання. Глибоке дослідження «поняття», як форми організації наукового знання у сфері інформаційного права, сприятиме розробці нових теорій, концепцій та ін.

Наукові пошуки у зазначеному напрямі будуть продовжені. Будемо вдячні за пропозиції та критичні зауваження.

Список літератури

1. Ліпкан В. А. Систематизація інформаційного законодавства України: Монографія/ В. А. Ліпкан, В. А. Залізняк/ за заг. ред. В. А. Ліпкана. – К.: ФОП О.С. Ліпкан, 2012. – 304 с.

2. Цимбалюк В. С. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства: Монографія/ В. С. Цимбалюк. – К.: Освіта України, 2011. – 426 с.

3. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика: Монографія / О. А. Баранов. – К.: Едельвейс, 2014. – 434 с.

4. Селезньова О. М. Теоретико-методологічні основи інформаційного права України: Монографія / О. М. Селезньова. – Чернівці: «Місто», 2014. – 408 с.

5. Арістова І. В. Наука «інформаційне право» на новому етапі розвитку інформаційного суспільства / І.В.Арістова // Правова інформатика. – 2011. – № 1. – С.3–11.

6. Философский словарь. – М.: Политиздат, 1986. – 518 с.

7. Теорія держави і права (Академічний курс): Підручник / за ред. О. В. Зайчука, Н. М. Оніщенко. – [вид 2-е, перероб. і доп.]. – К.: Юрінком Інтер, 2008.– 688 с.

8. Новиков А. М., Новиков Д. А. Методология научного исследования / А. М. Новиков, Д. А. Новиков. – М.: Либроком, 2009. – 280 с.

9. Философия и методология науки: Учебное пособие для аспирантов и магистрантов/ А. И. Зеленков и др./ под ред. А. И. Зеленкова. – [изд. 2-е, доп. и испр.].– Минск: ГИУСТ, 2011.– 479 с.

10. Арістова І. В. Становлення науки «інформаційне право»: питання методології (частина І) / І. В. Арістова // Публічне право. – 2016. – № 2. – С. 245-253.

11. Арістова І. В. Становлення науки «інформаційне право»: питання методології (частина 2) / І. В. Арістова // Публічне право. – 2016. – № 3. – С. 102-110.

Баїк О. І. –
доцент кафедри цивільного права та процесу Навчально-наукового інституту права та психології Національного університету «Львівська політехніка» кандидат юридичних наук

СУБ'ЄКТИ РЕГУЛЮВАННЯ ПРАВОВІДНОСИН У СФЕРІ ПОДАТКОВОЇ ІНФОРМАЦІЇ

Правове регулювання правовідносин, які виникають щодо збирання, зберігання, використання та поширення податкової інформації здійснюється Податковим кодексом України від 2 грудня 2010 р. № 2755-VI, Законом України від 2 жовтня 1992 р. № 2657-XII «Про інформацію», Законом України від 13 січня 2011 р. № 2939-VI «Про доступ до публічної інформації», постановою Кабінету Міністрів України від 27 грудня 2010 р. № 1245 «Про затвердження Порядку періодичного подання інформації органам державної податкової служби та отримання інформації зазначеними органами за письмовим запитом» та іншими нормативно-правовими актами.

Статтею 16 Закону України «Про інформацію» від 02.10.1992 р. № 2657-XII визначено, що податкова інформація – це сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України. Правовий режим податкової інформації визначається Податковим кодексом України та іншими законами [1]. Отже, інформація є об'єктом інформаційних відносин (ст. 4 Закону України «Про інформацію»).

Суб'єктами інформаційних відносин є: а) фізичні особи (резиденти і нерезиденти України, у тому числі самозайняті особи); б) юридичні особи (резиденти і нерезиденти України) та їх відокремлені підрозділи; в) об'єднання громадян, г) релігійні організації; д) суб'єкти владних повноважень, які є платниками податків; е) Національний банк, банки та інші фінансові

установи; є) міжнародні організації (ст. 4 Закону України «Про інформацію», ч. 4 Порядку періодичного подання інформації органам державної податкової служби та отримання інформації зазначеними органами за письмовим запитом, затвердженого постановою Кабінету Міністрів України від 27 грудня 2010 р.).

Процедуру періодичного подання органам державної фіскальної служби суб'єктами інформаційних відносин або подання за письмовим запитом таких органів податкової інформації визначено в Порядку періодичного подання інформації органам податкової служби та отримання інформації зазначеними органами за письмовим запитом, затвердженому постановою Кабінету Міністрів України від 27 грудня 2010 р. № 1245 [2].

Суб'єкт інформаційних відносин (платник податків) має право на нерозголошення контролюючим органом (посадовими особами) відомостей про такого платника без його письмової згоди та відомостей, що становлять конфіденційну інформацію, державну, комерційну чи банківську таємницю та стали відомі під час виконання посадовими особами службових обов'язків, крім випадків, коли це прямо передбачено законами (ч. 17.1 п. 17.1.9 ст. 17 ПК України).

Контролюючим органом є центральний орган виконавчої влади, що забезпечує формування єдиної державної податкової, державної митної політики в частині адміністрування податків і зборів, митних платежів та реалізує державну податкову, державну митну політику, забезпечує формування та реалізацію державної політики з адміністрування єдиного внеску, забезпечує формування та реалізацію державної політики у сфері боротьби з правопорушеннями при застосуванні податкового та митного законодавства, а також законодавства з питань сплати єдиного внеску, його територіальні органи. У складі контролюючих органів діють підрозділи податкової міліції (п. 41.1 ст. 41 ПК України) [3].

Інформаційно-аналітичне забезпечення діяльності контролюючих органів регулюється Главою 7 ПК України. Зокрема в даній главі закріплено правові норми щодо збору податкової інформації (ст. 72), її отримання контролюючими

органами (ст. 73), обробки та використання податкової інформації (ст. 74).

Посадові особи контролюючих органів зобов'язані:

– не допускати розголошення інформації з обмеженим доступом, що одержується, використовується, зберігається під час реалізації функцій, покладених на контролюючі органи (п. 21.1.6 ч. 21.1 ст. 21 ПК України);

– надавати органам державної влади та органам місцевого самоврядування на їх письмовий запит відкриту податкову інформацію в порядку, встановленому законом (п. 21.1.7 ч. 21.1 ст. 21 ПК України).

Беручи до уваги вищевикладене, а також положення ст. 20 Закону України «Про інформацію», за порядком доступу податкова інформація поділяється на:

1) відкриту податкову інформацію;

2) податкову інформацію з обмеженим доступом.

Відкрита податкова інформація – це будь-яка податкова інформація, крім тієї, що віднесена до податкової інформації з обмеженим доступом на підставі чинного законодавства. Відкритою вважається публічна інформація, крім випадків, встановлених законом (ст. 1 Закону України «Про доступ до публічної інформації»). В окремих випадках ця інформація стає «джерелом» для протиправних посягань «рекету» зі сторони злочинців для незаконного отримання грошей та інших матеріальних цінностей.

Оскільки контролюючі органи є центральним органом виконавчої влади, що забезпечує формування та реалізує державну податкову і митну політику, то інформацію, яка ними використовується є публічною. Публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом (ст. 1 Закону України «Про доступ до публічної інформації») [4].

Податковою інформацією з обмеженим доступом є:

1) конфіденційна інформація – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов;

2) таємна інформація – інформація, доступ до якої обмежується відповідно до ч. 2 ст. 6 Закону України «Про доступ до публічної інформації», розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю;

3) службова інформація – інформація, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; інформація, зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці (ст.ст. 6-9 Закону України «Про доступ до публічної інформації»).

Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами (ч. 3 ст. 21 Закону України «Про інформацію»).

Отримання податковим органом інформації про платників податків здійснюється в рамках правовідносин, які виникають у силу ПК України, мають публічно-правовий характер та засновані на владному підпорядкування однієї сторони іншій. У даних правовідносинах податковому органу, який діє від імені держави, належить владне повноваження вимагати необхідну інформацію, а платнику податків – обов'язок її надати [5, с. 99].

Платники податків несуть відповідальність у разі вчинення порушень, визначених законами з питань оподаткування та іншим законодавством, контроль за дотриманням якого покладено на контролюючі органи, зокрема за:

– за неподання, несвоєчасне подання декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, або в разі виявлення у ній недостовірних відомостей (ч. 4 ст. 45 Закону України «Про запобігання корупції«) [6];

– неподання, порушення порядку заповнення документів податкової звітності, порушення строків їх подання контролюючим органам, недостовірність інформації, наведеної у зазначених документах (ст. 47 ПК України);

– порушення строку та порядку подання інформації про відкриття або закриття банківських рахунків (ст. 118 ПК України);

– порушення платником податків порядку подання інформації про фізичних осіб-платників податків (ст. 119 ПК України);

– неподання або несвоєчасне подання податкової звітності або невиконання вимог щодо внесення змін до податкової звітності (ст. 120 ПК України);

– неподання або подання з порушенням строку банками чи іншими фінансовими установами податкової інформації контролюючим органам (ст. 128 ПК України) та ін.

Податковий контроль здійснюється шляхом: а) ведення обліку платників податків; б) інформаційно-аналітичного забезпечення діяльності контролюючих органів; в) перевірок та звірок відповідно до вимог ПК України, а також перевірок щодо дотримання законодавства, контроль за дотриманням якого покладено на контролюючі органи, у порядку, встановленому законами України, що регулюють відповідну сферу правовідносин (ст. 62 ПК України).

Узагальнюючи, звертаємо увагу на те, що правовідносини у сфері податкової інформації на сьогодні хоча і врегульовані законами України «Про інформацію», «Про доступ до публічної інформації» та іншими нормативно-правовими актами, однак у ПК України відсутнє чітке визначення відкритої податкової інформації та податкової інформації з обмеженим доступом.

Список літератури

1. Про інформацію: Закон України від 02 жовтня 1992 р. № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650 (редакція від 25.06.2016 р., підстава 1405-19).
2. Про затвердження Порядку періодичного подання інформації органам податкової служби та отримання інформації зазначеними органами за письмовим запитом: постанова Кабінету Міністрів України від 27 грудня 2010 р. № 1245 // Офіційний вісник України. – 2011. – № 1. – Ст. 30 (редакція від 04.10.2011 р., підстава 1007-2011-п).
3. Податковий кодекс України від 02 грудня 2010 р. № 2755-VI // Відомості Верховної Ради України. – 2011. – № 13-14, № 15-16, № 17. – Ст. 112 (редакція від 06.11.2016 р., підстава 1665-19).
4. Про доступ до публічної інформації: Закон України від 13 січня 2011 р. № 2939-VI // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 314 (редакція від 01.05.2015 р., підстава 319-19).
5. Бабін І. І. Правове регулювання податкової таємниці за законодавством України / І.І. Бабін // Науковий вісник Чернівецького університету. – 2012. – Випуск 618. – С. 98-101.
6. Про запобігання корупції: Закон України від 14 жовтня 2014 р. № 1700-VII // Відомості Верховної Ради України. – 2014. – № 49. – Ст. 2056 (редакція від 05.10.2016 р., підстава 1403-19).

Барабаш О.О. –
доцент кафедри адміністративного та інформаційного права, Навчально-наукового інституту права та психології Національного університету «Львівська політехніка», кандидат юридичних наук

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІНТЕРНЕТ-ПРАВОВІДНОСИН

Поняття «поведінка» – є багатогранне та полідисциплінарне, оскільки є предметом дослідження низки гуманітарних наук (філософії, психології, соціології, медицини, демографії тощо). Для соціології характерне розмежування понять «поведінка» і «соціальна поведінка». І якщо «поведінка» розглядається як взаємодія усіх живих істот із довкіллям, то «соціальна поведінка» розкривається вже як поведінка людини, що формується, розвивається і виявляється в умовах

суспільного життя, а тому має соціально зумовлений характер. Щодо сучасної психології, то термін «поведінка» розглядається як родове поняття, що охоплює всі вимірювані реакції організму: дію, діяльність, реакцію, рух, процес, операцію. У філософії поняття «поведінка» також характеризує процес взаємодії живих істот із довкіллям, а поведінка людини визначається як здатність людини до діяльності у матеріальній, інтелектуальній та соціальній сферах життя [1, с.230]. Враховуючи зазначене вище так чи інакше поведінка людини (її зовнішній вираз) пов'язаний з певним середовищем.

За останнє століття людство зробило значний стрибок в розвитку науки та техніки, що спричинило виникнення нового простору для зовнішнього вияву поведінки – мережі Інтернет. К.В. Єфремова, зазначає, що **склалося стале уявлення про Інтернет як про особливе, віртуальне середовище. Інтернет стає відображенням реального життя, в ньому складаються практично всі ті види відносин, які існують поза ним** [2, с.5].

Суспільні відносини як відносини між людьми так чи інакше визначаються напрямом поведінки їх суб'єктів, про що зазначають зокрема О. Ф. Скакун[3, с. 376], Є. П. Литвинов [4, с. 145], К. В. Єфремова [2, с. 7] та ін. Будь-які суспільні відносини потребують регулятора, найефективнішим регулятором суспільних відносин виступає право. Щодо правового регулювання суспільних відносин, що виникають в мережі інтернет існують різні думки, від повного заперечення необхідності правового регулювання таких суспільних відноси до створення спеціального законодавства, яке б регулювало такі відносини. Науковці, що говорять про неможливість правового регулювання інтернету - вказують на те, що фактично сама мережа створювалася для вільного доступу та спілкування без правових обмежень, а основні правила поведінки в Інтернеті встановлюються самими учасниками цих суспільних відносин. Тобто йдеться про саморегулюючу систему, яка має виключно внутрішні правила поведінки, прописані у різних кодексах поведінки, правилах користування. Такий підхід щодо ролі держави у регулюванні мережі Інтернет та встановленні законодавчого регулювання, пов'язаний з генезисом мережі. У більшості країн світу мережа Інтернет розвивалась

академічними спільнотами, які розробляли та використовували внутрішні регулятивні інструменти. Досить незначне поширення та чіткі внутрішні правила поведінки давали можливість регулювати суспільні відносини на перших етапах розвитку мережі Інтернет. Проте поява та бурхливий розвиток комерційних відносин у мережі Інтернет, створення умов для вільного широкого доступу усіх людей, з різними намірами, бажаннями, особливостями виховання загострили проблеми суспільного регулювання взаємозв'язків між окремими громадянами, групами осіб. Виникла потреба в регулюванні суспільних відносин, пов'язаних із підприємницькою діяльністю, із обігом цифрових продуктів (аудіо, відео, програмного забезпечення). У мережі почали надаватися платні послуги. Усе це стало причиною необхідного впливу держави на правове регулювання суспільних відносин у інтернеті [5, с. 52].

К. В. Єфремова [2], О. Р. Шишка [6] притримуються схожої думки та вважають, що суспільні відносини, що виникають в мережі інтернет – є надзвичайно широкими за обсягом та частина з них може регулюватися наявними законодавчими актами (наприклад **для боротьби з кримінальними злочинами в інтернеті, цілком достатньо чинного законодавства** [2, с. 6]), а частина потребує спеціального правового регулювання (**існує нагальна потреба правового регулювання у сфері електронного бізнесу й усіх його видів** [2, с. 6]).

Виникає питання про виділення правовідносин в інтернеті в окремий вид, серед науковців немає однозначної відповіді щодо цього питання. Ю. Е. Булатецький [7, с. 880], В. А. Копилов [8, с.135] у ході аналізу взаємовідносин інтернету і права та проблем правового забезпечення електронної торгівлі спеціально виділяють поняття «правовідносини в інтернеті» та «інформаційні відносини в інтернеті», під якими розуміють врегульовані нормами права відносини у віртуальному просторі інтернету. При цьому вони відзначають, що ці правовідносини мають у своєму складі суб'єктів (розробники мереж, провайдерів, споживачі інформації з інтернету) і спрямовані на певні об'єкти (інформаційні права і свободи, доменні імена,

сайти, інформаційні системи та ін.). Реалізація правовідносин передбачає тут поширення відомостей, даних у реальності, у віртуальному просторі, їх використання, інформаційну безпеку мереж, власників технічних засобів. М. В. Якушев вводить нове поняття «інтернет-відносини». Він за змістом визначає їх як віртуальні відносини в Інтернеті, регламентовані нормами права та етики, і говорять про необхідність правового регулювання відносин у мережах, в галузі електронної торгівлі, при укладанні зовнішньоекономічних угод, у сфері мережевих ЗМІ, інформаційного обміну провайдерів, організацій[9, с. 132]. Д. В. Грибанов, вважає, що суспільні відносини, що виникають з використанням глобальних комп'ютерних мереж, виступають особливими інформаційними відносинами, спрямованими на організацію руху інформації в суспільстві і зумовленими інформаційної природою самого суспільства. Ці особливі відносини автор називає інформаційно-кібернетичними [10, с .13-14].

Ми вважаємо слушною думку О. Р. Шишки, який зазначає, що галузевий критерій виділу правовідносин як предмету правового регулювання своє значення втрачає і окрім методу для цих правовідносин лише залишається системоутворюючий, який є засобом чи середовищем їх існування, таким є так зване віртуальне середовище – мережа інтернет [6, с. 1086], тому ми вважаємо, що відносини в інтернеті можна виокремити як окремий вид.

Щодо визначення інтернет-відносин вважаємо за необхідне погодитися з думкою К. В. Єфремової [2, с. 8] та Є. П. Литвинова [4, с. 147], які вважають, що **це новий тип суспільних відносин, що виникають, змінюються і припиняються у кіберпросторі. Це не правові в чистому вигляді і не фактичні відносини. Це соціальні зв'язки особливої правової, інформаційної та технічної природи.**

Особливостями досліджуваних відносин є: обов'язкова наявність технічних компонентів, інформаційне наповнення даного виду відносин і особливий суб'єктний склад. Крім того, вони не завжди гарантуються або забезпечуються примусовою силою якої-небудь однієї держави, так як досліджувана сфера планетарна за своєю суттю. Таким чином, досліджувані

відносини характеризуються головним чином тими особливостями, які випливають із специфічної середовища їх формування та існування – інформаційного середовища всесвітньої комп'ютерної мережі інтернет. Тому це суспільні відносини, що існують в електронній формі в кіберпросторі [11, с. 8].

Коротко охарактеризуємо склад інтернет-відносин. Суб'єкти є учасниками інтернет-відносин. *Під суб'єктами «розуміються – люди та їх об'єднання, які виступають в якості носіїв прав та обов'язків.* Всі суб'єкти інтернет-відносин (розробники мереж, фахівці, провайдери, клієнти та ін.) – це власники або носії певних прав та обов'язків у віртуальному просторі Інтернету. І суб'єктами тут можуть виступати, як юридичні особи (провайдери, які мають ліцензії на надання онлайнових послуг, так і ті провайдери, які купують інтернет-трафік у операторів, які мають ліцензію), фізичні особи (громадяни – споживачі інформації: громадяни України, іноземці, особи без громадянства та ін.). Причому зазначені особи повинні відповідати вимогам міжнародного та національного законодавства в частині правоздатності, дієздатності, деліктоздатності. Таким чином, основними учасниками мережі Інтернет виступають: користувачі; оператори зв'язку; сервіс-провайдери, які забезпечують доступ до Мережі; хост-провайдери, що мають за плату дисковий простір на своєму сервері клієнтам, а також інші базові послуги Інтернету; розробники транскордонних інформаційних мереж та мережевих технологій; спеціалісти [4, с. 147].

В якості об'єктів інтернет-відносин виступають будь-які явища, які відчувають на собі вплив з боку суб'єктів в інтернеті. Інакше кажучи, тут «об'єктом відносин виступає те, на що спрямовані суб'єктивні права і обов'язки його учасників». Здається, що сьогодні тут важко чітко визначити коло об'єктів інтернет-відносин. Більш того, якщо врахувати, що через інтернет можуть реалізовуватися всі види суспільних відносин, то, швидше за все, необхідно визнати правильним плюралістичний підхід до поняття об'єктів правових відносин в інтернеті. Тому в залежності від характеру і видів інтернет-відносин їх об'єктами можуть виступати: поведінка різних

суб'єктів, різного роду інформаційні послуги і їх результати, продукти духовної творчості, включаючи твори літератури, мистецтва, музики та ін., цінні папери, договори, офіційні документи, честь, гідність, безпека людини, речі, предмети та інші цінності.

Однак суб'єкти та об'єкти будуть «мертві», якщо не будуть тут приведені в дію суб'єктивні права і обов'язки суб'єктів інтернет-відносин. Соціальне регулювання в віртуальному просторі, включаючи норми моралі, етики та ін., як показує досвід, здійснюється через механізм реалізації суб'єктивних прав і обов'язків. Зазначені права та обов'язки взаємодіють один з одним у рамках інтернет-відносин, виступають змістом цього механізму.

Технічні засоби теж найважливіший компонент інтернет-відносин. Вони включають в себе глобальне об'єднання комп'ютерних мереж (регіональних, опорних, відомчих, корпоративних, локальних) та інформаційних ресурсів (сайтів, служб електронної пошти, пошукових систем). І головною тут є мережа самого інтернету. Вона виросла з мережі «Арпанет» (ARPANET), створеної десятки років тому для обміну інформацією між рядом дослідницьких центрів військової промисловості США. У даний час Мережа налічує багато мільйонів комп'ютерів і засобів доставки інформації. Вона може запропонувати споживачам численні бази даних, включаючи бази юридичної інформації [4, с.148].

Враховуючи наведене вище, можна зробити висновок, що відносини, які виникають між різними суб'єктами в мережі інтернет мають як спільні так і відмінні ознаки в порівнянні з іншими правовідносинами. Інтернет-відносини є самостійним видом відносин (виділені за ознакою специфічного середовища існування – мережі інтернет). Аналізовані суспільні відносини потребують подальшого наукового дослідження та відповідного правового регулювання.

Список літератури

1. Гарасимів, Т. З. Поняття «поведінка» та «діяльність» як основа філософеми девіантної поведінки [Текст] / Т. З. Гарасимів // Вісник Національного університету «Львівська політехніка». Юридичні науки. – 2015. – № 824. – С. 228-232.

2. Єфремова К.В. До перспектив правового регулювання інтернет-правовідносин: господарсько-правовий аспек / К.В. Єфремова // Право та інноваційне суспільство. – 2014. – № 1. – С. 5-11.

3. Скакун О. Ф. Теория государства и права (энциклопедический курс) : учебник / О. Ф. Скакун. – Харьков : Эспада, 2005. – 840 с.

4. Литвинов Є.П. Правовідносини в інтернет-праві / Є.П. Литвинов // Часопис Київського університету права. – 2013. – № 3. – С.145-149.

5. Новицький А.М. Міжнародний досвід правового регулювання Інтернет / А.М. Новицький // Повітряне і космічне право. – 2014. – № 2 (31). – С. 52-58.

6. Шишка О. Р. Приватноправові відносини та специфіка їх розвитку в мережі Інтернет / О. Р. Шишка // Форум права. – 2012. – № 1. – С. 1085-1090.

7. Булатецкий Ю. Е. Правовое обеспечение электронной торговки / Ю. Е. Булатецкий. – М., 2002. – 934с.

8. Копылов В. А. Информационное право./ В. А. Копылов. – М., 2008. – 512 с.

9. Якушев М. В. Интернет и право: новые проблемы, подходы, решения // Третья Всероссийская конференция «Право и Интернет: теория и практика», 28-29 ноября 2000 г. – М., 2000. – С. 132-133.

10. Грибанов Д. В. Правовое регулирование кибернетического пространства как совокупности информационных отношений: Дисс. ... канд. юрид. наук. – Екатеринбург, 2003. – 197с.

11. Тедеев А. А. Информационное право (право Интернета). А. А. Тедеев. – М., 2005. – 304с.

Bezzubov D.
Doctor of Juridical Science, assistant professor, National Aviation University, Educational and Research Institute of Law

ADMINISTRATIVE PHENOMENA OF SOCIAL SECURITY (INFORMATION VISION)

The modern state of the legal system of Ukraine is defined by the theoretical and practical significance of the challenging and outstanding issues connected with the optimization of formation and functioning of the mechanism of legal support of social security in term of the modern Ukrainian statehood and constant transformation of regulatory environment.

The changes in the regulatory stripped model provide taking into account all aspects of the functioning of the executive government authorities. The one of the most relevant aspects of the practical activity of the executive authorities is the notion of «social security» and its meaning. But the specified category is not directly specified in the positive law and is not sufficiently researched in the national science by the predecessor. Thus it is fragmentarily represented in the current legislative acts of Ukraine connected with it in Ukraine.

One of the most outstanding problems of the countries of the European Union is the problem of social security against the different threats. The main threats are: migration threats (illegal migration), terroristic threats (threat of terroristic attacks at the public places), war threats (intrusion of «hybrid armies») etc.

This makes the scientific researches in the field of social security of the society to be guaranteed by the administrative mechanisms important. One of these mechanisms is «the theory of social security». The main element of this theory is the features of the social security category. This forms the scientific foundation to research the phenomenon of the social security.

We ask to consider the features the of the category «social security» in the theoretical area providing the possibility to form the applied basis for the research of the problems of the social security. The phenomenon of the social security is expressed in the specification of the security features in the activity of all subjects of law. Herewith independent of the object and the subject this category is not changed and is constant.

Information vision of social safety provides a definition of a place and role information in a global safety of society. One of the directions of social safety is an IT sphere. This sphere forms a subject, method, principles and system of information protection of society.

The permanency means the existence of the security together with the life category in time and space being typical for the society. The security actually surrounds the environment in the condition the things happen according to the current and applicable laws (natural, human), furthermore there are no differences of behavior or actions of the participants of the relations. In this case the security is the

abstract category of the environment existing beyond the will of the participants of the relations. The other variant of the permanency is specified by the related components «time – action» and means that the security exists in the specific limited time period as it is actual only for the future. There is no security in the past, provided that it is connected with the list of the events being the precondition for the specific dangers and provide the search of the sources of the danger situations combating.

The structural properties mean the occurrence of the separate security elements whose absence make this category abstract. Such elements include: the environment – the objective reality, rules namely procedures or actions of the participants of the relations, subjects, namely the participants and their action directed on the specific result, the predicted purpose of the actions and the probability of danger namely the departure from the predicted goal of actions.

The systemacity is the security as the specific procedure of the actions of the subjects of the relations to obtain the specific result. The system on the philosophy means the complex integral background which elements have more intensive internal relations than between these elements and the environment. The security system as the applied notion can have two variations: 1) the assembly of elements: the environment – subject – situation – standard (security); 2) interaction of several elements (opposite to each other) namely the condition of the environment (safe) – security standard – difference from the standard – action of the subject – condition of the environment (safe).

Alternativeness is the way to specify the security limits of the activity and the parameters of the possible differences in the activity specified. Alternativeness actual creates several variants of the decision to ensure security and variability is the selection of the most safe variant to achieve purposes or the least harmful variants to cope with the threat connected with the selection category as the category of the philosophy of existentialism as it is deepened in the world, is not intended for the specific purpose, it is always in the situation of selecting the variant of its action to ensure security although can not to understand it while overcoming threats and dangers.

Distinctness covers the ultimate purpose of the security category in real time as the safety matters can come to the category of threat in future. This feature is fully connected with the purpose category being specified as the image of the future result of the activity formed by the human consciousness and which a human strives to implement by its actions. The main purpose of the security is to remove threats either by the individual or the society in general. Herewith its perception by the human and the society can differ in specific indexes but the formation of the security as the integral event of the social life will be specified by the parameters specified by the bigger part of the society.

The specificity of the achievement provides the existence of the specific procedure of the danger or direct threat. Such problem provides not only the existence but also the active activity of the specific subjects in order to achieve the positive result being the renewal of the situation of the threat absence.

The efficiency means that the end result of the decision made is the practical result of the actions of the subject being the renewal of the safety of the specific environment but taking into account the possible differences during the implementation of the task in hand, i.e. the result can be different from the task in hand both positive and negative. The negative result is the transfer from the security status to the threat status (direct danger) and the positive is the decrease of the time period to cope with danger.

The statics provides that security as the status exists constantly but there is a possibility of indirect threats being nowadays understood by the subject as secure but further are transferred into the dangerous ones; herewith the subject can either understand it at the conscious level or do not understand it at all. The security is a part of life; it is also a longstanding and permanent notion of the specific field of the human's activity. It depends on the level of the individual perception and adoption to it by the subjects and the level of readiness to the situations of danger and threats.

The personal (individual) and collective (group) approach means that the social security as a rule is effective for the specific subject or a group of the subjects but even in case of the group approach each element of the group understand the notion of the security in its own way being determined by the individual

psychological, social and other property of the subject. Actually each person understands the security in view of the specific situation or activity but even under the same objective circumstances each separate subject individually specifies the security level in the specific time limit or situation due to the individual perception of the environment.

The forecasting provides that the specific subject or a group of the subject (society) plan its own activity and beforehand specify the possible limits of the result obtained specifying the future security parameters using the obtained practical skills even if the actions have no historical analogy.

Each element consists of two main parts: the external circumstance specified as the absence of the threats and dangers and the peculiarity of the subjective perception of the security as the integral part of modern life at all levels and in all developments.

As can be seen from the above there are two categories of the phenomenon of the social security in the society:

1. The passive category of the social security namely the social security as the specific status of the environment where the danger is absent. Herewith the participation of the subjects is not necessary or obligatory, the system provides the absence of the danger, threat or risk.

2. The active category of the social security namely the social security shows itself as the interaction with the antagonistic notions of «security», «threat» or «risk» and is characterized by the actions of the subjects of the society to achieve security and to manage the quality system to avoid danger, threats and risks.

Бортник Н.П. –
завідувач кафедри адміністративного та інформаційного права Навчально-наукового інституту права та психології Національного університету «Львівська політехніка», доктор юридичних наук, професор
Пєтков С.В. –
заступник директора з навчальної роботи Інституту права та післядипломної освіти Міністерства юстиції України, доктор юридичних наук, професор

ЗАГРОЗИ ІНФОРМАЦІЙНОМУ РЕСУРСУ ДЕРЖАВИ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ ТА НАЦІОНАЛЬНОЇ БЕЗПЕК

Однією з обов'язкових умов збереження інформаційного суверенітету держави є додержання режиму доступу інших держав до її інформаційних ресурсів.

Загрози інформаційному ресурсу держави зачіпають інтереси не лише інформаційної безпеки, але й її національної безпеки і повинні попереджуватися, блокуватися і нейтралізовуватися шляхом організаційно-правової структури системи інформаційної безпеки, що формує і реалізує державну політику в цій сфері, що сьогодні надзвичайно актуалізується у зв'язку з військовою агресією РФ на сході нашої держави.

Впровадження в усі сфери життєдіяльності особи, суспільства та держави інформаційних технологій зумовило поширення значної кількості інформації в обчислювальних та інформаційних мережах на значні території.

За відсутності вітчизняних конкурентоспроможних інформаційних технологій надається перевага технічним засобам обробки інформації та засобам зв'язку іноземного та спільного виробництва, які здебільшого не забезпечують захист інформації. Комунікаційне обладнання іноземного виробництва, яке використовується в мережах зв'язку, передбачає дистанційний доступ до його апаратних і програмних засобів, у тому числі з-за кордону, що створює умови для

несанкціонованого впливу на їх функціонування і контроль за організацією зв'язку та змістом повідомлень, які пересилаються.

За таких умов створилися можливості витоку інформації, порушення її цілісності та блокування. Витік інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, – це одна з основних можливих загроз національній безпеці України в інформаційній сфері.

Загрози безпеці інформації в Україні зумовлюються:

– невиваженістю державної політики в галузі інформаційних технологій, що може призвести до неконтрольованого та незаконного доступу до інформації та її використання;

– діяльністю інших держав, спрямованою на одержання переваги в зовнішньополітичній, економічній, військовій та інших сферах;

– діяльністю політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб, що спрямована на одержання переваг у політичній боротьбі та конкуренції;

– злочинною діяльністю, що спрямована на протизаконне одержання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним чи фізичним особам;

– використанням інформаційних технологій низького рівня, що призводить до впровадження недосконалих технічних засобів із захистом інформації, засобів контролю за ефективністю ТЗІ та засобів ТЗІ;;

– недостатністю документації на засоби забезпечення ТЗІ іноземного виробництва, а також низькою кваліфікацією технічного персоналу у сфері ТЗІ.

Без сумніву, шкода, нанесена державі в результаті реалізації загроз, так або інакше проектується на всіх або багатьох членів суспільства. Але існує низка загроз, реалізація яких може завдати шкоди конкретному громадянину, при цьому шкода може бути матеріальна, моральна, або навіть фізична.

Світова практика свідчить, що методи і засоби реалізації загроз інформаційній безпеці розвиваються випереджувальними

темпами, порівняно з методами і засобами захисту інформації. Загалом знаходить своє відображення діалектика розвитку нападу і захисту. Крім цього, відомо, що розробка технічних засобів, які реалізують достатньо значну кількість загроз, базуються, як правило, на найостанніших досягненнях науки, техніки і технології, тому засоби протидії, тобто технічні засоби інформаційної безпеки (засоби технічного захисту інформації), повинні створюватись виходячи із цих умов.

Однак, необхідно зазначити, що незважаючи на зростаючу зацікавленість до інформаційної безпеки, її специфічні особливості, достатня складність і висока вартість засобів технічного захисту, відсутність чітких критеріїв захищеності інформації тощо., обмежують практичне вирішення проблеми. Тому, для вирішення проблеми інформаційної безпеки, необхідна не проста розробка приватних механізмів захисту, а передусім розробка ідеології, методологічних основ захисту, які б могли враховувати не тільки перспективи розвитку інформаційних технологій і систем, але й перспективи розвитку спеціальних засобів реалізації загроз.

Однією з найважливіших теоретичних проблем, що мають першочергове значення, є проблема визначення рівнів захищеності для різних видів загроз. Причому, рівні захищеності, як критерій, повинні мати такий часовий параметр, як витривалість системи інформаційної безпеки до її подолання. Це дозволить рівнозначно зв’язати рівні захищеності з категоріями інформації, які у свою чергу, визначають необхідний час захисту інформації.

Горкуша М. Ю. –
Голова Аналітичного центру «Інтернет-право ЮА»

ПРОБЛЕМИ НОРМАТИВНОГО РЕГУЛЮВАННЯ ВСТАНОВЛЕННЯ ДОВІРИ ДО ЕЛЕКТРОННОГО ПІДПИСУ В УКРАЇНІ

Розвиток ІТ дозволяє створювати нові технологічні рішення та інструменти, які спрощують наше життя: як у виконанні простих буденних задач, так і у проведенні надзвичайно складних обчислень, моделювань та ін. Удосконалюються і елементарні процеси у здійсненні базових правовідносин, зокрема й у сфері ідентифікації. Та чи готові ми повноцінно імплементувати та використовувати в національній правовій системі сучасні ідентифікатори? Якщо так, то чи легко обґрунтувати їх використання у відповідності до законодавства?

Наразі, законодавець увів до електронної площини електронний підпис, електронний цифровий підпис, паспорт громадянина України у формі карти з безконтактним електронним носієм (та електронним цифровим підписом), а також, нещодавно, нормативно визначений регулятором – Національним банком України Bank ID. Законом України «Про електронну комерцію» також було введено «підпис одноразовим ідентифікатором», а також додатково визначено «аналог власноручного підпису» [2]. У дослідній експлуатації зараз знаходиться розробка ще одного ідентифікатора – Mobile ID, однак, законодавчо, він залишається неврегульованим, тому його повноцінне використання поки що неможливе.

Відомо, що першочергово категорія «аналог власноручного підпису» визначалась та регламентувалась у Цивільному кодексі України, статтею 207 встановлено, що «використання при вчиненні правочинів факсимільного відтворення підпису за допомогою засобів механічного, електронного або іншого копіювання, електронного підпису або іншого аналога власноручного підпису допускається у випадках, встановлених законом, іншими актами цивільного законодавства, або за письмовою згодою сторін, у якій мають

міститися зразки відповідного аналога їхніх власноручних підписів» [3]. Одночасно, Закон України «Про електронну комерцію», статтею 12 визначає види підписів у сфері електронної комерції, одним з яких є «аналог власноручного підпису (факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, іншого аналога власноручного підпису) за письмовою згодою сторін, у якій мають міститися зразки відповідних аналогів власноручних підписів» [2].

Зазначені визначення є абсолютно однаковими, різниця лише в співвідношенні «електронного підпису», який в Законі України «Про електронну комерцію» використовується в окремій категорії, і розкривається, відповідно до статті 12 закону так «якщо відповідно до акта цивільного законодавства або за домовленістю сторін електронний правочин має бути підписаний сторонами, моментом його підписання є використання: електронного підпису або електронного цифрового підпису відповідно до Закону України «Про електронний цифровий підпис», за умови використання засобу електронного цифрового підпису усіма сторонами електронного правочину» [1].

Суперечливим вбачається зазначення «умови», за якої всі сторони електронного правочину повинні використовувати засіб електронного цифрового підпису, тоді як в самій категорії описується абсолютно повноцінне та рівноправне застосування як «електронного підпису», так і «електронного цифрового підпису». Вимушені визнати, що тлумачення Цивільного кодексу України вбачається більш універсальним, бо і в відносинах з використанням «електронного підпису» прямо визначено можливість його використання в тому числі і за письмовою згодою сторін, що є ключовим для його застосування сторонами.

До того ж, у Цивільному кодексі України відображається вимога відображення у письмовій згоді сторін зразків відповідного аналога власноручного підпису, тоді як Закон України «Про електронну комерцію» не має такої вимоги, зазначаючи лише про обов'язковість домовленості сторін, використовуючи умову, яка унеможливлює безпосереднє

застосування електронного підпису. Зважаючи на це, пропонуємо викласти редакцію першого пункту частини 1 статті 12 Закону України «Про електронну комерцію» [2] у наступній редакції: «…електронного підпису або електронного цифрового підпису відповідно до Закону України «Про електронний цифровий підпис» за умови використання засобу електронного цифрового підпису усіма сторонами електронного правочину при підписанні домовленості (згоди) сторін, у якій мають міститися зразки відповідного аналога їхніх власноручних підписів».

Основна особливість використання електронного підпису полягає в тому, що при його застосуванні в документообігу не обов'язкова наявність третьої сторони, як у випадку з використанням електронного цифрового підпису (далі - ЕЦП), де присутній інший суб'єкт – центр сертифікації ключів (далі - ЦСК), відповідальний за справжність підпису в документі, підписаному за допомоги засобів ЕЦП, які ним постачаються. В той же час, питання довіри до того чи іншого ЦСК, який надає послуги ЕЦП вирішується наступним чином: кожен центр зобов'язаний пройти процедуру реєстрації, визначену законодавством, та засвідчити свій відкритий ключ у центральному засвідчувальному органі (далі - ЦЗО). В такому випадку, при перевірці сертифікату відкритого ключа підписанта, ми також і побачимо, що ЦСК, в якому було отримано ЕЦП для підписання документу, засвідчив свій відкритий ключ у ЦЗО, а отже йому можна довіряти, як і довіряти тому, що документ підписала зазначена в сертифікаті особа.

Однак, наразі активно розвиваються й постачальники послуг електронного підпису, особливо в міжнародному контексті. Використання цієї технології забезпечує формування домовленостей в правому полі, а також сприяє настанню юридично значущих наслідків, відповідно до укладених в електронній формі правочинів.

Характерно, що відповідно до Закону України «Про електронний цифровий підпис», а саме – за статтею 3 «електронний підпис не може бути визнаний недійсним лише

через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа».

При системному аналізі законодавства бачимо, що використовувати електронний підпис без супутнього підтвердження та визначення правовідносин, в яких він може використовуватись неможливе. Для застосування електронного підпису необхідні додаткові умови:

– випадок встановлено законом;

– іншими актами цивільного законодавства;

– письмова згода сторін, у якій мають міститись зразки відповідного аналога їхніх власноручних підписів;

– використання засобу електронного цифрового підпису усіма сторонами електронного правочину.

Таким чином, електронний підпис, сформований звичайним графічним відтворенням не може бути визнаний повноцінним та легальним аналогом власноручного підпису, не дивлячись на те, що сама електронна його природа, або відсутність посиленого сертифікату ключа не повинні бути підставою для визнання його недійсним. Використання електронного підпису, за такого законодавчого регулювання, є доволі ускладненим, та інакше неможливо сформувати підстави для довіри до електронного підпису.

Та технологія електронного підпису продовжує активно розвиватись. Наразі вже працюють сервіси, які допомагають встановити додаткові підстави довіри до особи, яка поставила на документі свій електронний підпис. В такому випадку, справжність електронного підпису перевіряється іншими сторонами правочину за раніше відомими ідентифікаторами, у відповідності до яких вони можуть ототожнити отриманий підпис з особою, яка вказана, за набором даних, доданих провайдером до електронного підпису.

Приміром, така перевірка може відбуватись за номером телефону, або електронною адресою, яка вказується при реєстрації в системі надавача послуги електронного підпису. Обов'язок провайдера – перевірити за допомогою спеціального посилання-активації профілю та одноразового смс-паролю

справжність вказаних додаткових ідентифікаторів, а також їх належність особі, яка створила екаунт в системі.

Далі – користувач відкриває документ, який необхідно підписати, відтворює (на сенсорному моніторі, або за допомогою інших засобів маніпуляції курсором) свій власний підпис, чи використовує збережений графічний шаблон, і надсилає повідомлення іншій особі про успішне підписання документу. Паралельно, підписаний документ, разом із графічним відтворенням власноручного підпису (електронним підписом), а також додатковою інформацією про особу-підписанта (електронною поштою, та іншою інформацією - опціонально), зберігається на сервері. Така ж процедура відбувається при підписанні документу усіма наступними особами.

За такої моделі, на сервері постачальника послуги зберігаються усі копії з електронними підписами осіб, яким було надано доступ до документу, а також підтвердження справжності – додатковими ідентифікаторами. Погодження використання такої моделі полегшує встановлення правовідносин між сторонами, і вони можуть завчасно домовитись про використання конкретно визначеного постачальника в спеціальній угоді, а згодом – вести документообіг виключно засобами встановленого постачальника.

Проте, відповідний ризик компрометації електронного підпису все ж залишається, хоч і складно уявити одночасний несанкціонований доступ і до електронної пошти особи, і до мобільного телефону, хоча, окремі сервіси реєструють користувачів у системах надання електронних підписів виключно на основі вказаної при реєстрації електронної пошти.

Список літератури

1. Про електронний цифровий підпис : Закон України від 22 травня 2003 р. № 852-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 276.

2. Про електронну комерцію : Закон України від 03 вересня 2015 р. № 675 VIII // Офіційний вісник України. – 2015. № 78. – Ст. 2590.

3. Цивільний кодекс України : Кодекс України від 16.01.2003 № 435-IV // Відомості Верховної Ради України. – 2003. – № 40. – Ст. 356.

Дніпров О.С. –
докторант кафедри адміністративного та інформаційного права Навчально-наукового інституту права та психології Національного університету «Львівська політехніка», кандидат юридичних наук

ІНФОРМАЦІЙНО-ПРАВОВІ ЗАСАДИ ГРОМАДСЬКИХ СЛУХАНЬ І ОБГОВОРЕНЬ

Затвердження Національної стратегії сприяння розвитку громадянського суспільства в Україні на 2016–2020 роки зумовлено необхідністю створення державою сприятливих умов для розвитку громадянського суспільства, різноманітних форм демократії, налагодження ефективної взаємодії громадськості з органами державної влади та органами місцевого самоврядування [1].

Сьогодні в зазначеній сфері діють постанова Кабінету Міністрів України від 03.11.2010 р. № 996 «Про забезпечення участі громадськості у формуванні та реалізації державної політики» та постанова Кабінету Міністрів України від 30.01.2013 р. № 61 «Питання проведення антидискримінаційної експертизи та громадської антидискримінаційної експертизи проектів нормативно-правових актів», розпорядження Кабінету Міністрів України від 27.03.2013 р. № 168-р «Про схвалення Концепції реалізації державної політики у сфері інформування та налагодження комунікації з громадськістю з актуальних питань європейської інтеграції України на період до 2017 року» [2; 3; 4].

Указ Президента України від 26.02.2016 р. № 68/2016 «Про сприяння розвитку громадянського суспільства в Україні» зазначає, що недосконаліть чинного законодавства створює штучні бар'єри для реалізації громадських ініціатив, розгляду та врахування громадських пропозицій органами державної влади та місцевого самоврядування, відсутній ефективний громадський контроль за діяльністю органів державної влади, органів місцевого самоврядування. Недостатньою є практика

залучення громадськості до формування та реалізації державної політики і вирішення питань місцевого значення [1].

В основу правових відносин у сфері громадського контролю покладено право на вільний доступ до інформації, якщо він необмежений на законній підставі. Відповідно, будь-яка суспільно значуща інформація, тобто та, що зачіпає інтереси суспільства, повинна бути доступна для осіб, які бажають брати участь в здійсненні процедур громадського контролю. Максимально повною мірою це може бути забезпечено впровадженням у сферу громадського контролю інформаційно-комунікаційних технологій.

Різноманіття форм громадського контролю дозволить охопити всі рівні та сфери діяльності органів державної влади та місцевого самоврядування, які потребують громадської участі. Особливості кожної форми гарантують участь широкого кола осіб, зацікавлених у розвитку процедур громадського контролю та отриманні суспільно значущої інформації.

Форма громадського контролю обирається суб'єктами вільно в залежності від об'єкта контролю, необхідних процедур, ступеня участі та кваліфікації представників громадянського суспільства.

Існуючі форми участі інститутів громадянського суспільства у громадському контролі охоплюють громадські слухання, громадську експертизу, громадські обговорення.

Відмінною особливістю громадських слухань є їх очний, а також одноразовий характер їх проведення. Присутність учасників може бути забезпечена за допомогою інформаційно-комунікаційних технологій. Детальна регламентація проведення громадських слухань на законодавчому рівні відсутня.

Постанова Кабінету Міністрів України від 25.05.2011 р. № 555 «Про затвердження Порядку проведення громадських слухань щодо врахування громадських інтересів під час розроблення проектів містобудівної документації на місцевому рівні» розкриває процедурні питання проведення громадських слухань, але концентрує увагу виключно на предметі обговорення проекту будівництва [5].

Термін «громадські слухання» без пояснення позначений в низці інших нормативно-правових актів України.

Метою проведення громадських слухань є виявлення громадської думки на теми, що виносяться на громадські слухання та доведення думки громадськості, зацікавленої у вирішенні певних питань до відома органів влади.

За підсумками громадських слухань готуються пропозиції та рекомендації з теми і питань, що виносяться на громадські слухання, які повинні бути обов'язковими до розгляду органами влади.

Координаційна рада з питань розвитку громадянського суспільства при Президенті України розглядає громадські слухання з позиції одного з механізмів взаємодії органів місцевої влади та місцевого самоврядування, пропонує рекомендації щодо удосконалення нормативно-правового регулювання цієї демократичної процедури на місцевому рівні [6].

Водночас, слід зауважити, що на законодавчому рівні вирішення цього питання не пропонується.

Нормативно-правове регулювання проведення громадських слухань і інших процедур контролю за діяльністю органів влади доцільно розглядати у контексті використання інформаційно-комунікаційних технологій у поєднанні з нормами конституційного, адміністративного та інформаційного права.

Такий підхід вирішить низку нагальних питань і дасть змогу об'єднати правові норми, закріплені у постановах Кабінету Міністрів України «Про забезпечення участі громадськості у формуванні та реалізації державної політики» та «Питання проведення антидискримінаційної експертизи та громадської антидискримінаційної експертизи проектів нормативно-правових актів» [2; 3].

Використання електронного майданчика в мережі Інтернет дає змогу проводити громадські обговорення у вигляді дистанційних дискусій з тривалим строком розгляду питань.

Використання різних Інтернет-ресурсів дає змогу прискорити процес доведення необхідної інформації до відома зацікавлених осіб та розширити доступ громадян до участі в них.

З правової точки зору, особливість громадських обговорень як форми громадського контролю полягає у

характері інформаційного обміну, закладеного в інформаційно-правову природу цього інституту.

Беручи участь в такій формі громадського контролю, громадянин реалізує своє право на інформацію передбачене Конституцією України, Законами України від 02.10.1992 р. № 2657-XII «Про інформацію» та від 13.01.2011 р. № 2939-VI «Про доступ до публічної інформації».

Механізм інформаційного обміну думками та пропозиції громадян стають надбанням державних органів, які отримують уявлення про реальний стан обговорюваного в суспільстві питання.

Ці пропозиції повинні знайти своє відображення при прийнятті рішення, хоча нормативно-правовий механізм реалізації пропозицій, отриманих у ході громадських обговорень, детально не досліджено.

Сьогодні правову конструкцію громадських обговорень визначено в різних нормативних правових актах різних сфер правового регулювання. Це питання екології, науки, регуляторної діяльності та інших сфер правового регулювання.

Прийняття Закону України від 02.07.2015 р. № 577-VIII «Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції» дають змогу, у контексті моніторингу нормативно-правових актів, узагальнити отриманий досвід і розглянути його як можливу нормативну базу для правового регулювання питань громадських слухань і громадських обговорень з використанням інформаційно-комунікаційних технологій [7].

Такий підхід відповідає впровадженню в Україні Ініціативи «Партнерство «Відкритий Уряд» [8].

Доцільно зазначити, що громадські обговорення як форма громадського контролю не можуть здійснюватися органами виконавчої влади. Їх участь можлива в частині організації проведення таких слухань. Крім того, як вже зазначалося вище, сьогодні законодавство про організацію проведення громадських обговорень відсутнє.

Результатом громадських слухань і громадських обговорень може стати громадська ініціатива, що має на меті скасування, доповнення чи зміну діючого або прийняття нового

нормативного або правозастосовного акта. Мета формування механізму громадської ініціативи – розширення можливих форм реалізації права громадян України на участь в управлінні справами держави шляхом появи нового інформаційного каналу, яким громадянське суспільство могло б висловлювати свою думку з конкретних питань і гарантувати реакцію державних органів на цю інформацію.

Список літератури

1. Про сприяння розвитку громадянського суспільства в Україні: Указ Президента України від 26.02.2016 р. № 68/2016 // [Електронний ресурс]. – Режим доступу: [http://zakon5.rada.gov.ua/laws/show/68/2016/paran20#n20].
2. Про забезпечення участі громадськості у формуванні та реалізації державної політики: Постанова Кабінету Міністрів України від 03.11.2010 р. № 996 // [Електронний ресурс]. – Режим доступу: [http://zakon5.rada.gov.ua/laws/show/996-2010-%D0%BF].
3. Питання проведення антидискримінаційної експертизи та громадської антидискримінаційної експертизи проектів нормативно-правових актів: Постанова Кабінету Міністрів України від 30.01.2013 р. № 61 // [Електронний ресурс]. – Режим доступу : [http://zakon5.rada.gov.ua/laws/show/61-2013-%D0%BF].
4. Про схвалення Концепції реалізації державної політики у сфері інформування та налагодження комунікації з громадськістю з актуальних питань європейської інтеграції України на період до 2017 року: Розпорядження Кабінету Міністрів України від 27.03.2013 р. № 168-р // [Електронний ресурс]. – Режим доступу : [http://zakon3.rada.gov.ua/laws/show/168-2013-%D1%80].
5. Про затвердження Порядку проведення громадських слухань щодо врахування громадських інтересів під час розроблення проектів містобудівної документації на місцевому рівні: Постанова Кабінету Міністрів України від 25.05.2011 р. № 555 // [Електронний ресурс]. – Режим доступу: [zakon.rada.gov.ua/ laws/show/555-2011-п].
6. Правове регулювання громадських слухань / Координаційна рада з питань розвитку громадянського суспільства при Президенті України. Офіційний сайт // [Електронний ресурс]. – Режим доступу : [http://civil-rada.in.ua/?p=2081].
7. Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції: Закон України від 02.07.2015 р. № 577-VIII // Відомості Верховної Ради України. – 2015. – № 35. – Ст. 341.
8. Про схвалення плану дій з впровадження в Україні Ініціативи «Партнерство «Відкритий Уряд»: Розпорядження Кабінету Міністрів України від 05.04.2012 р. № 220-р // [Електронний ресурс]. – Режим доступу: [http://zakon3.rada.gov.ua/laws/show/220-2012-%D1%80].

Єсімов С.С. –
доцент кафедри права адміністративного та інформаційного права Навчально-наукового інституту права та психології Національного університету «Львівська політехніка», кандидат юридичних наук, доцент

ЮРИДИЧНА ПРИРОДА ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Реформи правоохоронної системи України наближають структури, які входять до складу правоохоронних органів, до європейської моделі діяльності у сфері захисту прав і свобод людини та громадянина, забезпеченні публічної безпеки, законності та правопорядку, боротьби зі злочинністю. Європейська модель показує високий рівень ефективності діяльності правоохоронних структур. Різноманітність функцій і завдань, що вирішуються в процесі діяльності поліції, обстановки і умов, в яких вона протікає, обумовлює застосування різних форм діяльності.

Закон України «Про Національну поліцію» виділив як один з напрямів діяльності – інформаційно-аналітичну діяльність.

Різноманітність функцій і завдань, що вирішуються в процесі функціонування системи МВС України, обумовлює застосування різних форм діяльності.

З погляду на дослідження польського вченого Е. Старосьцяка, у правовому сенсі термін «форма діяльності» розуміється як дозволений або врегульований правом спосіб діяльності поліції в конкретній роботі [1, с. 30].

В. Авер'янов, В. Селіванов, В. Семчик, В. Сіренко, В. Цвєтков у *науковому виданні «Совершенствование аппарата государственного управления. Конституционный аспект»,* яке вийшло у світ у 1982 році, обґрунтували підхід до визначення форм управлінської діяльності як зовнішнього організаційно-правового вираження конкретних, однорідних дій, що здійснюються з метою практичного здійснення функцій [2, с.21].

Проте в літературі висловлювалася дискусійна думка щодо класифікації інформаційної діяльності в разі конкретизації змістовної характеристики діяльності з предметної сфери. Водночас класифікатори видів інформаційної діяльності на даний час не конкретизують її галузь в одному конкретному галузевому або міжгалузевому сегменті, що, на нашу думку, характеризується математичним механізмом аналізу інформаційного масиву даних, який у більшості випадків не залежить від об'єкту дослідження. Даний підхід зумовлено науковими дослідженнями академіка В. Глушкова [3].

З погляду на дослідження Р. Калюжного, у функціональному, змістовно-цільовому аспекті діяльність структурується за програмними цілями і операціями, через систему яких досягається певна мета [4, с. 58].

Найбільш значущі види інформаційної діяльності за програмними цілями представлені у Законі України «Про інформацію» [5]. Це діяльність з одержання, використання, поширення, зберігання, захисту інформації законним способом. Важливо відзначити, що простежується тенденція трансформації терміна «інформаційне забезпечення» (наприклад, постанова Кабінету Міністрів України від 26.09.1994 № 663 «Про інформаційне забезпечення участі громадян України у приватизаційних процесах» не чинна з 2001 року) під яким розуміється діяльність уповноважених суб'єктів, зв'язана з наданням, отриманням, обробкою та розміщенням відповідної інформації своєчасно і в установленому порядку (наприклад, постанова Кабінету Міністрів України від 04.01.2002 № 3 «Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади»).

У структуру діяльності поліції поряд з цілями, мотивами включають способи та прийоми здійснення.

За висловлюванням В. Глушкова структура інформаційно-аналітичної діяльності повинна включати інформаційне забезпечення, інформаційно-аналітичну роботу, створення баз даних, що включає інформаційний пошук, цілі, мотиви, способи та прийоми їх здійснення [6].

На думку авторів навчального посібника В. Захарової, В. Філіпової «Основи інформаційно-аналітичної діяльності» інформаційно-аналітична діяльність є продукт інтелектуальних, творчих загально цивілізаційних тенденцій, що характеризують розвиток людства направлений на формування пріоритетів стійкого розвитку цивілізації та інформатизації [7].

Стаття 25 «Повноваження поліції у сфері інформаційно-аналітичного забезпечення» Закону України «Про Національну поліцію» передбачає, що поліція в рамках інформаційно-аналітичної діяльності: формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; здійснює інформаційно-пошукову та інформаційно-аналітичну роботу; користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади [8].

У зв'язку з цим необхідно звернути увагу на те, що аналітична складова інформаційно-аналітичної діяльності спирається на герменевтичні методи, що включають інтерпретацію документів, аналіз існуючих концепцій, пропозицій і теорій з застосуванням інструментарію формування математичного моделювання (англ. *Mathematical simulation*), використовуючи статичні (для опису оперативної обстановки) та динамічні (для опису результатів діяльності територіальних органів Національної поліції) моделі.

Розвиток інформаційно-аналітичної діяльності зумовив появу інформаційно-аналітичних підрозділів, практично за всіма напрямами діяльності, пов'язаної з інформаційними процесами, зокрема, з обробкою потоків інформації з метою прийняття оптимальних управлінських рішень.

Для вирішення питань впровадження інформаційно-аналітичної діяльності в органах виконавчої влади у 2000 році була створена Урядова комісію з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади (постанова Кабінету Міністрів України від 07.05.2000 № 777), яка проіснувала до схвалення Стратегії розвитку інформаційного суспільства в Україні (розпорядження Кабінету Міністрів України від 15.05.2013 № 386-р «Про схвалення Стратегії розвитку інформаційного суспільства в Україні»).

З концептуально-теоретичних позицій доцільно виділити ряд важливих особливостей інформаційно-аналітичної діяльності поліції, які мають істотне значення для інтеграції у європейські поліцейські структури.

Базовими елементами та засобами реалізації інформаційно-аналітичної діяльності виступають інформаційні системи, системи зв'язку та передачі даних, сучасна інформаційно-телекомунікаційна інфраструктура, бази даних правової інформації, технічні, програмні, лінгвістичні, правові, організаційні засоби. Це знайшло відображення у статтях 25, 26, 27 Закону України «Про Національну поліцію» [8].

З одного боку, інформаційно-аналітична робота дозволяє виявити і пізнати закономірності, у контексті кримінологічних досліджень (злочинність, порушення громадського порядку, дорожньо-транспортні пригоди і ін.).

З іншого боку, інформаційно-аналітична робота відображає результати повсякденної діяльності поліції з протидії негативним соціальним явищам. Це охоплює аналіз стану злочинності та охорони громадського порядку за певний проміжок часу, вивчення ефективності та практичної доцільності конкретної форми роботи, її нормативно-правове регулювання, що застосовується у протидії порушенням правопорядку, боротьбі зі злочинністю, за напрямами діяльності поліції визначеними законодавством України.

О. Негодченко, досліджуючи методологічні основи діяльності штабів (у даний час підрозділи організаційно-аналітичного забезпечення та оперативного реагування [9]) щодо побудови інформаційно-аналітичних систем і систем обліку, планування та контролю даних, розгадає ці явища з позиції кібернетики (наука про загальні закони одержання, зберігання, передавання й перетворення інформації у складних системах управління, за визначенням В. Глушкова [10]) для вирішення завдань побудови оптимальної інформаційно-аналітичної системи [11, с. 31].

Водночас, одними з найважливіших умов створення та функціонування ефективних інформаційно-аналітичних систем є:

– систематизоване накопичення знань поліцейськими про об'єкти управління в процесі виконання своїх професійних (посадових) обов'язків;

– створення нового класу інформації з уже існуючих класів шляхом залучення інформації від нижнього до вищого рівня управління;

– можливість декомпозиції інформації, що дозволяє замінити вирішення завдання рішенням серії менших взаємопов'язаних завдань на нижній рівень управління.

У даний час окремі завдання вирішуються за допомогою Інтегрованої інформаційно-пошукову систему органів внутрішніх справ України [12].

Для ефективної реалізації цих функцій в рамках окремо взятого територіальному органу поліції, потрібні об'єктивно встановлені та закріплені критерії збору інформації, встановлений порядок її обробки. Доцільно зауважити, що технологія збору і обробки даних повинна охоплювати усі напрями діяльності складових елементів системи Національної поліції, визначені Законом України «Про Національну поліцію», та складових системи МВС України (Державної служби України з надзвичайних ситуацій, Державної міграційної служби України, Державної прикордонної служби України, Національної гвардії України [13]), індикатори оцінки достовірності, релевантності, інших зовнішніх і внутрішніх властивостей зібраної і обробленої інформації.

Оптимізація вирішення завдань пошуку, відбору та систематизації інформації, необхідної в діяльності поліції, базується на конструкті єдиного інформаційного простору системи МВС України, який логічно визначити як сукупність спеціалізованих баз і банків даних, технологій їх ведення та використання, інформаційно-телекомунікаційних систем і мереж, суб'єктів інформаційно-аналітичної діяльності, які функціонують на основі єдиних принципів і за загальними правилами забезпечують інформаційну взаємодію системи Міністерства внутрішніх справ України і громадян [14].

Системо утворюючими компонентами єдиного інформаційного простору є:

– інформаційні ресурси, що містять дані, відомості і знання, зафіксовані на відповідних носіях інформації;

– організаційні структури, що забезпечують функціонування та розвиток єдиного інформаційного простору, зокрема, збір, обробку, зберігання, поширення, пошук і передачу інформації, об'єднання різних мереж, систем і комплексів засобів зв'язку;

– засоби інформаційної взаємодії громадян з системою Міністерства внутрішніх справ України України та доступу в певному правовому режимі до інформаційних ресурсів на основі відповідних інформаційних технологій.

Очевидно, що функціонування єдиного інформаційного простору сприяє суттєвому розширенню інформаційної бази, необхідної для інформаційно-аналітичної діяльності, зниженню витрат на процеси пошуку, обробки, зберігання та відбору вихідної інформації, виявлення тих аспектів, в рамках яких слід здійснювати аналітичну обробку інформації, виявлення суті та динаміки просторово-часових і причинно-наслідкових зв'язків між досліджуваними фактами, явищами, процесами. У результаті спочатку наявні дані перетворюються в нову інформацію про стан злочинності та результати оперативно-службової діяльності поліції, оперативно-довідкову, розшукову, криміналістичну, архівну, науково-технічну і іншу інформацію більш високого порядку, яка дозволяє приймати обґрунтовані оперативні і управлінські рішення, здійснювати координацію та взаємодію.

В аналітичній доповіді Національного інституту стратегічних досліджень «Національний інформаційний простір України: проблеми формування та державного регулювання» вказується: «Недостатня ефективність органів державної влади зумовлена низькою координованістю їх діяльності, частковим дублюванням повноважень, а також невідповідністю напрямів їх регулювання конвергентним процесам в інформаційно-комунікаційній сфері» [15, с. 22].

У ракурсі зазначеного та з ураховуючи вище викладеного доцільно відомчим нормативно-правовим актом Міністерства внутрішніх справ України визначити порядок інформаційної

взаємодії між Національною поліцією та Департаментом аналітичної роботи і організації управління МВС України, територіальними органами Національної поліції та відповідними підрозділами організаційно-аналітичного забезпечення та оперативного реагування. Форма реалізація можлива у вигляді Державної цільової науково-технічної програми створення державної інтегрованої інформаційної системи забезпечення управління в системі МВС України або відомчій цільовій науково-технічній програмі. Указаний підхід до організації інформаційного обміну відповідає положенням Стратегії кібербезпеки України. Здійснення заходів сприятиме адаптації національної правової бази діяльності поліції у сфері інформаційно-аналітичного забезпечення до стандартів Європейського Союзу, що передбачено у статті 22 «Боротьба зі злочинністю та корупцією» Розділу ІІІ «Юстиція, свобода та безпека» Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони.

Список літератури

1. Старосьцяк Е. Правовые формы административной деятельности / Е. Старосьцяк; перев. с польского Махненко А. Х. – М.: Госюриздат, 1959. – 330 с.

2. Совершенствование аппарата государственного управления. Конституционный аспект / Аверьянов В. Б., Селиванов В. Н., Семчик В. И., Сиренко В. Ф., и др.; под общ. ред.: Цветков В. В. – *К.*: Наук. думка, 1982. – 375 с.

3. Енциклопедія кібернетики / Відпов. ред. Глушков В. М. – Т.1 (А-Л). – К.: Вид-во УРЕ, 1973. – 584 с.

4. Калюжний Р. А. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики : монографія / Р. А. Калюжний, В. О. Шамрай, М. Я. Швець та ін. ; за ред. Р. А. Калюжного, В. О. Шамрая. – К : Акад. ДПС України, 2002. – 296 с.

5. Про інформацію: Закон України від 02.10.1992 № 2657-XII // Відомості Верховної Ради. – 1992. – № 48. – Ст.650.

6. Енциклопедія кібернетики / Відпов. ред. Глушков В. М. – Т.2 (М-Я). – К.: Вид-во УРЕ, 1973. – 576 с.

7. Захарова В. І. Основи інформаційно-аналітичної діяльності / Захарова В. І., Філіпова В. Я. – К.: «Центр учбової літератури», 2013. – 336 с.

8. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради. – 2015. – № 40-41. – Ст.379.

9. Наказ МВС України від 22.01.2016 № 39 «Про затвердження Типового положення про управління організаційно-аналітичного забезпечення та оперативного реагування головних управлінь Національної поліції України в Автономній Республіці Крим та м. Севастополі, областях, м. Києві». [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/z0216-16/paran7#n7

10. Кібернетика. [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B8%D0%BA%D0%B0

11. Негодченко О. В. Завдання та функції штабів органів внутрішніх справ щодо інформаційно-аналітичного забезпечення діяльності органів внутрішніх справ / О. В. Негодченко // Наук. вістник Херсон. держ. ун-ту. – 2015. – Вип. 3. – Т 5. – С.31-35.

12. Наказ МВС України від 12.10.2009 № 436 «Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України». [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/z1256-09

13. Постанова Кабінету Міністрів України від 28.10.2015 № 878 «Про затвердження Положення про Міністерство внутрішніх справ України». [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/878-2015-%D0%BF

14. Наказ МВС України від 26.09.2013 № 920 «Про затвердження Порядку організації доступу до інформаційних ресурсів під час інформаційної взаємодії між Міністерством внутрішніх справ України, Державною міграційною службою України та Державною прикордонною службою України». [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/z1771-13

15. Конах В. К. Національний інформаційний простір України: проблеми формування та державного регулювання : аналіт. доп. / В. К. Конах. – К.: НІСД, 2014. – 76 с.

Жаровська І.М. –
професор кафедри теорії та філософії права
Навчально-наукового інституту права та психології
Національного університету «Львівська політехніка»,
доктор юридичних наук

ІНФОРМАТИЗАЦІЇ У СФЕРІ ПРАВОВИХ ЗНАНЬ

Вплив таких процесів, як формування та реконструкція міжнародного простору, інформатизація, регіоналізація, а також геополітичні процеси, що відбуваються сьогодні на тлі глобалізації міжнародного простору, надають особливої гостроти проблемі інформатизації у сфері правових знань.

Рівень доступності законодавчих норм – один з найважливіших показників правової культури будь-якого суспільства, що здатний впливати на функціонування всіх елементів механізму соціальної дії права. Він визначається не тільки станом самих правових норм, їх систематизованістю, простотою і так далі, але й факторами, що знаходяться у сфері правової культури особистості, функціонуванням каналів правового інформування громадян. На сьогодні не достатньо класичних моделей правового інформування. Правова освіта в демократичній державі розширює свій потенціал шляхом імплементації новітніх інформаційних засобів у процес інформування громадськості.

В сучасних умовах, правова освіта населення полягає у здійсненні комплексу заходів виховного, навчального та інформаційного характеру, спрямованих на створення належних умов для набуття громадянами обсягу правових знань та навичок у їх застосуванні, необхідних для реалізації громадянами своїх прав і свобод, а також виконання покладених на них обов’язків.

Освіта повинна бути орієнтованою на ретрансляцію способів розуміння дійсності: мислення, діяльності, спілкування, поведінки. При цьому навчання передбачає накопичення теоретичних і практичних правових знань, навичок. Навчання сприяє розвитку загальнокультурних параметрів особи. Правова освіта впливає на становлення

правового життя суспільства, а також формує соціально-правову активність членів суспільства. Вона повинна складатися з: системного, планомірного впливу на особу з метою доведення до її свідомості системи правових цінностей, норм, принципів; забезпечення сприятливого впливу середовища; створення належних умов для інтенсивного засвоєння особою норм і принципів права, що діють у суспільстві; викорінення із свідомості громадян негативного ставлення до оточуючого світу; залучення підлітків в суспільно-практичну діяльність, що сприяє формуванню у них потреби у правових знаннях; закріплення і перетворення останніх в переконання, а також забезпечення правомірної поведінки і росту правової активності [1, с.121].

Правова освіта вміщує процес отримання та засвоєння знань про основні категорії держави і права, виховання у громадян поваги до закону, прав людини, небайдужого ставлення до порушень законності і правопорядку. Правова освіта – необхідний елемент правової культури, умова правової вихованості особи.

Значення юридичної освіти для нашої країни актуалізується у зв’язку з політико-правовими реформами. Нові соціально-економічні умови суттєво загострюють традиційну проблему освіти - пошук ідеалів, які могли б бути покладені в основу найважливішого компонента будь освітньо-виховної системи, визначення мети. Цільовий компонент освітньої системи визначає конкретику засобів досягнення цих цілей, критерій оцінки отриманих результатів, можливі корекції самого ходу освітньо-виховного процесу. В умовах модернізації права та юридичної освіти питання про формування правової культури, правосвідомості, ціннісних орієнтацій набуває особливого значення.

Громадськість отримує широкий доступ до інформаційних мереж, таким чином забезпечується можливість отримання правових знань, що спричиняє підвищення рівня правової освіти. Зокрема громадяни мають можливість використовуючи інформаційні ресурси отримати доступ до наочних трансляцій засідань парламенту, уряду, органів місцевого самоврядування, таким чином забезпечується зв'язок між владними структурами та

громадськістю. Особливо позитивно оцінюємо роботу щодо обов'язковості веб порталів органів державної влади різних рівнів. Ми вважаємо, електронні сторінки володіють цілим рядом переваг по деяких розуміннях: вони не дорогі; вимагають мінімальних зусиль; дозволяють постійно обновляти інформацію; доступні для необмеженого числа громадян без значних витрат; інформація може перейматися засобами масової інформації; дозволяють проводити опитування й обговорення в режимі он-лайн ідей і аргументів опонентів; спрощують обмін інформацією і взаємодії різних державних структур; забезпечують абсолютну транспарентність діяльності і процесу прийняття рішень; сприяють створенню об'єктивного позитивного іміджу даної структури на внутрішніх і зовнішніх зв'язках.

Інформаційні технології надають можливість громадськості активніше брати участь в управлінні державними справами. В першу чергу це можливо використовуючи систему «Good Governance». ООН визначила принципи такого врядування: участі, яка може бути як безпосередньою, так і опосередкованою через легітимізовані посередницькі інституції та представників; верховенства права, тобто правова система повинна бути справедливою і діяти однаково для всіх, особливо стосовно прав людини; прозорості, через свободу інформації, її повноту і доступність для всіх, хто в ній зацікавлений; відповідальності, оскільки інституції та процеси служать усім членам суспільства; консенсусу, дотримання балансу інтересів для досягнення широкого консенсусу з локальних і загальних питань та процедур; справедливості, добробут суспільства залежить від врахування інтересів кожного члена суспільства у ньому; ефективності та результативності, максимально ефективне використання ресурсів для задоволення потреб громадян; підзвітності уряд, приватний бізнес та структури громадянського суспільства підзвітні громадськості та інституційним носіям прав; стратегічного бачення лідери та громадськість мають довготермінову перспективу щодо Good Governance і людського розвитку і чітко уявляють собі ці заходи, які необхідні для їх реалізації є основні принципи такого врядування [2].

Важливо, що врядування на відміну від деяких інших форм забезпечує можливість громадян здійснювати публічну діяльність

у всіх сферах та на усіх етапах прийняття нормативно-публічного рішення. На первинному етапі проходить розповсюдження інформаційного ресурсу через створення мережі офіційних веб-порталів, у відкритому обігу є система діловодства, поширюються електронні оголошення та роз'яснення. Наступним етапом є забезпечення комунікативних відносин між органами публічної влади і громадськістю, що забезпечується шляхом електронних чатів, звернень, форумів та пошти, рідше застосовуються відеоконференції. Важливим етапом є електронне консультування, що проводиться через електронні опитування, голосування, електронні ініціативи та петиції. Також електронне врядування забезпечує важливу діяльність у сфері надання публічних послуг від можливості оплати комунальних послуг до голосування на виборах за допомогою мережі Інтернет.

Однак, не дивлячись на певні зрушення та новітні перспективи щодо удосконалення правової освіти громадськості, все ж залишається ряд не вирішених проблем, тому правова політика держави повинна першочергово повинна спрямовуватися:

– на підвищення рівня правової підготовки населення, насамперед учнівської та студентської молоді, громадян, які перебувають на державній службі, обрані народними депутатами України, депутатами місцевих рад, викладачів правових дисциплін та журналістів, які висвітлюють правову тематику;

– створення належних умов для набуття громадянами знань про свої права, свободи і обов´язки;

– широке інформування населення про правову політику держави та законодавство;

– забезпечення вільного доступу громадян до джерел правової інформації;

– вдосконалення системи правової освіти населення, збереження та розвиток вітчизняних традицій у цій сфері.

Список літератури

1.Рабинович П. М. Основы общей теории права и государства / П. М. Рабинович. – Харьков: Консум, 2005. – 317 с.

2.Governance for sustainable human development: A UNDP policy document [Electronic resourse] : United Nations Development Program (January, 1997). – Access mode : http://magnet.undp.org/policy/default.htm.

Золотар О. О. –
головний науковий співробітник
Науково-дослідного інституту інформатики і права
Національної академії правових наук України,
кандидат юридичних наук,
старший науковий співробітник

ПРАВА І СВОБОДИ ЛЮДИНИ: ІНФОРМАЦІЙНИЙ ВИМІР

Хоча і концепція прав людини, і концепція інформаційного суспільства починали з рівня наукових гіпотез, які від моменту свого зародження і до сьогодні зазнають змістовної критики, все ж шляхом міжнародно-правової легалізації вони виведені на рівень політико-правої дійсності. А їх симбіоз породив феномен інформаційних прав людини. Іноді здається, що інформаційних прав до винайдення комп'ютерів і Інтернету не було. Проте, один із засновників постмодернізму Жан Бодрійяр дав наступну оцінку інформаційного вибуху, який стався десь в 60-ті – 70-ті роки: «інформації стає все більше і більше, а сенсу – все менше і менше» [1, 22].

І ось тепер маємо і категорію «цифрових прав», і кібербезпеку, і віртуальну землю у реальному володінні з усіма похідними. Проте незалежно від цього людина тяжіє до становлення як особистості і зайняти належне їй місце в суспільстві, де будуть гарантовані її права і свободи, створено можливості для їх реалізцації.

Ще у 1946 році Генеральна Асамблея Організації Об'єднаних Націй ухвалила одну зі своїх найперших резолюцій, де зазначено таке: «*Свобода інформації є фундаментальним правом людини і … критерієм для всіх свобод, яким присвячено Організацію Об'єднаних Націй*»[2, с. 8]. Тому актуальність питання інформаційної безпеки людини визначається, насамперед, в контексті концепції природного права. При цьому природне право людини постає як усвідомлена нею можливість і необхідність жити, бути вільною, щасливою та вимагати від держави й суспільства сприяння реалізації своїх прав у межах, визначених принципами співжиття соціуму.

Конституції більшості демократичних і не лише держав в один голос «співають» про пріоритетність людини як основної соціальної цінності. А гарантування її прав і свобод – основне завдання. У сучасному світі, коли проблема прав людини вийшла далеко за межі окремої держави, а обсяг прав і свобод людини в сучасному суспільстві визначається не лише особливостями певного співтовариства людей – національної держави, а й розвитком людської цивілізації в цілому.

То що ж ми маємо: нове, четверте, покоління – права людини в інформаційній сфері чи новий інформаційний вимір прав і свобод людини?

Розробка «Декларації прав людини і правових норм в інформаційному суспільстві»[3] стала першою спробою визначення правових рамок в цій сфері. Декларація була розроблена Комітетом експертів Ради Європи з інформаційного суспільства. Основна увага на форумі було присвячено розробці норм відповідальної поведінки в інформаційному суспільстві. Експерти розглянули, яким чином різні дійові особи, включаючи уряд, приватні компанії, ЗМІ та неурядові організації можуть співпрацювати задля поваги до прав людини. Учасники Міжнародного форуму «Права людини в інформаційному суспільстві: відповідальна поведінка головних дійових осіб» ініційованого Радою Європи, закликали уряди захищати всі права людини, які стосуються інформаційного суспільства, від свободи слова до приватності і копірайту, не забуваючи про завдання подолання інформаційної нерівності і про належне управлінні. На їхню думку, «цілковита повага свободи слова та інформації державними та недержавними інститутами є необхідною передумовою побудови вільного інформаційного суспільства для всіх, а інформаційно-комунікаційні технології не повинні використовуватися для обмеження цієї фундаментальної свободи» [4].

Розділ «Права людини в інформаційному суспільстві» Декларації містить 8 пунктів:

– Право на свободу вираження, інформації та комунікацій;

– Право на повагу до приватного життя і таємниці листування;

– Право на освіту і загальний доступ до інформаційних технологій;

– Заборона рабства і примусової праці;

– Право на неупереджений суд і заборону на позасудове переслідування;

– Захист власності;

– Право на вільні вибори;

– Свобода зібрань [3].

Як можемо бачити – переважна більшість – це права, які вважалися базовими і до становлення інформаційного суспільства.

Власне, **завданням** цієї доповіді є розкриття інформаційного виміру так званих традиційних прав або прав і свобод трьох перших поколінь – особистих, політичних, економічних, соціальних, екологічних тощо..

Основоположне право людини – право на життя. Його зміст відомий кожному – містить позитивну і негативну складову, а також кореспондуючий обов'язок держави і суспільства. В розумінні цього права на сьогодні величезна кількість дискусій від його часових меж до питань щодо супутніх репродуктивно-генетичних прав. Що ж нового відбувається в інформаційному суспільстві з цим правом?

Хочу нагадати чи можливо ознайомити з справою Меган Майєр [5]. У 2006 році в маленькому американському містечку посварилися дві 13-річні школярки – Меган Майєр і Сара Дрю. Мати однієї з дівчаток сприйняла цю сварку близько до серця і вирішила встановити стеження за колишньою подругою дочки. Вона не стала наймати для цього приватних детективів, а просто створила в соціальній мережі MySpace аккаунт від імені симпатичного 16-річного хлопця на ім'я Джош Ивенс, який втерся в довіру до простодушної Меган Майєр і незабаром завів з нею роман. Лорі писала від імені Джоша втрьох з 13-річною Сарою і зі своєю молодою підпорядкованої на роботі Ешлі Грілс. Одного дня міфічний Джош, який зумів до того моменту підкорити серце провінційної школярки, раптом почав її всіляко ображати, принижувати і прямо порадив дівчинці позбавити світ від своєї присутності. У той же день Меган Майєр наклала на

себе руки, повісившись у шафі. І ФБР, розслідуючи обставини її самогубства, відразу вийшло на слід віртуального Джоша Івенса, чий рада привів до загибелі дівчинки.

Судова епопея 49-річної американської продавчині Лорі Дрю, яка на смерть зацькувала однокласницю дочки за допомогою соціальної мережі MySpace, завершилась передбачувано. Присяжні, під впливо природніх людських почуттів, визнали її винною за трьома пунктами пред'явленого їй звинувачення. А федеральний суддя Джордж Ву, який головував на процесі, керуючись буквою закону, скасував їх вердикт, звільнивши Лорі Дрю від будь-якої відповідальності за вчинене.

Лорі Дрю звинуватили в несанкціонованому доступі до комп'ютерних мереж на тій підставі, що вона зареєструвалася в MySpace, використовуючи вигадане ім'я, і тим самим порушила правила використання цієї соцмережі. Покарання за кожним з трьох пунктів звинувачення могло скласти до трьох років в'язниці і штраф до 300 000 доларів. Широкій публіці, волю якої в даному випадку виконували і обвинувачі, і присяжні, такий результат здавався справедливим. Але ні американські юридичні експерти, ні професійний суддя не могли погодитися з подібним трактуванням «несанкціонованого доступу».

Відповіддю на цю колізію став внесений до Конгресу США законопроект HR1966, що передбачає відповідальність за «кіберцькування» (cyberbullying)[6]. Перспективи його прийняття в нинішньому вигляді вельми сумнівні: визначити межу між злочинним «цькуванням» і свободою висловлювання для американського законодавця ніколи не було легким завданням. А навіть якщо і приймуть такий закон, проблему, що спонукала до його створення, він все одно не вирішить.

В чинному українському законодавстві є норма за доведення до самогубства ст. 120 КК – Доведення особи до самогубства або до замаху на самогубство, що є наслідком жорстокого з нею поводження, шантажу, примусу до протиправних дій або систематичного приниження її людської гідності. Немає потреби в створенні нового законодавства. Але чи можливо було б реальне доведення справи до вироку за цією нормою?

Відразу звернемо увагу на наступне – право на честь і гідність. При тому в його специфічному вияві – посмертно. На прикладі справи Ніккі Катсурас [7], дівчини, що в 2006 році загинула у автокатастрофі у штаті Каліфорнія, США. Її тіло було жахливим чином скалічене. В інтересах слідства поліція зробила декілька фотографій місця аварії. Декілька співробітників вирішили налякати своїх друзів на Хелоуін і надіслали їм зроблені фото. Знімки швидко поширилися Інтернетом, і батьки дівчини звернулися до суду з вимогою змусити Автодорожній патруль Каліфорнії позбутися світлин і визнати незаконність їх поширення мережею Інтернет. На першому етапі справу позов був викинутий. Суд зазначив, що Catsouras не мала ніяких підстав для позову. Справа була передана до вищої інстанції, і розгляд запланований у Верховному Суді в березні 2012 року. Проте, відповідач (CHP) погодилися виплатити родині Ніколь «Ніккі» Catsouras $ 2375000 на етапі досудового врегулювання.

Родина Catsouras найняли Reputation Defender, щоб видалити фотографії, але вони продовжували поширюватися. За оцінками Reputation Defender, вони переконали сайти, щоб видалити 2500 з фотографій, але визнає, що видалення їх з Інтернету абсолютно неможливе. Адвокат і блогер Тед Франк писав, що хоча засоби масової інформації з розумінням відноситься до тяжкого становища батьків, але так званий «ефект Стрейзанд»[1] призвів до набагато більшого поширення фотографій» [8].

Величезним питанням є так званий етикет смерті в онлайн-світі. Окрім питань честі гідності, виникають також питання майнового характеру – кому належить цифрова спадщина особи, як в неї вступити?

Ще один приклад щодо права на честь і гідність. Цього разу у зв'язку з використанням технологій Big Data (великих

[1] Ефе́кт Стре́йзанд – феномен, який виражається в тому, що спроба видалити певну інформацію призводить лише до її більш широкого поширення. Наприклад, спроба обмеження доступу до фотографії, файлу або тексту призводить до дублювання даної інформації на інших серверах або появи її в файлообмінних мережах.

даних). У 2013 році мережа магазинів роздрібної торгівлі Target мала прецедент з використанням великих даних в маркетингових цілях [9]. Одного дня в офіс компанії увірвався розлючений чоловік. Він звинуватив співробітників компанії в тому, що ті надсилають його дочці дисконтні купони на памперси, соски та інші дитячі аксесуари. Чоловік був розлючений, адже його дочка – школярка. Виявилося, що, використовуючи технології і методи обробки великих даних, мережа магазинів дізналася про вагітність дівчинки раніше, ніж її батько. Зі списку регулярних покупок зникли тести на вагітність. Хто і яким чином може оцінювати правомірність і етичність використання таких даних? Чи можливе притягнення в такому випадку до відповідальності?

З огляду на важливість інформації для існування людини як такої, розвиток ситуації можна оцінювати як критичний. Саме час говорити про необхідність інформаційної екології.

Людська психіка має певні обмеження. Експериментально доведено, що мозок звичайної людини здатен сприймати і безпомилково обробляти інформацію зі швидкістю не більше 25 біт на секунду (в одному слові середньої довжини міститься якраз 25 біт). При такій швидкості поглинання інформації людина за життя може прочитати не більше трьох тисяч книг. І то – за умови, що буде щодня освоювати по 50 сторінок[10].

У той же час сьогодні в одній тільки науковій сфері щорічно з'являється кілька мільйонів книг. І навіть якщо вивчати тільки новинки, на кожну прочитану сторінку буде припадати 10 тисяч інших, осилити які нереально. Фахівці навіть ввели визначення «макулатурний фактор» – для літератури, яка користується нульовим попитом. Німецькі дослідники провели в одній із берлінських бібліотек вивчення попиту на 45 тисяч наукових і технічних видань, які зберігаються в ній. І з'ясувалося, що «макулатурний фактор» спрацював практично для 90 відсотків книг[10]. Тобто мільйони сторінок, які зберігають новітні технічні знання, так і не були ніким прочитані. Мало того, що ми не встигаємо вивчити велику частину інформації, яка накопичується, вона ще й швидко застаріває і вимагає заміни. Професійні знання в середньому застарівають за 3-4 роки (потребують оновлення) [11, с. 78].

Тобто, на момент отримання диплому про вищу освіту, знання з першого курсу навчання можуть бути неактуальними.

Вперше над цим фактом застановились вчені у 70-х роках минулого століття. Тоді і з'явився термін «інформаційний вибух**».** Під ним розумілося лавиноподібне збільшення кількості публікацій у наукових журналах, яке призвело до страшних прогнозів кінця науки як такої. Пояснювалася паніка дуже просто – жоден учений не зможе відстежувати те, що відбувається у його галузі, за таких «прискорених» умов.

У наш час термін «інформаційний вибух» прижився, і його почали розглядати під ще одним кутом – переважна більшість світових знань непотрібні для пересічної людини. Більшості за все життя можуть ніколи не знадобитися технологічні інструкції якогось підприємства або основи агрокультури.

Крім того, виникає і питання якості, адже велика частина всієї людської інформації – нескінченне дублювання одного і того ж з незначними змінами. Яскравий приклад – сучасні новини, які ЗМІ переповідають на свій лад.

Однією з причин появи нікому не потрібної інформації є зростаюча кількість безпосередніх творців контенту. Сьогодні практично будь-яка людина може опублікувати «свою» інформацію для всього світу завдяки соціальним мережам, форумам, блогам і т. д. І тут перед нами виникає питання: а яка якість цієї інформації? Адже у більшості своїй люди не публікують нічого змістовного або радикально нового. Так може, і вибуху ніякого немає, просто засмічуємо віртуальний простір, намагаючись показати світу власне «я»?

Інформаційне перевантаження «*information overload*» – термін, що описує труднощі розуміння проблеми і прийняття рішень, причиною якої є надлишок інформації. Поняття згадується в книзі Бертрама Гросса «Управління організацією» (1964 р.) [12, с. 856.], але популяризував його Елвін Тоффлер у своєму бестселері «Шок майбутнього» 1970 року [13]. Термін і концепція передували виникнення мережі і становлення інформаційного суспільства.

В останні роки термін «інформаційне перевантаження» модифікувалося у «надлишок інформації» (*information glut*) та

«смогу даних» (*data smog*). Термін, який раніше мав місце в межах когнітивної психології перетворився в метафору широкого вжитку, яку використовують далеко поза академічними колами. Значним чином, поява інформаційних технологій збільшило фокус на інформаційне перевантаження: інформаційні технології можуть стати основною причиною інформаційного перевантаження через їх здатність виробляти додаткову інформацію швидше і поширити цю інформацію до широкої аудиторії, ніж будь-коли раніше [14].

Інформаційне перевантаження має не лише психологічні, а й фінансові наслідки. За підрахунками Натана Зельдеса компанія Intel понесла майже в 1 мільярд доларів збитків через зниженню ефективності роботи, у вигляді часу, витраченого на обробку непотрібних повідомлень електронної пошти і відновлення від інформаційних втручань.

Дослідження Microsost виявили, що для повернення до виконуваного завдання після перевірки електронної пошти пересічному працівнику необхідно в середньому 24 хвилини [15, с. 85].

Тобто, якщо говорити про прийдешню соціально-економічну формацію, з тотальними об'ємами різного характеру та сутності інформації, то сучасна людина, просто не готова до цього, її мозок ще не в змозі адекватно реагувати та опановувати такі масиви інформації. З цього приводу влучним є висловлювання наведене у Всесвітній доповіді ЮНЕСКО «До суспільства знань»: «В сучасних інформаційних потоках, знайти необхідну інформацію, аналогічно до спроби напитись із пожежного крану – води виставить, але треба примудритись не захлинутися»[16]. Звісно, ІКТ фільтрують інформацію, проте, вони не можуть забезпечити рівня фільтрування яким володіє людський мозок.

І тут означимо питання змісту освітніх програм. На безпеці життєдіяльності чи охороні праці досі немає ні слова про культуру поведінки в умовах інформаційного перенасичення. Студенти ВНЗ розраховують норми освітлення і радіус забруднення радіацією – ніби-то вони цим користуватимуться в повсякденному житті.

Наостанок, кілька слів про право на охорону здоров'я, але в світлі інформаційних реалій – про комп'ютерну та інтернет-залежності. Проблема аддикції (патологічної залежності) починається тоді, коли прагнення втечі від реальності, пов'язане зі зміною психічного стану, починає домінувати у свідомості, стаючи центральною ідеєю, що вторгається в життя, веде до відриву від реальності. Відбувається процес, під час якого людина не тільки не вирішує важливих для себе проблем (наприклад, побутових, соціальних), але й зупиняється у своєму особистісному розвитку. У серпні 1997 року перелік видів «нематеріальної» залежності розширився: патологічне використання Інтернету стало позначенням офіційно визнаного психічного розладу. Однак багато психотерапевтів говорять, що інтернет-залежність не є самостійним захворюванням. Як правило, цей діагноз свідчить про інші, серйозні відхилення клієнта – депресію, комунікаційні проблеми тощо. Всі вони, так чи інакше, є ознаками нездатності впоратися зі стресом і формами тієї або іншої дезадаптації в реальному житті.

Влітку 2005 року на конференції Supernova 2005 співробітниця Microsoft Research Лінда Стоун поділилася дуже цікавими роздумами. Стоун каже, що в 1997 році народилося поняття «перманентна часткова увага». Під цим мається на увазі режим існування, в якому людина звикає ні на чому довго не зосереджуватися, робити відразу кілька справ, при цьому постійно «скануючи» навколишнє середовище на предмет «нових можливостей», які в жодному разі не можна упустити. «Протягом майже двох десятиліть постійна часткова увага була способом існування, способом виконання своїх обов'язків і підтримки відносин. Наш канал уваги розширився до крайніх меж...». На думку, дослідниці, з 1985 по 2005 роки тривав цикл, де перманентно розсіяна увага стала цілковитою нормою. Так само як і існування в якості вузла мережі. Відчуваючи себе «на зв'язку» людина відчуває себе «живою». Але платить він за це синдромом дефіциту уваги (Attention Deficit Disorder) – який є лише варіантом «перманентної часткової уваги», варіантом, визнаний хворобою [17].

Висновки. Неможливо в межах однієї доповіді порушити так значний обсяг питань. Зокрема, поза увагою в цій публікації

авторка свідомо залишила питання реалізації політичних прав в умовах е-демократії і засилля політтехнологій, заснованих на маніпуляції інформацією; співвідношення свобода слова і права на захист від шкідливої інформації; трудові права і соціальний захист в умовах віддаленої праці та фрілансерства; свободи совісті і права на національну самоідентифікацію в умовах глобального інформаційного простору та багато інших.

Водночас, хотілось би окреслити деякі міркування авторки щодо порушеної проблематики.

По-перше, обсяг і зміст прав і свобод людини в сучасному суспільстві визначається не лише особливостями певного співтовариства людей, а й розвитком людської цивілізації в цілому.

По-друге, в умовах інформаційного суспільства можливості реалізації прав і свобод людини суттєво залежать від адаптованості до них самої особи, інститутів суспільства і держави, а також системи права.

По-третє, необхідною складовою такої адаптації і умовою реалізації і захисту прав і свобод людини є високий ступінь інформаційної та правової культури.

Список літератури

1.Webster F. Theories of The Information Society. London and New York, 1995. P. 22.

2.Свобода інформації : навчальний посібник для державних службовців. [пер. з англ. Р. Тополевського] – К. : Тютюкін, 2010. – 128 с.

3.Declaration on Human Rights and the Rule of Law in the Information Society. May, 13, 2005 //
https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805da1a0

4.Адылханов А. А., Казезов А. Н. Права человека в киберпространстве [Текст] // Актуальные вопросы юридических наук: материалы II междунар. науч. конф. (г. Челябинск, февраль 2015 г.). — Челябинск: Два комсомольца, 2015. – Режим доступа: moluch.ru/authors/10704/

5.Verdict in MySpace Suicide Case //
http://www.nytimes.com/2008/11/27/us/27myspace.html

6.http://cyberbullying.org/cyberbullying-laws

7.Frank, Ted (May 10, 2010). «Catsouras v. Department of California Highway Patrol» // Point of Law. – Retrieved July 23, 2015.

8.How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did // http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#f13e1ad34c62

9.Attorney Makes New Case Law to Protect Privacy of the Families of the Dead // https://www.lawyersandsettlements.com/articles/civil-human-rights/interview-civil-rights-human-keith-bremer-17460.html

10. «Інформаційний вибух» XXI століття, або Горе з розуму // http://for-ua.com/analytics/2012/11/26/084809.html

11. Семикіна М.В. Удосконалення підготовки професійних кадрів промисловості на засадах соціального партнерства // Проблема ефективного використання та професійно-технічної підготовки кадрів промислового сектору України: Доповіді між нар. наук.-практ. конф., м. Київ, 28-29 листопада 2007р.: У 2 томах. – К.: РВПС України НАН України, 2008. – Т.2. – С.76-88.

12. Gross, Bertram M.. The Managing of Organizations: The Administrative Struggle. Vol. 2. London/New York, 1964. P. 856.

13. Toffler A. Future Shock. USA, Random House, 1970. P. 576.

14. Evaristo, Adams, & Curley. INFORMATION Load Revisited: A Theoretical Model / http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1061&context=icis1995

15. Paul Hemp. Death by information overload. *Harvard Business Review.* (2009) 87(9). P. 83–89.

16. Toward knowledge societies, United Nations Educational, Scientific and Cultural Organization, 2005 // http://unesdoc.unesco.org/images/0014/001418/141843e.pdf

17. Stone L. Extracting Signal from Noise in Social Networking // www.research.microsoft.com/en-us/um/redmond/events/scs2005

Іваненко В. Г. –
президент Українського Університету,
Вашингтон, США,
доктор, професор

УКРАЇНІЗАЦІЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ ЯК ФАКТОР ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ Й ПОСИЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Інформаційний простір України – напевно найслабкіша ланка українського державотворення, і криза в цій сфері від часу проголошення незалежності лише поглиблюється. Це обумовлено тим, що інформаційний простір України монополізований Росією й проросійськими російськомовними суб'єктами, і україномовний сегмент має тенденцію до зменшення. Тільки українізація може

кардинально виправдати ситуацію й повернути інформаційний простір Україні й посилити її державний суверенітет та національну безпеку.

Інформаційний суверенітет України за роки незалежності по суті втрачено. Русифікація в таких масштабах, яких Україна не знала за всі роки радянської влади, й монополізація інформаційного простору російськими й проросійськими суб'єктами – головна загроза інформаційному суверенітетові України. Формально незалежна держава й суб'єкт міжнародного права та міжнародних відносин, Україна однозначно не може бути визначена як суверенна держава в інформаційній сфері. Тільки українізація може й повинна стати фактором і гарантом забезпечення інформаційного суверенітету України.

Інформаційна безпека України фактично зруйнована до цурки. Упродовж років від часу проголошення незалежності Україна не спромоглася налагодити, закріпити й посилити свою інформаційну безпеку. Внаслідок цього російська пропаганда змогла безперешкодно використовувати ситуацію, задіявши в Україні свої можливості для підриву національної безпеки України. Наслідком цьоно і стала окупація Росією Криму, розв'язана війна на Донбасі. Тільки українізація може стати вирішальним фактором і засобом утвердження інформаційної безпеки України.

Українізація інформаційного простору, а відтак забезпечення інформаційного суверенітету й зміцнення інформаційної безпеки перш за все можливі за рахунок максимально можливого розширення вживання державної, української мови в усіх сферах життя українського суспільства.

Виконавча влада (адміністрація президента України й уряд, а також структури обласних і районних адміністрацій) має формуватися виключно за рахунок осіб, які вільно володіють державною мовою, які добре обізнані з історією України, з традиціями і звичаями українського народу і які справді переймаються долею України й українського народу. Мовний фактор значно знизить вірогідність проникнення в урядові структури кремлівської агентури й агентів впливу «русского міра». Принаймні Москві доведеться витрачати більше зусиль і

матеріальних засобів, щоб ретельніше готувати своїх агентів для роботи в українських урядових структурах.

Законодавча влада (Верховна Рада України, ради областей, міст і районів) має формуватися з депутатського корпусу, який вільно володіє державною, українською мовою. Виступи на сесіях рад недержавною мовою мають бути законодавчо забороненні. Ця умова різно зменшить кількість антиукраїнських елементів у законодавчих органах, а отже – й кількість антиукраїнських ідей, антиукраїнських законів та ін. Вимога вільного володіння державною мовою, знання історії, традицій і звичаїв українського народу бодай на рівні середньої школи має бути обов'язковою умовою для реєстрації кандидатів у депутати усіх рівнів.

Судова влада усіх рівнів формально уже здійснює правосуддя на більшості території України державною мовою: судді послуговуються в процесі й виносять вироки та рішення українською мовою. Однак інші учасники процесу (прокурори, адвокати, позивачі й відповідачі) здебільшого послуговуються російською, і це створює ситуацію, яку Юрій Шевчук назвав «мовною шизофренією». Це явище становить велику загрозу інформаційному суверенітетові й підриває інформаційну безпеку України. З ним можна і треба боротися, зобов'язавши з державних службовців (прокурорів) послуговуватися державною мовою,для інших учасників процесу увівши обов'язковість використання перекладачів на комерційній (платній основі). Платність перекладу вдарить по кишенях позивачів і відповідачів і змусить їх переходити на державну мову, якщо вони володіють нею, але не користуються. Такі заходи посилять інформаційний суверенітет і інформаційну безпеку Україні в системі судової влади.

«Четверта влада» – влада громадської думки, головним суб'єктом якої є система засобів масової інформації (ЗМІ). ЗМІ чи не найбільшою мірою можуть і повинні повернути український інформаційний простір Україні, утверджувати інформаційний суверенітет і посилювати інформаційну безпеку України. З метою забезпечення цих функцій і ефективної реалізації цих завдань усі без винятку ЗМІ з державною формою власності мають бути переведені на державну, українську мову. При цьому іномовні учасники радіо- й телепередач мають озвучуватися перекладом, виводячи звучання оригінальной мови мовця на задні план. Усі

комерційні національні, регіональні й місцеві ЗМІ приватної форми власності так само мають бути переведені на державну мову, і ця умова має бути обов'язковою складовою реєстрації й ліцензування.

Держава через законодавство (можливо, навіть окремим законом) має гарантувати етнічним меншинам та їхнім представникам (місцевим підприємцям) право засновувати будь-які ЗМІ мовами меншин для обслуговування своїх інформаційних потреб. Це ж законодавство має обумовлювати фінансування й інше матеріальне забезпечення ЗМІ етнічних меншин виключно внутрішніми можливостями етнічних меншин і немовлювати неможливість фінансування й будь-якої матеріальної підтримки із-за кордону. За порушення цього принципу повноважні державні органи мають позбавляти ЗМІ етнічних меншин відміною реєстрації та відкликанням ліцензії, а також порушувати кримінальні справи та передавати їх до суду.

Повноважні державні органи у порядку нагляду (не попереднього цензурування контенту) повинні моніторити зміст тих ЗМІ, які викликають занепокоєння в українському суспільстві щодо лояльності цих ЗМІ до української держави, українського суспільства, етнічних груп та ін. Будь-які прояви у будь-яких ЗМІ тенденцій до публікацій антиукраїнського й українофобського характеру й нелояльності до української держави та українського суспільства мають ставати предметом серйозного розслідування відповідно до законодавства, яке у свою чергу має передбачати наслідки за такі дії: від відміни реєстрації та відкликання ліцензії до адміністративного чи кримінального покарання. (Зразком такого законодавства може бути, скажімо, американський закон, відомий як Hate Crime Law – закон проти ненависництва.)

Важливими чинниками окреслення національного інформаційного простору, захисту інформаційного суверенітету й утвердження інформаційної безпеки є пропаганда, контрпропаганда і спецпропаганда.

Після проголошення незалежності Україна фактично відмовилася від пропаганди, яка була потужною складовою комуністичного режиму в СРСР, тоді як Росія зберегла всю радянську пропагандистську машину і задіяла її на повну силу в інформаційному просторі України, завдяки чому Кремлю вдалося

захопити цей простір без спротиву з боку України й утримувати Україну й українське суспільство у сфері свого імперського впливу. Намагання України відірватися від Москви й переорієнтуватися на Європу за такого стану в інформаційній сфері й призвели до втрати частини території, до напруги в проблемних з пропагандистського погляду регіонах та українсько-російської війни на Донбасі.

У протистоянні пропагандистській машині Кремля й наступові «русского міра» проявилися проблеми інформаційного характеру, про які в Україні за всі роки незалежності навіть не думали.

Перша проблема: Україна не налагодила належну інформаційну роботу, зокрема – українську пропаганду на територіях, де переважає російськомовне населення (значну частину якого складають етнічні росіяни), яке було використано Московією для антиукраїнської й україножобської пропаганди та просування ідей «русского міра», внаслідок чого Кремлеві і вдалося монополізувати інформаційний простір України й підготувати грунт для дестабілізації політичного, економічного, культурного життя України і зрештою – для військової агресії проти України. Отже, Україні треба серйозно замислитися над створенням потужного пропагандистського механізму.

Друга проблема: дестабілізація ситуації в південно-східних областях України російською пропагандою (і агентурою), окупація Криму й війна на Донбасі показали, що навіть для цих викликів Україна не спромоглася створити потужний центр для налагодження системної й масованої контрпропаганди для протидії російській пропагандистській машині. Створеня спеціалізованого міністерства інформації, знаного в народі як МінСтець, не принесло навіть мінімального результату. Міністерство інформації, як і міністерство оборони, не спромоглося налагодити ефективну контрпропаганду хоча б у зоні воєнних дій та проблемних регіонах.

Третя проблема: потужним чинником виправлення ситуації, що склалася в інформаційному просторі України, для захисту інформаційного суверенітету й зміцнення інформаційної безпеки України мала б стати спецпропаганда – пропаганда серед військ і населення супротивника, а також на ті зарубіжні країни, де

супротивник (Росія) проводить активну пропагандистську роботу проти України. Для реалізації цього завдання у відомствах, які відповідають за воєнні дії на сході України (СБУ, ЗСУ, МВС) мали бути створені потужні підрозділи спецпропаганди, об'єднані єдиним пропаганлистським проектом. Наскільки мені відомо, цього не зроблено і, здається, цим взагалі ніхто не переймається. Так само під егідою МЗС у співпраці з державними ЗМІ мав би бути створений потужний центр інформаційно-пропагандистського впливу на країни зарубіжжя, передусім – хоча б на ту частину території Росії, яка історично була і є ареалом розселення українців (Чорноземна зона, Кубань, Ставропілля та ін.), а також країни, в яких компактно проживають великі українські громади. На жаль, мушу констатувати, що в Україні нічого не було зроблено й нічого не робиться в царині спецпропаганди.

Таким чином, питання інформаційного простору, інформаційного суверенітету й інформаційної безпеки України залишаються відкритими. Отож роботи тут – непочатий край. Якщо держава цими проблемами не переймається, цим має занепокоїтися суспільство, принаймні його національно свідома й громадянськи активна частина. Очевидно, що розв'язання усіх зазначених вище проблем буде можливе лише в умовах українізації України.

Ісакова Н.М. –
здобувач кафедри адміністративного права
Інституту права ім. князя Володимира Великого МАУП

ПОНЯТТЯ ТА ЗМІСТ ІНФОРМАЦІЇ ЯК ОБ'ЄКТА АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ

Інформація відіграє важливу роль у суспільній життєдіяльності протягом всієї історії людства і виступає одним із ключових ресурсів цивілізаційного розвитку. Процес становлення та розвитку інформаційного суспільства в Україні на сучасному етапі зумовлює необхідність подальшого вдосконалення системи адміністративно-правового регулювання

суспільних відносин, об'єктом яких є інформація, та актуалізує наукові дослідження в цій сфері.

Інформація виступає важливим і необхідним елементом діяльності окремої людини, суспільства і держави. Соціальна корисність, економічна цінність і потенційна небезпека інформації вимагають детальної правової регламентації інформаційної сфери, режиму та порядку її використання та розроблення механізмів, що гарантують інформаційну безпеку особи, суспільства і держави.

Інформаційні відносини врегульовано різними нормами права: цивільного, сімейного, господарського, конституційного, кримінального, адміністративного, інформаційного тощо. У кожному із зазначених видів правовідносин інформація як об'єкт правового регулювання виявляє себе по-різному і має специфічні риси.

Упродовж багатьох років державна інформаційна політика в Україні охоплювала, головним чином, проблеми пов'язані з діяльністю засобів масової інформації. На початку 90-х років XX ст. зміст державної інформаційної політики було дещо розширено і до неї потрапили окремі елементи захисту прав громадян та організацій на загальнодоступну інформацію, гарантованих Конституцією країни, запроваджено право власності на інформацію, а також визначені аспекти інформаційної безпеки.

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

В контексті досліджуваного питання зазначимо, що латинське «*informatio*» походить від кореня *form* – форма, до

якого приєднується префікс *in* – у, всередині. Отже, етимологічно інформація означає «те, що знаходиться всередині форми», тобто зміст.

З огляду на це видається не зовсім обґрунтованою думка Г. В. Бромберга та Б. С. Розова про те, що інформація виступає як форма передачі знання – продукту розумової діяльності людини [1, с. 10-11]. Інформація не є формою передачі знання. Інформація – це і є самі знання.

Такий висновок знайшов своє підтвердження і в науковій літературі. Окремі автори розуміють під інформацією корисний (чи вигідний) зміст про річ, явище, факт, людину, суспільство, державу тощо, тобто вилучені з них чи про них усвідомлені дані у формі знань [2, с. 25].

Серед позитивних рис наведеного вище підходу варто виділити такі:

1) винайдення на уніфікованому природничому рівні відносно визначеної категорії – знання, – через яку можлива дефініція такого явища, як інформація;

2) демонстрація чітких відмінностей між поняттями «інформація» та «дані», що сьогодні є вельми актуальним у світлі повсюдного їх ототожнення у нормативно-правових актах.

Отже, головне завдання для юристів-науковців полягає в тому, щоб віднайти вже відому юридичну категорію, через яку можна було б виразити поняття інформації. Категорія «знання», хоча і є по суті вірною, проте в силу свого загальнонаукового і, навіть, більше філософського забарвлення для поставленого завдання не придатна, бо позбавлена юридичного значення (змісту). Тому, на нашу думку, видається цілком логічним спроектувати цю категорію на правову сферу та віднайти її юридичний аналог.

Список література

1.Бромберг Г.В. Интеллектуальная собственность: действительность переходного периода и рыночные перспективы / Г.В. Бромберг, Б.С. Розов. – М.: ИНИЦ, 1998. – 208 с.

2.Цит. за: Цимбалюк В. Інформація як об’єкт культурного усвідомлення та пізнання в суспільних відносинах / В. Цимбалюк // Правова інформатика. – 2004. – № 2. – С. 25.

Карчевский Н. В. –
Луганский государственный университет внутренних дел им. Э.А. Дидоренко,
доктор юридических наук, професор

УГОЛОВНО-ПРАВОВОЕ ОТРАЖЕНИЕ СОЦИАЛЬНЫХ ТЕНДЕНЦИЙ ИНФОРМАТИЗАЦИИ

Появление преступлений в сфере компьютерной информации является далеко не единственным последствием взрывной информатизации общества. Значительным потенциалом общественной опасности характеризуются также следующие факторы: чрезмерная капитализация информационного пространства; развитие возможностей манипуляции общественным сознанием в политической сфере; формирование сверхмощных баз персональных данных, представляющих опасность тотального контроля над личностью; рост уровня идеологической уязвимости политических систем из-за наличия глубоких социальных конфликтов, которые могут быть задействованы путем использования информационных технологий; интеллектуальная и духовная деградация общества и т. д. Все это означает, что *задача совершенствования уголовно-правового обеспечения противодействия преступлениям в сфере компьютерной информации должна решаться не самостоятельно, а в контексте уголовно-правового обеспечения процессов информатизации в целом.*

Прежде всего должен быть решен вопрос объекта уголовно-правовой охраны в сфере информатизации. Какие общественные отношения должны охраняться нормами права с тем, чтобы обеспечивать развитие положительных и минимизацию негативных социальных последствий информатизации? Очевидно, что речь идет об общественных отношениях, в пределах которых обеспечивается реализация информационной потребности граждан, общества или государства. Именно необходимость реализации возрастающей информационной потребности вызвала в своё время появление речи, письма и технологий книгопечатанья, стимулировала

развитие радио и телевидения и обусловливает сегодня постоянное совершенствование и расширение сферы применения современных компьютерных технологий. Поэтому правовое регулирование и охрана именно этих отношений, отношений в сфере реализации информационной потребности, может обеспечить предупреждение негативных последствий информатизации.

Для обозначения системы общественных отношений, направленных на обеспечение реализации информационной потребности граждан, общества или государства предлагается использовать термин *«информационная безопасность»*. Информационную безопасность субъекта следует считать обеспеченной тогда, когда он имеет возможность получать полную, достоверную и достаточную для принятия эффективных решений информацию. Такое состояние достигается социальной активностью в трех взаимосвязанных группах общественных отношений, представляющих собой структурные элементы информационной безопасности. Это общественные отношения: в сфере использования информационных технологий, в сфере обеспечения доступа к информационному ресурсу и в сфере формирования информационного ресурса.

В пределах первой группы общественных отношений выполняется задание обеспечения функционирования эффективных средств информационной деятельности, в пределах второй – обеспечивается возможность субъектов получать беспрепятственный доступ к необходимым информационным ресурсам, а в пределах третьей – обеспечивается формирование информационного ресурса, который отвечает потребностям субъектов[3].

Функционирование и эффективность каждого из элементов системы информационной безопасности обусловлены другими её элементами. Предоставление доступа к информации не имеет смысла без формирования информационного ресурса и является неэффективным без использования информационных технологий. Значение формирования информационного ресурса определяется возможностью дальнейшего доступа к нему и обеспечивается путем использования информационных

технологий. Функционирование информационных технологий приобретает социальное значение именно как средства доступа и формирования информационных ресурсов.

Социальная значимость как формирования информационного ресурса, так и предоставления доступа к информации, а также использования информационных технологий определяется значением тех общественных отношений, в пределах которых возникает информационная потребность. То есть общей чертой отношений информационной безопасности является то, что целесообразность их уголовно-правовой охраны определяется социальной значимостью тех общественных отношений, в пределах которых возникает информационная потребность. Именно актуальность последних определяет значимость отношений информационной безопасности, а также целесообразность и интенсивность соответствующих мер правового регулирования. Например, значимость доступа к информации и, как следствие, необходимость его правового регулирования не является самостоятельной и определяется важностью той деятельности, для осуществления которой нужен доступ. Последствия незаконного получения доступа к информации определяются не самим фактом незаконного ознакомления с определенной закрытой информацией, а содержанием тех отношений, в пределах которых возникла потребность ограничения доступа. Опасность нарушения функционирования определенной компьютерной сети определяется важностью заданий, для которых она используется, именно последние выступают критерием обоснованности применения соответствующих средств уголовной юстиции.

Таким образом, *информационная безопасность* понимается как система общественных отношений, обеспечивающих возможность реализации информационной потребности граждан, общества, государства. Реализация информационной потребности осуществляется путем получения доступа к необходимой информации, базируется на использовании информационных технологий и обеспечивается формированием информационного ресурса.

В наиболее общем понимании лицо следует считать находящимся в состоянии информационной безопасности тогда, когда его потребность в информации обеспечена должным образом. То есть тогда, когда лицо имеет возможность получать достоверную и достаточную для осуществления эффективной деятельности информацию. А общественно опасными следует признавать такие посягательства в сфере информационной безопасности, которые исключают или значительно усложняют реализацию информационной потребности.

Отметим также, что термин «информационная безопасность» достаточно широко применяется в информатике и обозначает, как правило, комплекс мероприятий по обеспечению защиты информации от уничтожения или незаконного доступа; совокупность организационных, программных и технических средств, обеспечивающих целостность, конфиденциальность и доступность данных. Тем не менее, применение его в юридическом контексте для обозначения самостоятельного объекта уголовно-правовой охраны, также представляется обоснованным. Вызвано это достижением соответствующими отношениями социального значения, требующего применения средств уголовной юстиции. Можно утверждать, что современные тенденции информатизации позволяют рассматривать информационную безопасность как в узком смысле (обеспечение защиты информации) так и в широком – обеспечение реализации социальной информационной потребности.

Итак, *обеспечение уголовно-правового стимулирования положительных и минимизации негативных социальных последствий информатизации, предполагает определение в качестве самостоятельного объекта уголовно-правовой охраны системы общественных отношений, обеспечивающих реализацию информационной потребности. Для обозначения данной системы предлагается использовать термин «информационная безопасность», её структуру составляют отношения в сфере формирования информационного ресурса, обеспечения доступа к информации, а также отношения в сфере использования информационных технологий. Социальная значимость отношений информационной безопасности, а*

следовательно и целесообразность их уголовно-правовой охраны, определяются значимостью тех отношений, в пределах которых возникает информационная потребность.

Вместе с тем, обеспечение уголовно-правовой охраны каждой из обозначенных групп имеет определённую специфику.

Начнём с отношений *в сфере использования информационных технологий*. Основная правовая проблема здесь – обеспечение нормативно-правовой базы противодействия так называемым «компьютерным» преступлениям. С учётом высказанных ранее положений, сформулируем следующее положение: критерием отнесения определённых деяний к преступлениям в сфере использования информационных технологий следует считать вред, причиняемый той социально значимой деятельности, для осуществления которой применяется компьютерная техника. Очевидно, что уничтожение информации, обрабатываемой в компьютерной системе, опасно настолько, насколько социально значимой является задача, для решения которой используется определенный компьютер. Тем не менее, законы об уголовной ответственности некоторых государств не учитывают такой специфики. Так, судя по решению, принятому украинским законодателем, утечка, потеря, подделка, блокирование информации, нарушение установленного порядка ее маршрутизации или искажение процесса ее обработки (ст. 361, 362 УК Украины) признаются общественно-опасными сами по себе. Лишь на уровне квалифицирующих признаков мы встречаем зависимость уголовной ответственности от наступления «существенного вреда».

Подобная ситуация приводит к вполне ожидаемым проблемам: из-за отсутствия в законодательных определениях преступлений в сфере использования информационных технологий четких критериев общественной опасности под уголовно-правовой запрет и, соответственно, в сферу действия уголовной юстиции попадают не только деяния, которые действительно являются общественно опасными, но и не являющиеся таковыми. Это приводит к существенному снижению эффективности уголовно-правового противодействия указанным преступлениям. Данный вывод был доказан в ходе

исследования практики применения украинского уголовного законодательства[3]. Проведенное исследование судебных решений, связанных с применением ст.ст. 361–362 КК Украины, позволяет утверждать, что эффективность уголовно-правовых мер противодействия преступлениям в сфере использования информационных технологий является недостаточной. Большинство исследованных приговоров не могут рассматриваться как средство противодействия действительно общественно опасным проявлениям в отмеченной сфере. При этом непоследовательность изученных судебных решений не в последнюю очередь обусловлена недостатками действующего уголовного законодательства, отсутствием в нем четких, понятных критериев общественной опасности посягательств в сфере использования информационных технологий. Необходимо отметить: *при криминализации преступлений в сфере использования электронно-вычислительных машин, систем, компьютерных сетей и сетей электросвязи был нарушен принцип общественной опасности. Сущность этого нарушения можно сформулировать следующим образом: из-за отсутствия в законодательных определениях данных преступлений четких критериев общественной опасности под уголовно-правовой запрет и, соответственно, в сферу действия уголовной юстиции попадают не только деяния, которые действительно являются общественно опасными, но и не являющиеся таковыми. Именно это отчасти и приводит к существенному снижению эффективности уголовно-правового противодействия исследуемым преступлениям.*

Исправление ситуации в первую очередь предусматривает включение в диспозиции соответствующих уголовно-правовых норм четких положений относительно критериев общественной опасности посягательств. Одним из возможных и наиболее оптимальных решений является обращение к законодательным конструкциям, свойственным преступлениям с производными последствиями. Структура объективной стороны преступлений в сфере использования компьютерной техники должна включать: 1) основные последствия – различные формы нарушения информационных отношений, выступающих непосредственными объектами

(уничтожение, блокирование, нарушение целостности информации и т.д.); 2) производные последствия - нарушение отношений в сфере реализации прав и свобод отдельных физических лиц, государственных или общественных интересов, деятельности юридических лиц. Лишь при наличии совокупности таких последствий совершенное посягательство следует считать преступлением в сфере использования информационных технологий.

В самом общем смысле, правовое регулирование *отношений обеспечения доступа к информации* представляет собой поиск баланса между двумя группами противоположных социальных интересов: с одной стороны – интересов определенных субъектов в ограничении доступа к информации, а с другой – интересов определенных субъектов в получении информации. Поэтому, сущность нарушений информационной безопасности в данной сфере заключается в том, что нарушение реализации информационной потребности обусловлено или нарушением установленного режима доступа к определенному ресурсу, или неправомерным ограничением доступа к определенной информации. Следует отметить, что отношения доступа к информации весьма продолжительный период времени регулировались правом и охранялись уголовным законом, хотя до определенного уровня технологического развития не имели самостоятельного значения. С компьютеризацией общества, появлением Интернета произошел взрывной рост количественных и качественных показателей накопления и использования информации во всех сферах социальной жизни и жизни отдельных граждан. Современные информационные технологии радикально изменили структуру и формы общения. Сегодня сама форма организации общества, его эффективность прямо зависят от обеспечения достоверности информации, сохранения сформированных потоков данных и скорости их передачи. Если еще сто лет тому назад посягательства на информационные отношения преимущественно не рассматривались как такие, что характеризуются существенной общественной опасностью, то сегодня есть все основания ставить знак равенства между информационной безопасностью и безопасностью общества в

целом. Нужно признать, что уголовным законодательством такие изменения остались скорее незамеченными. *Нормы об уголовной ответственности за нарушения ограниченного доступа к информации рассредоточены, встречаются в различных законах об уголовной ответственности*, хотя очевидно, что интенсивность уголовно-правовой охраны отношений в сфере ограниченного доступа к информации должна определяться не видом информации (государственная тайна, коммерческая, тайна усыновления и т. д.), а содержанием наступивших последствий.

Таким образом, имеющаяся в действующем законодательстве система норм об ответственности за преступления в сфере информационной безопасности должна рассматриваться с позиций ее оптимизации. Очевидно, что в ходе ее совершенствования *должен решаться вопрос о целесообразности, обоснованности и пределах замены имеющейся рассредоточенной системы специальных уголовно-правовых запретов такими нормами, которые бы обеспечивали охрану более широких сегментов отношений информационной безопасности. Есть смысл отказаться от чрезмерной детализации уголовно наказуемых видов нарушений ограниченного доступа к информации.*

Наконец, об уголовно-правовой охране общественных отношений в сфере *формирования информационного ресурса*. Следует отметить, что проблема уголовно-правового обеспечения формирования информационных ресурсов не является новой. Уголовное законодательство подавляющего числа государств содержит нормы об ответственности за: призывы к насильственному свержению конституционного строя; умышленные действия, направленные на разжигание национальной, расовой или религиозной вражды и ненависти, на унижение национальной чести и достоинства, или обиды чувств граждан в связи с их религиозными убеждениями; публичные призывы к совершению террористического акта; призывы к совершению действий, которые угрожают общественному порядку; изготовление или распространение порнографических предметов и т.д.

Однако, в современных условиях – условиях повышения интенсивности массовой коммуникации – соответсвующие угрозы, обусловленные нарушениями в сфере формирования информационного ресурса, гораздо глубже и сложнее. Уже сегодня специалисты отмечают, что средства массовой коммуникации все чаще вводят своего потребителя в состояние, при котором действуют механизмы и неписаные законы личного обогащения, отчужденности, безразличия к обществу, все более развращают его насилием, пропагандой наркотиков, алкоголя, преступности и безнаказанности[5]. Обосновывается, что одним из факторов формирования мотивации противоправного поведения несовершеннолетних является деструктивное влияние СМИ[1]. Современная массовая коммуникация, ориентированная в первую очередь на философию потребления, может привести к духовному и интеллектуальному вырождению общества[4].

При этом обоснованно прогнозировать, что ожидаемое увеличение интенсивности массовой коммуникации существенно обострит данные угрозы, приведет к тому, что их развитие ускорится. Зафиксировав, настолько тревожные социальные тенденции, рассмотрим, какие меры уголовно-правовой охраны могут быть использованы для их предупреждения и минимизации последствий. Наиболее распространенным и, возможно, исторически первым средством противодействия общественно опасным проявлениям в сфере формирования информационного ресурса является контроль за содержанием сообщений и ограничение доступа к ним. Именно к таким средствам следует относить упомянутые ранее нормы действующего уголовного законодательства. Однако эти уголовно-правовые запреты нельзя рассматривать как целостную систему, они представляют собой законодательную реакцию на наиболее опасные проявления нарушений формирования информационного ресурса, относящиеся к разнообразным сферам социального бытия: национальной безопасности, противодействию расовой неприязни и ксенофобии, общественной безопасности, морали и т. д.

Возможно, установленные общественно опасные последствия современных процессов формирования

информационного поля требуют уголовно-правовых запретов более широкого спектра действия? Таких, которые бы обеспечивали противодействие включению любого негативного контента в общественный информационный ресурс, исключали бы возможность манипулирования общественным сознанием [див. 7]?

Ответ на поставленные вопрос является негативным. И дело не только в том, что усиление государственного контроля за деятельностью средств массовой информации путем включения дополнительных уголовно-правовых норм потенциально опасно свертыванием процессов демократизации и, естественно, повлечет нарушения прав человека. Попытка сформулировать подобные новеллы приведет к ожидаемой проблеме: принципиально невозможно сформулировать определение для обозначения тех сведений, включение которых в информационное поле следует считать общественно опасным. Весьма проблематичной будет и попытка четкого (что является обязательным для уголовно-правовой нормы) определения общественно опасных последствий. Такая ситуация с необходимостью приведет к формулировке уголовно-правового запрета на основе оценочных понятий, что, в свою очередь, *создаст необоснованный риск злоупотреблений уголовным правом.*

Кроме того, *распространение глобальных информационных технологий (Интернет, сети спутникового вещания) вообще делает все менее эффективными методы, основывающиеся на ограничении или запрете распространения определенной информации*. Например, тотальный мониторинг Интернета, по мнению западных специалистов по вопросам информационной безопасности, не может помочь в борьбе с экстремизмом даже теоретически. Плотность современных информационных потоков настолько велика, что даже для выборочной своевременной проверки отдельных информационных источников понадобится такое количество специалистов, которое в несколько раз превышает экономически обоснованную численность всех правоохранительных органов государства[6].

Стоит согласиться и с тем, что вертикальная регуляторная схема, срабатывающая относительно минимизации угроз, связанных с распространением вредоносного контента в традиционных масс-медиа, не действует в условиях интерактивности и глобальности[2]. Ярким примером здесь может послужить широко известный «эффект Стрейзанд».

Очевидно, что *комплекс вопросов, связанных с правовым регулированием процессов формирования информационного ресурса, имеет свое решение преимущественно за пределами уголовно-правового поля.* Вместе с тем, следует учитывать, что вывод о потенциальной неэффективности и, как следствие, отсутствии целесообразности расширения средств уголовно-правовой охраны отношений информационной безопасности в сфере формирования информационного ресурса, сделан с учетом современного уровня развития науки и техники. Вместе с тем развитие компьютерных технологий, психологии, социологии и криминологии может обеспечить возможность формулирования четких уголовно-правовых норм. В таком случае, дополнение предложенного УК нормами, обеспечивающими уголовно-правовую охрану отношений в сфере формирования информационного ресурса станет целесообразным.

Таким образом, основные требования к содержанию уголовно-правовой охраны общественных отношений в сфере информатизации заключаются в следующем:

1) объектом уголовно-правовой охраны в данной сфере следует считать информационную безопасность – систему общественных отношений, в пределах которых обеспечивается реализация информационной потребности граждан, общества, государства;

2) указанная система состоит из трёх элементов – отношения в сфере формирования информационного ресурса, отношения в сфере обеспечения доступа к информации, отношения в сфере использования информационных технологий;

3) целесообразность уголовно-правовой охраны информационной безопасности, определяются значимостью тех

отношений, в пределах которых возникает информационная потребность;

4) повышение эффективности уголовно-правовой охраны отношений в сфере использования информационных технологий предполагает включение в соответствующие законы четких положений относительно критериев общественной опасности посягательств, обеспечивающих применение средств уголовной юстиции только в тех случаях, когда имеет место обусловленное посягательством в сфере информационных технологий существенное нарушение отношений в сфере реализации прав и свобод отдельных физических лиц, государственных или общественных интересов, деятельности юридических лиц;

5) система норм об уголовной ответственности за преступления в сфере ограниченного доступа к информации требует оптимизации, в ходе ее совершенствования должен решаться вопрос о целесообразности, обоснованности и пределах замены имеющейся рассредоточенной системы специальных уголовно-правовых запретов такими нормами, которые бы обеспечивали охрану более широких сегментов отношений информационной безопасности;

6) несмотря на то, что количественные и качественные показатели информатизации позволяют прогнозировать усиление развития негативных социальных последствий в сфере формирования информационных ресурсов, расширение уголовно-правовых средств в данной сфере, дополнение уголовного законодательства новыми нормами об ответственности за распространение «общественно опасной информации», является нецелесообразным из-за прогнозируемой неэффективности таких норм, непринадлежности решений данных социальных проблем к уголовно-правовому полю.

Список литературы

1. Бугера О. Засоби масової інформації: проблема вдосконалення діяльності щодо запобігання протиправної поведінки неповнолітніх / О. Бугера // Підприємництво, господарство і право. – 2005. – № 7. – С. 70–73.

2.Зернецкая О. Интернет-ловушка для молодежи [Электронный ресурс] / О. Зернецкая // Зеркало недели. – 2007. – № 11. – Режим доступу : http://zn.ua/articles/49507.

3.Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / М. В. Карчевський – Луганськ, 2011. – 538 с.

4.Кендюхов О. Суспільство споживання як національна трагедія України [Електронний ресурс] / О. Кендюхов // Дзеркало тижня. – 2011. – № 1. – Режим доступу : http:// dt.ua/articles/73290.

5.Коваленко В. В. Сучасна масова комунікація: носій добра чи криміногенний фактор? / В. В. Коваленко // Право України. – 2008. – № 4. – С. 84–89.

6.Паньо Е. Сито со слишком большими дырочками [Электронный ресурс] / Е. Паньо, Т. Паньо // Зеркало недели. – 2006. – № 24. – Режим доступу : http://zn.ua/articles/47040.

7.Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти : монографія / Н. А. Савінова. – К. 2012. – 340 с.

Козюренко Р.С. –
здобувач кафедри адміністративного права
Інституту права ім. князя Володимира Великого МАУП

АДМІНІСТРАТИВНА ВІДПОВІДАЛЬНІСТЬ ЗА ПРАВОПОРУШЕННЯ У СФЕРІ ІНФОРМАЦІЇ

У світлі сучасних державотворчих та правотворчих процесів в Україні, зорієнтованих на практичну реалізацію положень Конституції щодо побудови демократичної, соціальної, незалежної, правової держави; визнання особи найвищою соціальною цінністю; реформування організаційно-правової структури та функціонального призначення публічних органів; запровадження моделі партнерських відносин особи та органів держави особливого значення набувають питання правової регламентації змісту та структури адміністративного процесу. Його складний системний характер зумовлюється значним обсягом предметної регламентації, яка охоплює найрізноманітніші сфери діяльності публічної адміністрації та численні категорії індивідуальних справ. Особливої уваги заслуговує питання наукової детермінації окремих утворень адміністративного процесу, адже від того, наскільки динамічно буде розв’язуватися проблема ланок системи адміністративного

процесу, залежатиме вся кодифікаційна діяльність в царині адміністративно-процесуального права, а також ефективне функціонування усієї системи державної влади на благо людини, суспільства та держави загалом.

Одними з основоположних напрямів Концепції адміністративної реформи є оновлення інституту державного управління та розв'язання проблем адміністративно-юрисдикційної діяльності державних органів та судової гілки влади. Це значною мірою зумовлено тим, що вказані органи функціонують у різних сферах суспільного життя, а громадяни практично щодня звертаються до них задля вирішення широкого кола питань, пов'язаних з реалізацією своїх прав. На адміністративний процес покладається важливе завдання регулювання поведінки учасників правовідносин, визначення їх статусу на конкретних стадіях адміністративного провадження.

Стан законодавства України про адміністративну відповідальність, особливо процесуальних норм, які встановлюють порядок притягнення винної особи до відповідальності, на жаль, суперечливий і недосконалий. Необхідність розв'язання цих проблем визріла вже давно, однак без достатньо обґрунтованих наукових розробок в окресленій сфері змінити якість вітчизняного законодавства неможливо.

Зокрема, така ситуація стосується адміністративної відповідальності за правопорушення у сфері інформації.

У КУпАП, існує більше 20 статей, що мають безпосереднє відношення до інформаційної сфери, а правопорушень значно більше, ніж статей. Так, лише ч. 1 ст. 212^2 КУпАП («Порушення законодавства про державну таємницю») містить дев'ять пунктів, більшість із яких встановлюють відповідальність за декілька різних адміністративних порушень у сфері інформаційної безпеки.

Окремого розгляду потребує питання адміністративної відповідальності юридичних осіб за вчинення правопорушень в інформаційній сфері. Насамперед слід зазначити, що у науковій літературі широко дискутується питання про адміністративну відповідальність юридичних осіб. Натомість, аналіз відповідних статей чинного КУпАП дозволяє дійти висновку, що суб'єктом адміністративного правопорушення віднедавна визнається не

лише фізична особа, але й юридична, які передбачають накладення стягнень на юридичних осіб, зокрема, за правопорушення в інформаційній сфері. Так, згідно з ч. 6 ст. 20 Закону України «Про державну таємницю» від 21.01.1994 р. дозвіл на провадження діяльності, пов'язаної з державною таємницею, може бути скасовано Службою безпеки України на підставі акту проведеної нею перевірки, висновки якого містять дані про недотримання органом державної влади, органом місцевого самоврядування, підприємством, установою, організацією умов, передбачених цією статтею Закону. Відповідно до ч. 3 ст. 18 Закону України «Про друковані засоби масової інформації (пресу) в Україні» від 16.11.1992 р. суд припиняє випуск видання у разі поширення відомостей, розголошення яких забороняється ст. 46 Закону України «Про інформацію», закликів до захоплення влади, насильницької зміни конституційного ладу або територіальної цілісності України; пропаганди війни, насильства та жорстокості; розпалювання расової, національної, релігійної ворожнечі; розповсюдження порнографії, а також з метою вчинення терористичних актів та інших кримінально караних діянь.

Законодавство про адміністративну відповідальність юридичних осіб в Україні на сьогодні недостатньо розроблене. Загальні положення та принципи стосовно адміністративної відповідальності юридичних осіб у нормативних актах майже повністю відсутні. Механізм притягнення юридичних осіб до адміністративної відповідальності майже не врегульований. Немає системності й у видах санкцій, що застосовуються до юридичних осіб. У деяких випадках юридичні особи несуть відповідальність нарівні з фізичними особами [2, с. 175].

За вчинення адміністративного правопорушення у сфері обігу інформації на фізичних осіб найчастіше накладається штраф. На нашу думку, цей вид адміністративного стягнення слід накладати і на юридичних осіб – порушників законодавства про інформацію.

Викладене свідчить, що для запровадження логічно завершеної, ефективної правової регламентації адміністративної відповідальності за правопорушення в інформаційній сфері необхідно передбачити у чинному КУпАП розділ, який би

містив правопорушення у сфері обігу інформації, а також закріпити у чинному КУпАП (або у новому Кодексі України про адміністративні проступки) норму, яка б передбачала адміністративну відповідальність юридичних осіб за вчинення правопорушень в інформаційній сфері.

Список літератури

1.*Агапов А. Б.* Основы государственного управления в сфере информатизации в Российской Федерации / *А. Б. Агапов*. – М., 1997. – 343 с.

2.*Адміністративне* право України / Ю. П. Битяк, В. М. Паращук, О. В. Дьяченко та ін. / За ред. Ю. П. Битяка. – К., 2005. – 544 с.

Кропивницький М. О. –
аспірант кафедри адміністративного та інформаційного права
Навчально-наукового інституту права та психології
Національного університету «Львівська політехніка»

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ ФІНАНСУВАННЯ СОЦІАЛЬНОГО ЗАБЕЗПЕЧЕННЯ ГРОМАДЯН УКРАЇНИ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Протягом останніх років в Україні та світі, спостерігається стрімкий розвиток інформаційних технологій. Прогресивні тенденції у сфері інформаційних технологій зумовлюють переорієнтацію органів державної влади, зокрема і у сфері соціального забезпечення на застосування новітніх технологій у своїй діяльності.

Побудова сучасного інформаційного суспільства є пріоритетним завданням для нашої держави.

Відповідно до Закону України від 09.01.2007 № 537-V «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» основним завданням розвитку інформаційного суспільства в Україні є сприяння кожній людині на засадах широкого використання сучасних інформаційно-комунікаційних технологій можливостей створювати інформацію і знання, користуватися та обмінюватися ними,

виробляти товари та надавати послуги, повною мірою реалізовуючи свій потенціал, підвищуючи якість свого життя і сприяючи сталому розвитку країни [1].

Інформаційні технології створюються з метою: оптимізації внутрішньої діяльності органів державної влади; підвищення ефективності у взаємодії з іншими органами державної влади, громадянами, підприємствами, установами, організаціями, економії часу та коштів. У сфері фінансування соціального забезпечення громадян це дозволить: оперативно і точно обліковувати прибутки державного бюджету та бюджету Пенсійного фонду; ефективно взаємодіяти між державним і місцевими бюджетами всіх рівнів; швидко доводити кошти державного бюджету, місцевих бюджетів, бюджету Пенсійного фонду та Фонду соціального страхування до кінцевих споживачів; здійснювати поточний контроль та аналіз за цільовим використанням бюджетних коштів.

Впровадження інформаційних технологій в діяльності органів державної влади потребує прийняття відповідних нормативно-правових актів.

На сьогоднішній день прийнято ряд нормативно правових актів у сфері інформаційних технологій, зокрема, Закон України від 04.02.1998 № 75/98-ВР «Про Концепцію Національної програми інформатизації», Закон України від 04.02.1998 № 74/98-ВР «Про Національну програму інформатизації», Закон України від 22.05.2003 № 851-IV «Про електронні документи та електронний документообіг», Закон України від 22.05.2003 № 852-IV «Про електронний цифровий підпис», Закон України від 09.01.2007 № 537-V «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», також, розпорядження Кабінету Міністрів України від 13.12.2010 № 2250-р «Про схвалення Концепції розвитку електронного урядування в Україні», розпорядження Кабінету Міністрів України від 15.05.2013 № 386-р «Про схвалення Стратегії розвитку інформаційного суспільства в Україні», розпорядження Кабінету Міністрів України від 11.09.2013 № 718-р «Про затвердження плану заходів щодо створення Єдиного державного порталу адміністративних послуг» розпорядження Кабінету Міністрів України від 08.04.2015

№ 338-р «Про затвердження плану заходів з підтримки розвитку індустрії програмної продукції на 2015 рік» та інші.

Спостерігається ряд позитивних зрушень щодо інформатизації діяльності органів, які здійснюють фінансування соціального забезпечення громадян України, а саме: органів Пенсійного фонду України, органів соціального захисту населення, та органів казначейської служби.

Так, в територіальних органах Пенсійного фонду України встановлено інформаційні кіоски для доступу громадян до відомостей, які зберігаються в Інформаційному центрі персоніфікованого обліку Пенсійного фонду України, запроваджено нову систему обслуговування громадян та обробки пенсійної документації на базі централізованих інформаційних технологій, створено web-портал електронних послуг Пенсійного фонду тощо.

Для автоматизації процесів призначення, перерахунку, нарахування пенсій, допомог, компенсаційних виплат тощо, масових перерахунків, формування документів з виплати, бухгалтерської та статистичної звітності в органах Міністерства соціальної політики України (далі – Мінсоцполітики), Пенсійного фонду України на базі діючих законодавчих та нормативних актів України функціонує *Автоматизована система оброблення пенсійної документації на базі комп'ютерних технологій (АСОПД/КОМТЕХ-W)*[2].

В перспективі, у сфері пенсійного забезпечення передбачається запровадження електронних пенсійних справ, створення реєстру електронних пенсійних справ та систем їх технічної підтримки, комплексної системи захисту інформації. Планується залучення для обслуговування громадян банків, відділень поштового зв'язку, об'єднаних громад з подальшим розширенням мережі таких пунктів обслуговування [3].

В своїй діяльності органи соціального захисту населення використовують автоматизовані інформаційні системи: *«Наша сім'я»,* для обліку на місцевому рівні соціального стану інвалідів та їх сімей, одиноких непрацездатних громадян, малозабезпечених громадян та їх сімей для організації соціальної допомоги по видах послуг, *«Єдиний державний реєстр осіб, які мають право на пільги»* для обліку осіб, які

мають право на пільги згідно із Законами України, та для автоматизації звірки правових даних, зареєстрованих в реєстрі громадян, з даними організацій надавачів послуг. Окрім того, використовуються програмні комплекси: *«Житлові субсидії»* для автоматизації процесів призначення, перерахунку житлових субсидії, формування звітності у відповідності до чинних законодавчих та нормативних актів України, «*Статистичний моніторинг бідності»,* що забезпечує оброблення регламентних запитів центрального рівня (Мінсоцполітики) до баз даних регіонального (обласні управління соціального захисту населення) та районного рівнів та формування звітів на трьох рівнях функціонування [2].

В майбутньому у сфері соціального захисту населення планується модернізувати Інформаційно-аналітичну систему соціального захисту населення відповідно до вимог часу, максимально автоматизувати усі процеси надання громадянам України різних видів соціальної допомоги, компенсаційних виплат, санаторно-курортного лікування тощо. Особлива увага буде приділятися новому порядку нарахування та оформлення субсидій на оплату послуг житлово-комунального господарства. Разом з тим, до 1 січня 2017 року в Мінсоцполітики буде запущено електронну систему внутрішнього документообігу [4].

Використання автоматизованих систем органами Державної казначейської служби забезпечує створення єдиного інформаційного простору, що охоплює всі ділянки та всіх учасників бюджетної сфери, зокрема і сферу бюджетного фінансування соціального забезпечення.

Автоматизована казначейська система обліку доходів та видатків бюджетів усіх рівнів являє собою комплекс, у якому взаємодіють декілька систем, а саме: «Казна-Доходи» для обліку дохідної частини бюджетів і взаємодії із системою електронних платежів Національного банку України та «Казна-Видатки» для обліку видаткової частини бюджетів.

У кожну із систем закладені функції виходячи зі специфіки діяльності казначейства, до яких відносяться: відкриття рахунків розпорядникам і одержувачам бюджетних коштів і їхнє обслуговування, складання звітності про розподіл і використання бюджетних коштів; відкриття рахунків для збору

доходів державного і місцевого бюджетів у розрізі видів доходів та територій , їхнє обслуговування відповідно до діючого законодавства і складання звітності про виконання бюджетів усіх рівнів по доходах; введення мережі розпорядників бюджетних коштів, починаючи від головних розпорядників і закінчуючи одержувачами; контроль за цільовим використанням бюджетних коштів; ведення бухгалтерського обліку [5].

Окрім того, Державна казначейська служба України повноцінний учасник системи електронних переказів Національного банку України; має власну внутрішню платіжну систему; має сучасну інформаційно-телекомунікаційну систему; роботу органів казначейства забезпечує сучасний центр обробки даних, обладнаний необхідним серверним та телекомунікаційним обладнанням.

В подальшому у сфері казначейського обслуговування бюджетних коштів планується: ввести в експлуатацію централізовану систему формування оперативної звітності АС «Є-Звіт»; завершити централізацію системи управління бюджетною установою «Парус-Бюджет»; повністю запровадити систему дистанційного обслуговування клієнтів через програмно-технічний комплекс «Клієнт Казначейства – Казначейство»; інтенсифікувати використання хмарних технологій для забезпечення відмовостійкості баз даних як центрального апарату, так і територіальних органів казначейської служби [6].

Слід відмітити, що, як і більшість органів державної влади, органи, які здійснюють фінансування соціального забезпечення мають власні сайти та сторінки в соціальних мережах, де оперативно висвітлюється інформація про діяльність вказаних органів, а також електронну пошту, що дає можливість звертатися до таких органів в електронній формі. Окрім того, функціонує Урядовий контактний центр для взаємодії органів виконавчої влади з громадянами, що дозволяє оперативно вирішувати проблемні питання, які порушуються у зверненнях громадян, а також удосконалювати роботу органів виконавчої влади з урахуванням громадської думки.

Водночас, попри зазначене, стан впровадження інформаційних технологій у сфері фінансування соціального

забезпечення є далеким від ідеального та потребує значного покращення. Насамперед слід зазначити про відсутність адекватної нормативно-правової бази для розвитку та впровадження інформаційних технологій, також виникають проблеми в процесі функціонування програмного забезпечення, автоматизованих систем, електронного документообігу тощо. Окрім того, відсутнє належне забезпечення комп'ютерною технікою та програмним забезпеченням, значна частина комп'ютерів та програм морально застаріли як в частині використання так і обсягу та характеру виконуваних функцій, також не у всіх органах державної влади є доступ до мережі Інтернет.

На наш погляд, пріоритетними кроками для впровадженні інформаційних технологій у сфері фінансування соціального забезпечення мають бути, зокрема: розробка відповідної нормативно-правової бази для впровадження інформаційних технологій; створення єдиних стандартів взаємодії суб'єктів електронного обміну, та гармонізація їх з міжнародними стандартами; оновлення комп'ютерної техніки та програмного забезпечення; впровадження єдиної системи електронного документообігу з використанням електронного цифрового підпису; поглиблення впровадження спеціалізованого програмного забезпечення за принципом «Єдиного вікна», що передбачає наявність однієї точки входу для взаємодії громадян з органами влади всіх рівнів та інші.

Отже, незважаючи на ряд позитивних зрушень у сфері інформаційно-комунікаційних технологій, стан впровадження інформаційних технологій у діяльності органів, які здійснюють фінансування соціального забезпечення громадян залишає бажати кращого. Вказані органи недостатньо використовують потенціал інформаційних технологій. З метою підвищення ефективності впровадження інформаційних технологій необхідно вживати заходів щодо автоматизації та інформатизації усіх напрямів діяльності у сфері фінансування соціального забезпечення.

Список літератури

1.Закону України від 09.01.2007 № 537-V «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/537-16.

2.Продукти Інформаційно-обчислювального центру [Електронний ресурс]. – Режим доступу : http://www.mlsp.gov.ua/labour/control/uk/publish/article%3Bjsessionid=B6FD962ECE0162F6818F4D0ACE0EC90E?art_id=38045&cat_id=35150.

3.Розпорядження Кабінету Міністрів України від 14.09.2016 № 672-р «Про схвалення Стратегії модернізації та розвитку Пенсійного фонду України на період до 2020 року» [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/ru/672-2016-%D1%80.

4.Василь Шевченко: Усі процеси надання соціальної допомоги будуть максимально автоматизовані [Електронний ресурс]. – Режим доступу : http://www.mlsp.gov.ua/labour/control/uk/publish/article;jsessionid=B05EE56C537BF07346D0626FF7CED140.app1?art_id=175588&cat_id=107177.

5.Автоматизація інформаційна система державного казначейства України Електронний ресурс]. – Режим доступу : http://constantine-mf.blogspot.com/2010/01/blog-post.html.

6.Концепція розвитку інформаційних технологій Державної казначейської служби України на 2015-2017 роки [Електронний ресурс]. – Режим доступу : http://desn.gov.ua/index.php?option=com_content&view=article&id=13046%3A----------2015-2017-----le-treasuryr&catid=481%3A2015-08-06-11-54-00&Itemid=3172&lang=ua.

Кузьменко Б.В. –
професор кафедри комп'ютерно-інтегрованих технологій Таврійського національного університету ім. В.І. Вернадського, доктор технічних наук, професор

КІБЕРВІРУСИ ВІЙСЬКОВОГО ТА СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

До 2012 року сталися всього два випадки використання кіберзброї – Stuxnet і Duqu. Проте їх аналіз привів до того, що теоретичне уявлення про те, що таке «кібервійна», у ІТ-співтовариства значно розширилося. Події 2012 року не лише збільшили число реальних інцидентів з кіберзброєю у декілька разів, але і виявили давню і серйозну залученість в розробку кіберозброєнь багатьох країн світу. Те, що раніше залишалося предметом секретних розробок і ідей, в 2012 році активно

обговорювалося в засобах масової інформації. Більше того, в 2012 році тема кібервійн стала одним з головних в публічних обговореннях офіційних представників різних держав.

Таким чином, можна з упевненістю сказати, що рік став переломним в цій області, не лише по кількості інцидентів, але і з точки зору формування загального погляду на розвиток кіберзброї. представників різних держав.

Таким чином, можна з упевненістю сказати, що рік став переломним в цій області, не лише по кількості інцидентів, але і з точки зору формування загального погляду на розвиток кіберзброї, [1,2].

У 2012 році зона застосування кіберзброї розширилася: якщо раніше це був один Іран, то тепер вона охоплює увесь прилеглий до нього регіон Західної Азії. І така динаміка є точним відображенням політичних процесів, що відбуваються в цьому регіоні, що давно вже є «гарячою точкою». І без того непросту обстановку в регіоні, яка склалася внаслідок іранської ядерної програми, в 2012 році доповнили політичні кризи в Сирії і Єгипті. Лівані, Палестинській автономії, хвилювання у ряді країн Персидської затоки доповнюють загальну картину нестабільності. У цих умовах цілком логічне прагнення інших держав світу, що мають інтереси в регіоні, використати усі можливі інструменти - як для захисту своїх інтересів, так і для збору інформації. Усе це привело до того, що в регіоні сталося декілька серйозних інцидентів, аналіз яких дозволяє класифікувати їх як використання кіберзброї.

Duqu. Шкідлива програма-шпигун, виявлена у вересні 2011 року і розкрита в публікаціях в жовтні, стала об'єктом дослідження експертів «Лабораторії Касперского». В ході його вдалося отримати доступ до ряду серверів управління, використаних Duqu, і зібрати значний об'єм інформації про архітектуру програми і її історії. Було безперечно доведено, що Duqu є розвитком платформи Tilded, на якій був створений і інший відомий черв'як, – Stuxnet. Крім того, було встановлено існування ще як мінімум трьох програм, що використали єдину з Duqu/Stuxnet базу, які досьогодні не виявлені. Така увага і активність дослідників привели до того, що оператори Duqu спробували знищити усі сліди своєї роботи з серверів

управління, а також із заражених систем. За станом на кінець 2011 року Duqu перестав існувати «в дикій природі», проте у кінці лютого 2012 року експерти Symantec виявили в Ірані новий варіант драйвера, аналогічного використаному в Duqu, але створений вже 23 лютого 2012 року. Сам основний модуль виявлений не був, і після цього, до теперішнього часу, нових модифікацій Duqu не було виявлено.

Wiper. «Містична» Троя у кінці квітня 2012 року сильно стривожила Іран: з'явившись невідомо звідки, він (комп'ютерний вірус) знищив безліч баз даних в десятках організацій. Одним з тих, хто найбільше постраждав від нього, став найбільший в Ірані нафтовий термінал, робота якого була зупинена на декілька днів через те, що були знищені дані про нафтові контракти. Проте не було знайдено жодного зразка шкідливої програми, використаної в цих атаках, що багатьох змусило засумніватися в точності відомостей, що містяться в повідомленнях ЗМІ. У зв'язку з цими інцидентами Міжнародний союз електрозв'язку (МСЕ) звернувся до «Лабораторії Касперского» з проханням провести їх розслідування і визначити потенційні деструктивні наслідки активності цього нового шкідливого ПЗ. Творці Wiper зробили усе можливе, щоб знищити абсолютно усі дані, які можна було б використати для аналізу інцидентів. Тому ні в одному з випадків, які були проаналізовані, після активації Wiper від шкідливої програми не залишилося майже ніяких слідів. В процесі розслідування таємничої квітневої шкідливої атаки вдалося отримати і проаналізувати образи декількох жорстких дисків, атакованих Wiper. Можна з упевненістю стверджувати, що інциденти дійсно мали місце і що шкідлива програма, використана в цих атаках, існувала в квітні 2012 року. Крім того, було відомо про декілька дуже схожих інцидентів, що мали місце з грудня 2011 року. В основному атаки відбувалися в останню декаду місяця (у період з 21 по 30 число), проте не було підстав стверджувати, що причина цього криється в спеціальній функції, що активується при настанні певної дати. Через декілька тижнів після початку розслідування так і не вдалося знайти файли шкідливого ПЗ, властивості якого співпадали б з відомими характеристиками Wiper. Проте була виявлена кампанія, що

проводилася на державному рівні, по киіершпигунству, відому сьогодні як Flame, а пізніше – ще одну систему кибершпигунства, що дістала назву Gauss.

Flame. Flame є дуже хитрим набором інструментів для проведення атак, що значно перевершує по складності Duqu. Це троянська програма – бекдор, що має також риси, властиві черв'яка і що дозволяють їй поширюватися по локальній мережі і через знімні носії при отриманні відповідного наказу від її хазяїна. Після зараження системи Flame приступає до виконання складного набору операцій, у тому числі до аналізу мережевого трафіку, створення знімків екрану, аудіозапису розмов, перехоплення клавіатурних натиснень і так далі. Усі ці дані доступні операторам через командні сервери Flame. Надалі оператори можуть прийняти рішення про завантаження на заражені комп'ютери додаткових модулів, що розширюють функціонал Flame. Всього було виявлено близько 20 модулів. У чому секрет ефективності і комп'ютерних вірусів і запальних боєприпасів? Та в тому, що вони використовують те, що вже запасене жертвою/супротивником. Є на світі така організація - Міжнародний союз електрозв'язку International Telecommunication Union. Її історія сходить аж до позаминулого століття. І у колиски її стояли двоє – Інформаційні технології і Глобалізація. Вірус «Полум'я» – «напалм» для вашого комп'ютера. Flame містив в собі унікальну функцію поширення по локальній мережі, з використанням методу перехоплення запитів Windows на отримання оновлень і підміни їх власним модулем, підписаним сертифікатом Microsoft. Дослідження цього сертифікату виявило використання унікальної криптоатаки, яка дозволила зловмисникам згенерувати власний підробний сертифікат, що повністю відповідає легальному. Зібрані дані свідчать про те, що розробка Flame почалася приблизно в 2008 році і активно тривала аж до моменту виявлення в травні 2012 року. Більше того, вдалося встановити, що один з модулів на платформі Flame був використаний в 2009 році в якості модуля поширення черв'яка Stuxnet. Цей факт доводить наявність тісного співпраці між двома групами розробників платформ Flame і Tilded, аж до рівня обміну початковими кодами.

Gauss. Після виявлення Flame було реалізовано декілька евристичних методів, грунтованих на аналізі схожості коду і досить скоро це принесло черговий успіх. В середині червня була виявлена ще одна шкідлива програма, створена на платформі Flame, проте що відрізняється по функціоналу і ареалу поширення. Gauss – це складний комплекс інструментів для здійснення кібершпигунства, реалізований тією ж групою, що створила шкідливу платформу Flame. Комплекс має модульну структуру і підтримує видалене розгортання нового функціонала, який реалізується у вигляді додаткових модулів. Відомі на сьогодні модулі виконують наступні функції:

– перехоплення cookie- файлів і паролів у браузері;

– збір і відправка зловмисникам даних про конфігурацію системи;

– зараження USB- носіїв модулем, призначеним для крадіжки даних;

– створення списків вмісту системних накопичувачів і тек;

– крадіжка даних, необхідних для доступу до облікових записів різних банківських що діють на Близькому Сході;

– перехоплення даних по облікових записах в соціальних мережах, поштовим сервісам і системам миттєвого обміну повідомленнями.

Модулі мають внутрішні імена, які, очевидно, дані на честь знаменитих математиків і філософів, таких як Курт Гедель, Йоганн Карл Фрідріх Гаусс і Жозеф Луї Лагранж. Виходячи з результатів аналізу і тимчасових міток наявних в розпорядженні шкідливих модулів, зроблено висновок, що Gauss почав функціонувати в серпні-вересні 2011 року. Починаючи з кінця травня 2012 року хмарним захисним сервісом «Лабораторії Касперского» зареєстровані більше 2500 заражень Gauss; при цьому, за оцінкою, загальне реальне число жертв шкідливої програми вимірюється десятками тисяч. Абсолютна більшість жертв Gauss виявилися на території Лівану. Є також жертви в Ізраїлі і Палестині. Крім того, невелике число потерпілих зареєстроване в США, ОАЄ, Катарі, Йорданії, Німеччині і Єгипті.

miniFlame. На початку липня 2012 року, коли було виявлено невеликий, але цікавий модуль на платформі Flame. Ця шкідлива програма, яку називають miniFlame, є невеликим за розміром повнофункціональним шпигунським модулем, призначеним для крадіжки інформації і безпосереднього доступу до зараженої системи. На відміну від Flame і Gauss, які використовувалися для великомасштабних шпигунських операцій із зараженням тисяч користувачів, miniFlame/SPE - інструмент для хірургічно точних атак. miniFlame дійсно грунтований на платформі Flame, але реалізований у вигляді незалежного модуля, здатного функціонувати і самостійно, без наявності в системі основних модулів Flame, і в якості компонента, керованого Flame. Примітним фактом є використання miniFlame в комплекті з іншою шпигунською програмою – Gauss. Судячи з усього, розробка miniFlame почалася кілька років тому і тривала до 2012 року. Згідно з кодом серверів управління, протоколи для обслуговування SP і SPE були створені раніше або одночасно з протоколом роботи для FL (Flame), а це означає як мінімум 2007 рік. Основне призначення miniFlame – виконувати функції бекдора на заражених системах, забезпечуючи можливість безпосереднього управління ними з боку тих, що атакують.

Назва	Число інцидентів (статистика ЛК)	Число інцидентів (приблизне)
Stuxnet	Більше 100 000	Більше 300 000
Gauss	~ 2500	~10 000
Flame (FL)	~ 700	~5000-6000
Duqu	~20	~50-60
miniFlame (SPE)	miniFlame (SPE)	~50-60

Досвід виявлення і дослідження усіх вищеописаних шкідливих програм, дозволяє нам сформулювати наступний погляд на сучасні загрози і їх класифікацію. Найбільш точним відображенням поточного стану справ є представлення у вигляді

піраміди. У її основі знаходиться найрізноманітніші загрози. Це те, що ми називаємо «традиційною» кіберзлочинністю. Її відмінними рисами є масовість атак і націленість на звичайних користувачів. Основною метою зловмисників є отримання прямої фінансової вигоди. Банківські троянці, клікери, ботнети, здирники, мобільні загрози і т. п. Усе це складає більше 90% від загальної кількості сучасних загроз. На другому рівні розташовані загрози для організацій. Це цільові атаки. Тут і промислове шпигунство, і цільові хакерські атаки, завдання яких дискредитувати жертву. Ті, що атакують вузько спеціалізуються або під конкретну мету, або під конкретного замовника. Мета – крадіжка інформації, інтелектуальної власності. Безпосередня фінансова вигода не є прямою метою тих, що атакують. У цю ж групу ми включаємо різні види шкідливих програм, що створюються деякими компаніями за замовленням правоохоронних органів різних країн і практично відкрито пропонованих на продаж, наприклад розробки компаній Gamma Group, Hacking Team SRL. Третій рівень, верхня частина піраміди, зайнятий тим ПЗ, яке можна класифікувати саме як «кіберзброя». Сюди відносяться шкідливі програми, створення і фінансування яких здійснюється державними структурами різних країн світу. Ці шкідливі програми застосовуються проти громадян, організацій і відомств інших країн світу. На основі усіх відомих нам зразків подібних програм, ми можемо виділити три основні групи загроз в цій категорії: «Руйнівники». Це програми, які призначені для знищення баз даних і інформації в цілому. Можуть бути реалізовані у вигляді «логічних бомб», або заздалегідь впроваджених в системи і таких, що спрацьовують в певний момент часу, або в ході цілеспрямованої атаки з моментальним виконанням. Найбільш близьким прикладом подібної програми є Wiper. Шпигунські програми. У цю групу потрапляють Flame, Gauss, Duqu, miniFlame. Їх основною метою є збір усієї можливої інформації, в основному дуже специфічної (наприклад, дані проектів Autocad, SCADA- систем і так далі), яка потім може бути використана для створення інших груп загроз. Інструменти кібердиверсії. Це вища форма кіберзброї - загрози, в результаті дій яких об'єкту атаки буде нанесений

фізичний збиток. Зрозуміло, в цю категорію потрапляє черв'як Stuxnet. Цей вид загроз є унікальним і його застосування бачиться є рідкісним явищем, проте з кожним роком все більше і більше зусиль різних держав будуть спрямовано як на розробку саме такого виду загроз, так і на створення захисту від них.

Список літератури

1.Кузьменко Б.В., Заіка Ю.О. Кібертероризм: світові й українські реалії. – Науковий вісник Академії внутрішніх справ, №2(81)2012, с. 92-98.

2.Кузьменко Б.В., Заіка Ю.О. Типи сучасного особливо небезпечного (шкідливого) програмного забезпечення: правові та технічні аспекти. – Юридична наука, №7, 2013, с. 29-35.

Малиновська Ю.Б. –
асистент кафедри зовнішньоекономічної та митної діяльності Навчально-наукового інституту економіки та менеджменту Національного університету «Львівська політехніка»

Мороз Н.С. –
фахівець деканату повної вищої освіти Навчально-наукового інституту права та психології Національного університету «Львівська політехніка»,

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНИХ ВІДНОСИН

З-поміж низки проблем в галузі інформаційної безпеки особливе місце займає правова. Особливість цієї проблеми полягає в тому, що інформаційні відносини можна розглядати як складові всіх інших відносин – матеріальних, духовних, інтелектуальних тощо. І в той же час їх можна розглядати як суто інформаційні відносини, незалежно від об’єктивного складу. Недосконаліть правового регулювання інформаційних відносин гальмує як розвиток і вдосконалення політичних, економічних, матеріальних та інших відносин у суспільстві, так і, власне, сам процес забезпечення інформаційної безпеки держави. Очевидно, що це, особливо в сучасних умовах нашого

суспільства (перехідний період, ламання старих і створення нових підвалин зовнішньої і внутрішньої політики, зростання ролі загальнолюдських цінностей та ін.), визначає необхідність швидкого вирішення правових проблем інформаційних відносин.

Проблема створення законодавчої бази в інформаційній сфері не нова. Найбільш розвинута система законодавства у згаданій сфері в США. У цій країні законодавчі акти створювались послідовно, у міру виникнення відповідних проблем. Загальна їх кількість сягає кількох сотень. Не менш інтенсивно ведеться робота в цьому напрямі і в європейських країнах.

Для країн Східної Європи характерне значне відставання в галузі правового регулювання інформаційних відносин. Нерозуміння важливості цих проблем позначилося на тому, що в національних законодавствах не так активно організовувалась і велась законотворча робота в цій галузі.

В Україні також була проведена певна робота зі створення низки законів. Сьогодні діє базовий закон «Про інформацію», прийняті кілька законів, які можна віднести до спеціальних в цій галузі – «Про державну статистику», «Про науково-технічну інформацію», «Про національний архівний фонд і архівні установи», «Про державну таємницю», «Про захист інформації в автоматизованих системах», «Про Державну службу спеціального зв'язку та захисту інформації України» та інші.

Крім цього, є окремі норми в складі законодавчих актів різних видів і рівнів, за допомогою яких зроблена спроба врегулювати інформаційні відносини в різних предметних галузях. Це такі закони як: «Про оперативно-розшукову діяльність», «Про Службу безпеки України», «Про нотаріат», «Про адвокатуру», «Про цивільну оборону України», «Про організаційно-правові основи боротьби з організованою злочинністю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України та низка інших нормативно-правових та підзаконних актів.

Аналіз чинних законодавчих актів показує, що незважаючи на прогресивну роль у становленні основ правової

бази інформаційних відносин у державі сьогодні, вони починають гальмувати не тільки становлення цивілізованих інформаційних відносин, але й інші суспільні відносини, у тому числі й процес забезпечення інформаційної безпеки, і тому потребують достатньо термінового і суттєвого доопрацювання.

Упорядкування і розвиток існуючої, а також створення нової законодавчої бази в галузі інформаційних відносин потребує системного підходу.

У першу чергу, необхідно вирішити такі проблеми:

– правове визначення інформації, як стратегічно важливого для держави ресурсу;

– визначення взаємопов'язаної системи інформаційних масивів держави різного рівня і призначення, а також державних органів, відповідальних за формування, зберігання, використання і захист цих масивів;

– визначення прав, обов'язків, гарантій забезпечення прав і відповідальності суб'єктів інформаційних відносин в різних прикладних галузях;

– визначення раціонального монопольного і немонопольного сполучення в інформаційній сфері;

– ліцензування і сертифікація окремих видів інформаційної діяльності і продукції;

– створення на основі понять інтелектуальної власності системи захисту авторських, майнових прав на різні інформаційні продукти, на засоби обробки інформації;

– чіткого законодавчого визначення виду, типу, обсягу інформації з обмеженим доступом, визначення процедур віднесення до такої інформації і зняття обмежень, визначення прав, обов'язків і відповідальності суб'єктів інформаційних відносин у питаннях категорування такої інформації, її використання й охорони;

– створення загальної системи забезпечення інформаційної безпеки.

Мороз Н. С. –
фахівець деканату повної вищої освіти
Навчально-наукового інституту права та психології
Національного університету «Львівська політехніка»,

ПРИНЦИПИ КОНТРОЛЮ У СФЕРІ ІНФОРМАТИЗАЦІЇ

Сьогодні Стратегія сталого розвитку «Україна–2020» [1], Національна стратегія сприяння розвитку громадянського суспільства в Україні на 2016–2020 роки [2] визначають необхідність формування правової бази, яка свідчить про необхідність і неминучість контролю у сфері інформатизації.

Для реального і ефективного створення, збору, обробки та передачі інформації в процедурах контролю у сфері інформатизації діяльність його суб'єктів повинна відповідати таким принципам: 1) самостійності об'єднань громадян, що беруть участь у формуванні інститутів контролю; 2) самостійності суб'єктів контролю; 3) всеосяжності контролю; 4) загальності контролю; 5) гласності контролю; 6) обов'язковості контролю; 7) різноманіття форм контролю; 8) визнання суб'єктів контролю представниками невизначеного кола осіб, що діють на захист громадських інтересів.

Поле контролю в сфері інформатизації відкриває широкі горизонти для політичного маніпулювання громадськістю, а через неї і органами державного управління. Механізми дезінформації, подібні важелі впливу контролю в сфері інформатизації, опинившись доступними для громадських об'єднань з цілями, протилежними підтримці єдності та демократичних основ держави, можуть завдати істотної шкоди безпеці та незалежності країни. Можна тільки вітати цивілізовану роботу гуманітарних і благодійних неурядових організацій.

Принцип самостійності суб'єктів контролю у сфері інформатизації повинен знайти своє вираження у двох напрямах: відсутність відносин співпідпорядкованості між суб'єктами контролю в сфері інформатизації та створення умов для партнерства між ними для інформаційного обміну, надання взаємної допомоги та сприяння, об'єднання зусиль і ресурсів.

Принцип всеосяжності контролю в сфері інформатизації означає поширення контролю на діяльність органів державної влади, органів місцевого самоврядування, державних корпорацій та установ, правоохоронних, наглядових і судових органів, установ виконання покарання, Збройних Сил і спецслужб.

Актуальним питанням є поширення системи контролю в сфері інформатизації на діяльність недержавних установ, що використовують бюджетні асигнування або податкові пільги та своєю діяльністю зачіпають, тією чи іншою мірою, громадські інтереси. Така повсюдність упровадження процедур контролю в сфері інформатизації повинна бути заснована, насамперед, на суспільній значимості діяльності осіб і органів–власників інформації, що зачіпає інтереси суспільства.

Принцип загальності контролю в сфері інформатизації означає гарантованість можливості участі в процедурах контролю всім громадян, незалежно від статі, раси, національності, соціального походження та інших чинників. Контроль повинен бути доступний рівною мірою для всіх громадян, які бажають захищати суспільні інтереси. Інформація, яка становить суспільний інтерес, повинна бути доступна для всіх громадян. Цей принцип безпосередньо підтриманий в Конституції: громадяни України мають право брати участь в управлінні справами держави як безпосередньо, так і через своїх представників, а держава гарантує рівність прав і свобод людини та громадянина незалежно від статі, раси, національності, мови, походження, майнового та посадового становища, місця проживання, ставлення до релігії, переконань, належності до громадських об'єднань, а також інших обставин.

Принцип гласності контролю в сфері інформатизації, його абсолютна інформаційна відкритість. Ідея контролю в сфері інформатизації включає в себе активне та критичне спостереження за діяльністю органів державного управління та іншими об'єктами контролю в сфері інформатизації. Але виникає питання як буде забезпечуватися адекватність, об'єктивність і законність подібних процедур, і хто дасть гарантії, що не виникне зловживання і фальсифікації з боку суб'єктів контролю в сфері інформатизації? Тут відповідь може бути лише одна – тільки повна інформаційна відкритість і внутрішнє саморегулювання

дозволить забезпечити всі перераховані вище особливості контролю в сфері інформатизації. Цього можна домогтися шляхом створення електронного ресурсного центру контролю в сфері інформатизації [3].

Принцип обов'язковості контролю в сфері інформатизації – це гарантія його ефективності. Для того, щоб громадський контроль набрав своєї дії, він повинен бути повсюдним і обов'язковим.

Принцип різноманіття форм контролю в сфері інформатизації повинен забезпечуватися змогою визначати форму, структуру та найменування органів контролю в сфері інформатизації. Крім того, громадський контроль в різних регіонах може здійснюватися з урахуванням місцевих, національних, культурних і релігійних звичаїв і традицій [4].

До основних форм контролю в сфері інформатизації можна віднести громадські такі: слухання; обговорення; експертиза; перевірка; розслідування; моніторинг; ініціатива як особлива форма контролю в сфері інформатизації та інші форми. Крім того, слід мати на увазі особливості здійснення контролю в сфері інформатизації в окремих сферах, що мають свою специфіку. У кожній сфері можуть виникати притаманні лише їй форми контролю в сфері інформатизації.

Принцип визнання суб'єктів контролю в сфері інформатизації представниками невизначеного кола осіб, що діють на захист громадських інтересів.

Введення в національне право універсального інституту захисту інтересів невизначеного кола осіб (суспільного інтересу) дозволить озброїти громадян прямим і легітимним інструментом впливу на владу. Тут важливо окремо зупинитися на формуванні поняття суспільних інтересів. Сьогодні таке визначення, на жаль, у вітчизняному законодавстві відсутнє, хоча посилання на громадські інтереси у тексті нормативно-правових актів зустрічаються часто (наприклад, Закон України «Про доступ до публічної інформації).

Аргументом на користь необхідності визначення поняття «суспільний інтерес» на рівні державного законодавства, слід зазначити те, що прогалини в праві, як-от відсутність визначення такого правового явища як суспільний інтерес,

відкривають куди більше поле для порушень закону, аніж наявність хай не ідеального, але закріпленого законодавчого визначення, яке буде мати офіційне тлумачення, що внесе ясність у правозастосування. Тому, на нашу думку, доцільно закріпити в законодавстві таке визначення суспільних інтересів як: «суспільні інтереси – це законні інтереси громадян, пов'язані із забезпеченням їхньої безпеки і благополуччя, стабільного і стійкого розвитку суспільства».

Деякі дослідники доповнюють наведений вище набір принципів, включаючи в нього: справедливість, об'єктивність, доказовість, громадянську активність, динамічність.

Ми не включаємо до цього переліку принцип незалежності самого контролю в сфері інформатизації, оскільки на відміну від принципу самостійності, незалежність має на увазі відсутність взаємозв'язку з будь-якими структурами, здатними надати зовнішній вплив на процедури, що описуються. Вплив може бути і негативним, і позитивним. У нашому випадку, кажучи про контроль, ми враховуємо, що він неможливий без співпраці громадськості з органами державного управління, сприяння яких процедурі контролю в сфері інформатизації є їх обов'язковістю. Повинен бути гарантований вільний обмін інформацією. Тому в цьому випадку принцип незалежності не повною мірою відображає характер правовідносин, що виникають при здійсненні процедур контролю в сфері інформатизації.

Список літератури

1. Про Стратегію сталого розвитку «Україна–2020»: Указ Президента України від 12.01.2015 № 5/2015 // [Електронний ресурс]. – Режим доступу: [http://zakon0.rada.gov.ua/laws/show/5/2015].

2. Про сприяння розвитку громадянського суспільства в Україні Національній стратегії сприяння розвитку громадянського суспільства в Україні на 2016-2020 роки: Указ Президента України від 26.02.2016 №68/2016 // [Електронний ресурс]. – Режим доступу: [http://zakon5.rada.gov.ua/laws/show/68/2016].

3. Єсімов С.С. Формування єдиного інформаційного простору в діяльності державних органів України / С.С. Єсімов // Вісник Національного університету «Львівська політехніка». Серія. Юридичні науки. – 2015. – № 813. – С. 48–53.

4. Shah A. The Right to Know / A. Shah // Journal of Malaysian and Comparative Law. – 1986. – Vol. 13. – P. 12–17.

***Нерсесян А.С.* –**
старший науковий співробітник Інституту держави і права
ім. В.М. Корецького НАН України,
кандидат юридичних наук, адвокат

ЗБЕРЕЖЕННЯ КОМЕРЦІЙНОЇ ТАЄМНИЦІ СУБ'ЄКТА ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Одним із найважливіших прав суб'єкта господарської діяльності є право на комерційну таємницю. Розуміння важливості цього права вже досить давно існує на міжнародному рівні. Так, частиною 2 ст. 39 Угоди про торговельні аспекти прав інтелектуальної власності (Угода TRIPS) встановлено, що фізичні та юридичні особи повинні мати можливість перешкоджати тому, щоб інформація, яка законно знаходиться під їх контролем, розголошувалась, збиралась або використовувалась іншими особами без їхньої згоди у такий спосіб, який суперечить чесній комерційній практиці, якщо така інформація:

– є секретною у тому розумінні, що вона як єдине ціле або у точній сукупності та поєднанні її компонентів не є загальновідомою або доступною для осіб у колах, що звичайно мають справу з інформацією, про яку йдеться;

– має комерційну цінність через те, що вона є секретною;

– зберігається у секреті внаслідок вжиття за відповідних обставин певних заходів особою, яка законно здійснює контроль за цією інформацією.

При цьому «спосіб, який суперечить чесній комерційній практиці» означає принаймні таку практику, як порушення контракту, порушення довіри та спонукання до порушення, і включає придбання інформації, що не підлягає розкриттю третіми сторонами, які знали або не могли не знати, що з цим придбанням пов'язана така практика [5].

На законодавчому рівні питання захисту комерційної таємниці також належним чином врегульоване нормами цивільного та господарського законодавства. Зокрема, ст. 505 ЦК України визначає, комерційною таємницею є інформація,

яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Пунктом 3 ч. 1 ст. 506 ЦК України встановлене виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці [6].

Дані форми порушення прав на комерційну таємницю визначені нормами ч.ч. 2-5 ГК України. Зокрема, неправомірним збиранням відомостей, що становлять комерційну таємницю, вважається добування протиправним способом зазначених відомостей, якщо це завдало чи могло завдати шкоди суб'єкту господарювання. Розголошенням комерційної таємниці є ознайомлення іншої особи без згоди особи, уповноваженої на те, з відомостями, що відповідно до закону становлять комерційну таємницю, особою, якій ці відомості були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків, якщо це завдало чи могло завдати шкоди суб'єкту господарювання. Схилянням до розголошення комерційної таємниці є спонукання особи, якій були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків відомості, що відповідно до закону становлять комерційну таємницю, до розкриття цих відомостей, якщо це завдало чи могло завдати шкоди суб'єкту господарювання. Неправомірним використанням комерційної таємниці є впровадження у виробництво або врахування під час планування чи здійснення підприємницької діяльності без дозволу уповноваженої на те особи неправомірно здобутих відомостей, що становлять відповідно до закону комерційну таємницю.

За неправомірне збирання, розголошення або використання відомостей, що є комерційною таємницею, винні особи несуть відповідальність, встановлену законом [1].

Така відповідальність встановлюється, зокрема, встановлено ч. 3 ст. 164-3 КУпАП, яка передбачає відповідальність за отримання, використання, розголошення комерційної таємниці, а також іншої конфіденційної інформації з метою заподіяння шкоди діловій репутації або майну іншого підприємця, що тягне за собою накладення штрафу від дев'яти до вісімнадцяти неоподатковуваних мінімумів доходів громадян [2].

Кримінальна відповідальність за незаконні дії з комерційною таємницею встановлено ст.ст. 231, 232 КК України. Так, ст. 231 КК визначає, що умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності караються штрафом від трьох тисяч до восьми тисяч неоподатковуваних мінімумів доходів громадян.

Стаття 232 КК встановлює відповідальність у вигляді штрафу від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років за умисне розголошення комерційної або банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності [3].

Серед суб’єктів злочинного розголошення комерційної таємниці є співробітники органів кримінальної юстиції. Так, ч. 1 ст. 159 КПК України надає стороні кримінального провадження право тимчасового доступу до речей і документів, який полягає у наданні стороні кримінального провадження особою, у володінні якої знаходяться такі речі і документи, можливості ознайомитися з ними, зробити їх копії та вилучити їх (здійснити їх виїмку). Тимчасовий доступ до електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку

здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення.

При цьому, відповідно до п. 6 ст. 160 КПК України, у клопотанні про тимчасовий доступ до речей і документів сторона кримінального провадження має зазначити можливість використання як доказів відомостей, що містяться в речах і документах, та ***неможливість іншими способами довести обставини,*** які передбачається довести за допомогою цих речей і документів, у випадку подання клопотання про тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю. До таких видів таємниць відноситься також конфіденційна інформація, в тому числі така, що містить комерційну таємницю (п. 4 ч.1 ст. 162 КПК України).

Частина 1 ст. 166 КПК України встановлює, що у разі невиконання ухвали про тимчасовий доступ до речей і документів слідчий суддя, суд за клопотанням сторони кримінального провадження, якій надано право на доступ до речей і документів на підставі ухвали, має право постановити ухвалу про дозвіл на проведення обшуку згідно з положеннями цього Кодексу з метою відшукання та вилучення зазначених речей і документів [4].

У нормах ст.ст. 234-236 КПК про обшук не врегульоване питання збереження комерційної таємниці, що в умовах тотальної корумпованості органів досудового розслідування дає потужний інструмент для рейдерських захоплень. При цьому отримання стороною кримінального провадження (зокрема, слідчого) комерційної таємниці в процесі обшуку або тимчасового доступу до речей та документів фактично надає даній особі статус суб’єкта злочину передбаченого ст. 232 КК України.

Відтак, для вдосконалення правового захисту комерційної таємниці слід встановити прямий обов’язок прокурора (ст. 36 КПК), слідчого (ст. 40 КПК) та оперативних підрозділів (ст. 41), а також інших осіб яким надано тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю зберігати дану таємницю та нести відповідальність за її розголошення.

Список літератури

1.Господарський кодекс України // Голос України. – 2003. – № 49-50.

2.Кодекс України про адміністративні правопорушення // Ліга. Закон [Електронний ресурс] – Режим доступу: https://ligazakon.net/document/view/KD0005?an=1629

3.Кримінальний кодекс України // Офіційний вісник України. – 2001. – № 21. – ст. 92.

4.Кримінальний процесуальний кодекс України // Голос України. – 2012. – № 90-91.

5.Угода про торговельні аспекти прав інтелектуальної власності // Офіційний вісник України. – 2010 р. – № 84. – С. 503.

6.Цивільний кодекс України // Офіційний вісник України. – 2003 р. – № 11 – С. 461

Новицький А. М. –
професор кафедри цивільного права та процесу
Навчально-наукового інституту права
Університету Державної фіскальної служби України,
доктор юридичних наук, професор

МІСЦЕ ІТ-ПРАВА В ЗАГАЛЬНІЙ СИСТЕМІ ІНФОРМАЦІЙНОГО ПРАВА

Розвиток нових суспільних відносин, пов’язаних із інформатизацією останнім часом займає все більш розповсюдженого характеру не тільки в окремим галузях економіки країни а і у повсякденному житті пересічних громадян. Все більше адміністративних послуг переходить в розряд електронних, все більше елементів звичайних відносин називають цифровими чи електронними (як то електронні гроші, електронна торгівля, електронний банкінг тощо). Виникає закономірність – нові суспільні відносини повинні бути врегульовані певними нормами, прийнятними для всіх учасників даних відносин.

Існує декілька способів виникнення правових норм, що пов’язані із генезисом відносин та відповідним приведенням складених традицій до відповідної норми права. Інший спосіб правотворчості пов’язаний із глобалізацією відносин, відповідно до якого, держава змушена приймати певні норми, які нав’язані

міжнародною спільнотою та впроваджуються із політичних мотивів тощо.

Говорячи про норми права, що регулюють суспільні відносини в сфері ІТ України можемо констатувати різні види формування правових норм:

– ті, що склались історично(«Про інформацію»);

– ті, що були прийняті на вимогу світової спільноти (ЗУ «Про електронний цифровий підпис», «Про електронні документи та електронний документообіг»;

– ті, що прийняті на вимогу розвитку індустрії (ЗУ «Про Національну програму інформатизації»).

В залежності від способу виникнення правової норми залежить і її впровадження, відповідно, і зацікавленість щодо негайної реалізації норми права.

Говорячи про ІТ-право необхідно зазначити, що всі перелічені способи виникнення правової норми є прийнятними. А сам напрямок ІТ-права досить швидкими темпами розвивається в Україні, і стає одним із самих перспективних напрямів підготовки юристів для роботи в зазначеній сфері.

Для нашої держави постає нагальним питання врегулювання суспільних відносин в зазначеній сфері, адже за даними Exploring Ukraine IT Outsourcing Industry 2012, Україна посідає четверте місце в світі за кількістю сертифікованих ІТ-фахівців після США, Росії та Індії [1].

В Україні сформувалось стале визначення поняття ІТ-право, яке врегульовує питання правового забезпечення функціонування ІТ-сфери, встановлює правове регулювання суспільних відносин суб'єктів зазначених відносин, визначає права та обов'язки учасників та відповідальність за порушення норм права, визначає державну політику в зазначеній сфері. В той же час, практично неможливо виокремити ІТ право, як окремий галузевий чи інституціональний елемент структури права.

Доктринально склалось, що норми права, які регулюють відносини в ІТ-сфері, відносяться до інформаційного права, та займають чільне місце в його структурі. В теорії наукових досліджень відзначається, що структуризація системи є

необхідною умовою її вивчення, та дозволяє виділити, а потім описати її суттєві ознаки, визначити спільні характерні особливості, притаманні всім елементам правової науки та встановити особливі, характерні лише для інформаційного права особливості правового регулювання. Поглиблене дослідження структури інформаційного права, як системи, дасть можливість показати цілісність такої системи та визначити рівні відповідності окремих інститутів. В той же час, багато спеціальних норм, що регулюють конкретно питання функціонування ІТ-сфери, за своєю будовою, особливістю формування та галузевою належністю становлять елементи господарського права, фінансового (податкового) права, кримінального, цивільного права та інших галузей права.

Аналізуючи структуру інформаційного права викладену схематично, можемо сказати про комплексну, взаємопов'язану та цілісну систему суспільних відносин.

Рис. 1

У даній системі визначено Інформатизаційне право, як структурна одиниця інформаційного права. Я навмисно не визначав цю структурну одиницю як ІТ-право, так як воно не відображає всього спектру відносин, які регулює історично складена структура ІТ-права, що регламентує різноманітні сфери ІТ-галузі.

Наведу приклад формування спеціальної норми, що регламентує відносини в ІТ-сфері: обіг електронних грошей. По своїй суті, електронні гроші це продукт генезису, розвитку платіжних доручень, якими виступають звичайні гроші. Входження нового виду грошей – а саме їх електронного виразу викликали ряд проблем, які визначались різними галузями права по-різному. Для представників інформаційного права – як забезпечити рівність платежів у електронній та готівковій формі, як забезпечити надійність функціонування системи інформаційного захисту, як визначити місце електронних грошей в системі електронного документообігу тощо. В той же час, представників фінансового права більше цікавили питання віднесення електронних платежів до готівкового чи безготівкового обігу, визнання електронних грошей як категорії платіжних доручень, чи як форми здійснення платежів і тд.

Всі питання, які виникають є актуальними і регулюють одну сферу, тому їх не можна ігнорувати. Відповідно, більшість відносин, які на перший погляд визначають сферу ІТ-права, як правило, регулюється встановленими правовими нормами, які ускладнені інформатизаційними особливостями їх застосування.

Тому можна з впевненістю говорити про формування специфічний міжгалузевих особливостей правового регулювання відносин у сфері ІТ.

Список літератури

1.Украина стала первой страной в Европе по количеству IT-специалистов / http://zn.ua/TECHNOLOGIES/ukraina-stala-pervoy-stranoy-v-evrope-po-kolichestvu-it-specialistov-207911_.html

Ортинський В. Л. –
директор Навчально-наукового інституту права та психології Національного університету «Львівська політехніка», доктор юридичних наук, професор

ПРІОРИТЕТИ ТА НАПРЯМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Водночас, переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною, здатною завдати значної шкоди інтересам особи, суспільства і держави.

Указом Президента України від 27 січня 2016 р. затверджено «Стратегію кібербезпеки України» [3]. Основною метою Стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

У Стратегії передбачено комплекс заходів, пріоритетів та напрямів забезпечення кібербезпеки в Україні, зокрема розвиток безпечного, стабільного і надійного кіберпростору; кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки

інформації, вимога щодо захисту якої встановлена законом; кіберзахист критичної інфраструктури; розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки; боротьба з кіберзлочинністю.

Крім цього, для забезпечення кібербезпеки, необхідне залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки, здійснення заходів державної підтримки стратегічно важливих для кібероборони держави наукових установ і організацій, проведення наукових досліджень у галузі кібербезпеки та кіберзахисту для потреб національної безпеки і оборони та підвищенні цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту [2-3].

«Кіберпростір має стати одним з елементів нашої асиметричної відповіді на агресію РФ, дієвим фронтом нашого опору», – зазначає Володимир Горбулін, директор Національного інституту стратегічних досліджень. За його словами, держава має для цього майже все необхідне, а чого немає у держави, є у його громадян [1].

У 2016 р. Україна посіла перше місце в Європі за кількістю ІТ-фахівців. Понад 100 тисяч українських програмістів працюють в різних компаніях, а попит на ІТ-фахівців на світовому ринку продовжує рости. Кількість ІТ-спеціалістів в Україні є найбільшим і найбільш швидко зростаючим у Європі. Очікується, що до 2020 року кількість ІТ-фахівців в країні наблизиться до позначки 200 тисяч [4].

Взагалі, варто поставитися серйозніше до різноманітних заходів, котрі сприяють зацікавленості молоді кібербезпековою проблематикою. Нам потрібні як уже згадані національні кіберзмагання, так і регулярні хакатони та інші види заходів, де безпекові відомства зможуть відбирати для себе молодих фахівців на реальній конкурентній основі.

Слід шукати та впроваджувати ефективні форми використання вітчизняних програмних і технічних напрацювань у розвитку кібербезпекового потенціалу держави. Одразу кілька потужних ВНЗ України (Національний університет «Львівська політехніка», Національний технічний університет України «Київський політехнічний інститут», Київський національний університет ім. Т. Шевченка, Харківський національний університет радіоелектроніки та ін.) готують високо-кваліфікованих фахівців і вже мають відповідні технічні напрацювання, що можуть і повинні бути впроваджені у вітчизняний сектор кібербезпеки. Власне, йдеться про формування комплексного програмного та конструкторського забезпечення функціонування державної системи кібернетичної безпеки України як пріоритетного напряму забезпечення державної безпеки України.

Список літератури

1. Горбулін В. У пошуках асеметричних відповідей: кіберпростір у гібридній війні // Дзеркало тижня. – № 6. - 20 лютого 2015 р.

2. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07 червня 2016 р. № 242/2016 // Офіційний вісник України. – 2016. - № 17. – Ст. 468.

3. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. № 96/2016 // Офіційний вісник України. – 2016. – № 10. – Ст. 39.

4. Report: Ukraine has become Europe’s #1 IT outsourcing and software development powerhouse [Електронний ресурс]. – Режим доступу: http://itonews.eu/report-ukraine-powerhouse/

Остапенко О.І. –
професор кафедри адміністративного та інформаційного права Навчально-наукового Інституту права та психології Національного університету «Львівська політехніка», доктор юридичних наук, професор

ПРО ІНФОРМАЦІЙНУ ФУНКЦІЮ УКРАЇНСЬКОЇ ДЕРЖАВИ

Серед великої кількості зовнішніх та внутрішніх функцій української держави інформаційна функція займає особливе місце. Однією з особливостей інформаційної функції держави є ефективна організація розвитку інформаційного суспільства, що сприяє впровадженню е-урядування.

Правова природа інформаційної функції в українській державі є достатньо обґрунтованою та врегульованою рядом нормативно-правових актів. В першу чергу, це закони України та інші нормативно-правові акти:

1) Закон України «Про засади внутрішньої і зовнішньої політики»;

2) Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»;

3) Закон України «Про інформацію»;

4) «Стратегія розвитку інформаційного суспільства в Україні», схвалена розпорядженням Кабінету Міністрів України від 15 травня 2013 року № 386-р;

5) «Концепція розвитку електронного урядування в Україні», схвалена розпорядженням Кабінету Міністрів України від 13 грудня 2010 року № 2250-р;

6) «Концепція створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів», схваленої розпорядженням Кабінету Міністрів України від 5 вересня 2012 року № 634-р.

Наявність цих та інших нормативно-правових актів, на думку Д. О. Петрова, свідчить про те, що «інформаційно-правові відносини виступають специфічним видом суспільних відносин, які виникають на підставі норм інформаційного права, учасники

якого є носіями суб'єктивних прав та юридичних обов'язків [1, с. 7].

Інформаційно-правові відносини є складовим елементом інформаційної функції держави. Вони впливають на:

1) сутність та зміст інформаційної функції держави;

2) ознаки, що характеризують інформаційну функцію держави взаємопов'язані та взаємообумовлені з ознаками інформаційно-правових відносин (наявність регулятивних, охоронних та спеціалізованих норм права, наявність суб'єктів, які реалізують інформаційну функцію держави);

3) середовище формування інформаційної функції держави;

4) методи та засоби реалізації інформаційної функції держави.

Так, серед основних принципів запобігання і протидії корупції зі сторони державних органів було комплексне здійснення інформаційних заходів (ст. 3 Закону України від 7 квітня 2011 року «Про засади запобігання і протидії корупції») [2], які у більшості випадків залишилися невиконані в силу об'єктивних і суб'єктивних причин.

Важливим зі сторони органів державної влади є оприлюднення інформації про вакантну посаду державної служби (ст. 23 Закону України «Про державну службу» [3].

Наведені приклади лише частково відображають сутність інформаційної функції держави, яка об'єднує на сьогодні десять видів інформації (ст. 10 Закону України «Про інформацію») [4]. Можна зазначити, що на сьогодні в українській державі і суспільстві існує інформаційне мегасередовище, що свідчить як про позитивні, так і негативні сторони цього глобального явища.

Негативний вплив нових інформаційних технологій зачіпає політичну, соціально-економічну та інші сфери людської діяльності і свідчить про криміналізацію окремих її сторін.

Послугами Інтернету користуються особи, які готують терористичні акти. В Інтернеті є сайти, що пропонують насильство над фізичною особою, наркотики, психотропні речовини (наприклад, російськомовний сайт з інформацією про маріхуану та гриби псилоцибахи) і багато іншого матеріалу [5, с. 203]. Україна залишається відкритою в інформаційному

просторі для комп'ютерної розвідки. Сучасні системи комп'ютерних технологій дозволяють шляхом аналізу отриманих даних не тільки якісну їх обробку, а й здійснювати прогнозування тих чи інших подій, що можуть негативно впливати на українське суспільство та державу в цілому.

Слушною з цього приводу є теза про те, що рівень безпеки українського суспільства залежить від рівня його відкритості. Вразливість деліктогенних громадян стає більш відкритою з урахуванням того, що в соціальній інформаційній мережі залишається їх «деліктний слід», який повинен цікавити правоохоронні органи.

Важливим інструментом захисту прав, свобод і законних інтересів громадян є застосування інтегрованих інформаційно-аналітичних систем. Вказані системи дозволяють з самого початку «відсіяти» інформацію, яка є випадковою, необґрунтованою чи просто фальшивою і дискредитує особу.

Революційні зміни в частині впровадження та застосування нових технічних засобів інформації вимагають від органів державної влади вживати заходи, спрямовані на реалізацію та забезпечення інформаційної функції держави. Як недолік, слід зазначити, що Україна відстає навіть у розвитку бездротового зв'язку [6, с. 5].

Узагальнюючи, слід зазначити, що інформаційна функція держави вимагає постійної уваги від органів державної влади, яка повинна бути спрямована на її розвиток, матеріально-технічне забезпечення, підготовку відповідної інфраструктури та спеціалістів.

Список літератури

1. Петров Д.О. Інформаційні правовідносини в Україні : автореф. дис. канд. юрид. наук. – Київ: Міністерство освіти і науки України, Національний авіаційний університет, 2014. – 18 с.

2. Закон України: Про засади запобігання і протидії корупції: чинне законодавство з 1 липня 2011 р.: (офіц. текст). – К.: Паливода А.В. – 2011. – 44 с. – (Закони України).

3. Закон України «Про державну службу»: чинне законодавство з 01.05.2016 р.: офіц. текст. – К.: Паливода А.В., 2016. – 88 с. – (Закони України).

4. Закон України «Про інформацію»: чинне законодавство зі змінами та допов. станом на 12 верес. 2011 р.: (офіц. текст). – К.: Паливода А.В., 2011. – 32 с. – (Закони України).

5. Дремін В.І. Інформаційне середовище в механізмі криміналізації суспільства // Актуальні проблеми держави і права: Збірник наукових праць. Вип. 27 А-437 / Редкол. С.В. Ківалов (голов. ред.) та ін. Відп. за вип. Ю.М. Оборотов. – Одеса: Юридична література, 2006. – 452 с.

6. Лапін С. На шляху до 5 G: чи буде чергова революція у сотовому зв'язку // Еженедельник 2000. – 2016. – 28 жовтня.

Пестова К.В. –
фахівець сфери захисту інформації Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України
Кравчук В.В. –
начальник Сектору захисту інформації Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України

ІТ-ЗАКОНОДАВСТВО: ПРОБЛЕМИ, ПРІОРИТЕТИ ТА НАПРЯМИ РОЗВИТКУ

Розвиток інформаційного суспільства призвів до появи інформаційних технологій, які стали невід'ємною частиною нашого життя. Вони дають не тільки можливість для розвитку здібностей, покращення знань та розширення кола інтересів, але й містять у собі реальні загрози. Одна з найсерйозніших загроз – виникнення нового виду злочинності – комп'ютерна злочинність. Для України комп'ютерна злочинність є відносно новим видом злочинності. На сьогоднішній день в країні є низка нормативно-правових документів та законів, що описують проблеми забезпечення кібербезпеки держави. Проте ця база у сфері кіберзлочинності лише частково охоплює елементи, які потрібні для протидії кіберзагрозам.

Метою даної статті є розгляд законодавства України у сфері ІТ-права, а також формування проблем, пріоритетів та напрямів розвитку нормативно-правової бази в сфері кібербезпеки.

Правову основу кібернетичної безпеки України становлять Конституція України, закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», та інші закони, Конвенція Ради Європи про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України, а також видані на виконання законів інші нормативно-правові акти [1, с 312].

Необхідність створення ефективної системи кібернетичної безпеки України відбулася після подій 2014 року. Інформаційна війна, яка відбувається між Росією і Україною, включає не тільки воєнні дії та інформаційно-психологічні операції, а також проведення кібернетичних атак. Виклик та загрози національній безпеці України в кібернетичному просторі призвели до створення Стратегії кібербезпеки України, що була введена в дію указом Президента України від 15 березня 2016. Стратегія є важливим кроком на шляху розбудови системи кібербезпеки України та являє собою програму дій, за якою мають слідувати державні органи. До стратегії було створено Розпорядження Кабінету Міністрів України від 24.06.2016 № 440-р «Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України», в якій описано заходи, які покладені на органи виконавчої влади та деяких військових формувань.

Стратегія базується на положеннях Конвенції про кіберзлочинність, яка ратифікована Законом України від 7 вересня 2005 року № 2824-IV.

Метою даної стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства, держави [2, с 1].

Вона складається з загальних положень, основних загроз кібербезпеці, основних суб'єктів забезпечення кібербезпеки, пріоритетів та напрямів забезпечення кібербезпеки України та прикінцевих положень.

У законі України «Про основи національної безпеки України» та в «Доктрині інформаційної безпеки України» згадуються поняття про «комп'ютерна злочинність» та «комп'ютерний тероризм», проте визначення цих термінів в законі немає. В законі «Про боротьбу з тероризмом» поняття «комп'ютерний тероризм» не висвітлюється зовсім, а те що до нього відноситься називається «технологічним тероризмом». Для покращення нормативно-правової бази у сфері кіберзлочинності Верховною Радою України було розглянуто законопроекти: «Про основні засади забезпечення кібербезпеки України» (реєстр. № 2126а від 19.05.2015) та «Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кібезлочинністю» (реєстр. № 2133а від 19.06.2015). В законопроекті № 2126а визначили терміни «кіберзлочинність» та «кібертероризм».

На даний час законопроекти відпрацьовуються фахівцями зацікавлених органів (СБУ, МВС, НБУ, МО, ДССЗЗІ та інші), якими у тому числі пропонуються термін «кіберзлочин» узгодити із положенням України про кримінальну відповідальність. Законопроект № 2133а розроблено у зв'язку з необхідністю підвищення ефективності заходів спрямованих на протидію кіберзлочинності. У ньому пропонується внести зміни до низки законодавчих актів, а також запропоновано внести терміни «кіберпростір» та «кібербезпека» до закону України «Про основи національної безпеки».

Також необхідно зазначити, що питання змін в законодавстві у вказаній сфері на даний час розглядається у більшості технологічно розвинених країнах. Так 6 липня 2016 року Європейський парламент ухвалив нову «Директиву з питань безпеки мереж та інформації» («Network and Information Security Directive»), яка встановлює єдині правила та вимоги для всіх країн ЄС у галузі кібербезпеки. На цей час Україна також частково виконала вимоги, та надалі продовжує роботу у цьому напрямку.

Основою кіберзлочинів, згідно чинного законодавства України є передбачені Кримінальним кодексом України суспільно небезпечні діяння і закріпленні в окремому Розділі

XVI «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України. З точки зору кримінального права до кіберзлочинів відносяться тільки злочини, передбачені розділом XVI КК України, а в рамках криміналістики доцільно включити до даного поняття інші злочини, для скоєння яких застосовується комп'ютер та використовується Інтернет. Проте у розділі зовсім відсутні поняття пов'язані з кібербезпекою, натоміть є лише деякі поняття злочинів, які вчиняються за допомогою електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Розділ складається з трьох статей:

ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»;

ст. 361-1 «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»;

ст. 361-2 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерів), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації»;

ст. 362 «Викрадання, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем»;

ст. 363 «Порушення правил експлуатації автоматизованих електронно-обчислювальних систем»;

ст. 363-1 «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку» [3].

З розпорядження Кабінету Міністрів України «Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України» та законопроектом «Про основні засади забезпечення кібербезпеки України» одним з військових формувань, яке займається питаннями кібербезпеки є Державна

служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язок). На Держспецзв'язок покладені такі задачі:

– бере участь у формуванні та реалізації державної політики у сфері кібербезпеки;

– розробляє критерії та порядок оцінки стану кіберзахисту об'єктів критичної інформаційної інфраструктури, забезпечує її організацію та проведення;

– здійснює державний контроль за станом захисту інформації, яка циркулює на об'єктах критичної інформаційної інфраструктури;

– створює у межах затвердженої чисельності та забезпечує функціонування підрозділу з питань оперативного реагування на кіберінциденти;

– забезпечує функціонування системи захищеного доступу державних органів до Інтернету;

– координує діяльність державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форми власності з питань запобігання, виявлення та усунення наслідків кіберінцидентів;

– вживає організаційно-технічних заходів із збору та обліку інформації про кіберінциденти і кіберзагрози, узагальнює і надає таку інформацію суб'єктам забезпечення кібербезпеки постійної готовності відповідно до їх повноважень;

– за результатами аналізу кіберінцидентів координує діяльність операторів, провайдерів телекомунікацій з питань забезпечення збереження ними необхідних даних про відповідні кіберінциденти в інтересах суб'єктів забезпечення кібербезпеки постійної готовності;

– здійснює міжнародне співробітництво і взаємодіє з компетентними органами інших держав у рамках надання міжнародної технічної допомоги з питань кіберзахисту [4].

В Державному центрі кіберзахисту та протидії кіберзагрозам Держспецзв'язку є структурований підрозділ Computer response team of Ukraine (далі – Cert-UA) – команда реагування на комп'ютерні надзвичайні події України. Основна

мета Cert-UA – забезпечити захист інформаційних ресурсів та інформаційних та телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності. Також сфера діяльності включає заходи, що спрямовані на ліквідацію інцидентів інформаційної безпеки, які виникають в кіберпросторі українського сегменту мережі Інтернет. В 2016-2017 рр. планується створення штатного підрозділу, який буде займатися деякими заходами, які покладені з розпорядження Кабінету Міністрів України «Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України» на Держспецзв'язок .

Розглядаючи нормативно-правову базу у сфері регулювання кібербезпеки України, можна виділити деякі проблеми:

– відсутність єдиного понятійного апарату та норм, щодо кваліфікації комп'ютерних злочинів;

– відсутність у державі розвинутих інститутів програмно-технічної та судово-кібернетичної експертизи як одного з головних механізмів у процесі документування та закріплення доказів «комп'ютерного» злочину та відповідних методик їх проведення;

– відсутність необхідного рівня координації та взаємодії між відповідними підрозділами правоохоронних структур при проведенні адекватних загрозам в зазначеній сфері запобіжних та правозастосовних заходів;

– малорозвинена загальнодержавна система протидії кіберзлочинності; (хоча на даний час активізувалась робота по даному напрямку – Указом Президента України № 242/2016 від 7 червня 2016 року було затверджено «Положення про Національний координаційний центр кібербезпеки», який за своїми функціями відповідає загальнодержавній системі протидії кіберзлочинності. Одним з представником Центру є Голова Держспецзв'язку).

Пріоритетами у вдосконаленні нормативно-правової бази сфери кібербезпеки є:

– розвиток та удосконалення системи державного контролю за станом захисту інформації, а також системи незалежного аудиту інформаційної безпеки, запровадженні кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

– розроблення нових методів запобігання кібератакам, кіберінцидентам та поширенню інформації про них;

– здійснення захисту технологічних процесів на об'єктах критичної інфраструктури, в яких управління або моніторинг здійснюється за допомогою інформаційно-комунікаційних технологій, від несанкціонованого втручання у їх роботу;

– вдосконалення загальнодержавної системи протидії кіберзлочинності.

Виходячи в цього побудова національної системи кібербезпеки повинна складатися з двох напрямків: захист інформаційного простору України в комп'ютерних мережах та протидія кіберзлочинності.

Отже, кіберпростір на сьогоднішній день відіграє велику роль у забезпеченні інформаційної безпеки людини, суспільства, держави. За останній час Україна зробила прогресивні кроки у створенні ефективної національної системи кібербезпеки. Чітке окреслення термінів дало змогу вдосконалити нормативно-правове регулювання діяльності правоохоронних органів, органів виконавчої влади та військових формувань. Але цього виявляється не достатньо для повного подолання кіберзлочинності в нашій країні. В країні потрібно підвищити обізнаність населення щодо кіберзагроз, збільшити кількість кваліфікованих спеціалістів у цій сфері. Правове реагування на проблеми посилення комп'ютерної злочинності є надзвичайно важливим. І тому, представляється досить важливим розширити правову і законодавчу базу у сфері боротьби з комп'ютерними злочинами, а саме прискорити прийняття вказаних законопроектів з обов'язковим врахуванням пропозицій державних органів, що в подальшому будуть застосовувати таку нормативно базу та постійно удосконалювати національне законодавство з метою успішної співпраці з іншими країнами та міжнародними організаціями.

Список літератури

1. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення/ Шеломенцев В.П. – К. : наук.-практ. журнал «Боротьба з організованою злочинністю і корупцією (теорія і практика)», 2012. –324 с.

2. Указ Президента України. «Про Стратегію кібербезпеки України». – Відомості Верховної Ради – 2016. – №96/2016.

3. Кримінальний кодекс України. Розділі XVI «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» – Відомості Верховної Ради (ВВР) – 2001. – №25-26, ст. 131.

4. Законопроект. Про основні засади забезпечення кібербезпеки України. – Відомості Верховної Ради України (ВВР) – 2015. – 2126а.

Радейко Р.І. –
асистент кафедри адміністративного та інформаційного права Навчально-наукового інституту права та психології Національного університету «Львівська політехніка», кандидат юридичних наук

СОЦІАЛЬНІ МЕРЕЖІ ЯК ОБ'ЄКТ ПРАВОВОГО РЕГУЛЮВАННЯ

Винахідник Всесвітньої мережі «Інтернет» Тімоті Бернерс-Лі у книзі «Заснування Павутини» зазначає: «Мережа – це більше соціальне, ніж технічне явище». Задумував я її для досягнення результату – допомогти людям працювати разом, – а не як технічну іграшку. Найзагальніша мета Мережі – підтримка і поліпшення нашого існування у світі, яке саме багато в чому є мережевим» [2, с. 107].

Протягом останніх десяти років особливої популярності набувають «соціальні мережі». Соціальна мережа – це інтернет-сервіс, призначений одночасно для комунікації користувачів і для розміщення і поширення ними інформації [1, с. 236].

За даними дослідження CMeter, компанії TNS, за квітень 2016 р. найбільш популярними серед українських інтернет-користувачів залишаються соціальні мережі «Вконтакте» (vk.com), «Facebook» (facebook.com) [5]. Однак, соціальні мережі розвиваються настільки стрімко, що суспільство та

держава не встигають визначитися з відповідними моральними, правовими та соціальними аспектами їх регулювання.

Відповідно до дослідження, проведеного компанією IpsosMori (опитування ґрунтується на відповідях 1000 британців у віці від 16 до 64 року) на замовлення провідного видання Великобританії «TheGuardian» у 2008 р., дев'ять з десяти осіб, вважають, що необхідне жорстке регулювання обігу інформації на веб-сайтах соціальних мереж. Дослідження показало, що більшість британців, вважають, що такі соціальні мережі як Facebook і MySpace повинні підпадати під дію загальних правил, які б допомагали користувачам цих мереж скаржитися на нав'язливі матеріали, що розміщені на сайті.

У даний час кожна зі соціальних мереж керується виключно власними сформованими правилами. Проте, 89 % опитаних осіб вважають, що повинні існувати загальноприйняті норми для ефективного захисту інформації у цих базах даних [6].

Відсутність правого регулювання соціальних мереж в Україні зумовило те, що вони відігравали одну з ключових ролей у розпалюванні ненависті та ескалації насильства. На самому початку російської операції було створено численні групи в соціальних мережах (передусім у «ВКонтакте»), присвячені ідеям Антимайдану в різних форматах. Спочатку значна кількість дописувачів мала «прописку» в російських містах, у лютому – березні 2014 року серед дописувачів з'явилося багато користувачів із Криму, що свідчить про активне залучення місцевого населення до інформаційної війни на боці Росії. Проте з березня кількість членів груп і дописувачів збільшилася за рахунок населення безпосередньо східних та південних областей, що стало наслідком ескалації напруженості та залучення до конфлікту більшої кількості людей.

У соціальних мережах поширюються великі обсяги недостовірної інформації: неперевірені «фотофакти», «відео очевидців», «коментарі учасників» тощо. Російські ЗМІ та проросійські громади в соціальних мережах маніпулюють інформацією, фотографіями і відео. Найчастіше вони беруть

одіозні, криваві або емоційні знімки з інших країн і подій, видаючи їх за українські [3, с. 27-28].

Крім названої проблеми, існує чимало інших, які не мають конкретного правового вирішення. Серед таких проблем варто виділити:

– відсутність уніфікованих принципів правового регулювання відносин у соціальних мережах;

– відсутність захисту та відповідальності за порушення прав інтелектуальної власності у соціальних мережах;

– проблеми правового регулювання реклами, електронної комерції і використання товарних знаків у соціальних мережах;

– забезпечення інформаційної безпеки і захисту персональних даних користувачів соціальних мереж. Для прикладу, реєструючись у соціальній мережі «Вконтакте», адміністрація цього сайту, відповідно до «Правил захисту інформації про користувачів сайту vk.com», «діючи розумно і сумлінно», вважає, що користувач: «усвідомлює, що інформація на даному сайті, що розміщається користувачем про себе, може ставати доступною для інших користувачів сайту і користувачів інтернету, може бути скопійована і поширена такими користувачами; усвідомлює, що деякі види інформації, передані ним іншим користувачам, не можуть бути видалені самим користувачем» [4].

Вбачаю, що у даний час існує чимало прогалин і суперечностей, пов'язаних з правовим регулюванням відносин у соціальних мережах. Звичайно, певні норми містяться у різних галузях права (в цивільному та кримінальному законодавстві існує територіальний принцип, який поширює дію законів на всю територію України і принцип громадянства, який встановлює, зокрема, кримінальну відповідальність громадян України, які вчинили злочинне діяння за межами України). Проте, цих норм і принципів явно недостатньо для регулювання інформаційних процесів в соціальних мережах. Глобальний характер соціальних мереж зумовлює необхідність вироблення єдиних уніфікованих інформаційних норм для врегулювання правових відносин у соціальних мережах.

Список літератури

1.Архипов В.В. Интернет-право: учебник и практикум для бакалаврата и магистратуры / В.В. Архипов. – М.: Издательство «Юрайт», 2016. – 249 с.

2.Бернерс-Лі Т. Заснування Павутини: З чого починалася і до чого прийде Всесвітня мережа / Т.бернерс-Лі, М. Фічетті; Пер. з англ. А.Іщенка. – К.: Вид. дім «Києво-Могилянська академія», 2007. – 207 с.

3.Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. / за заг. ред. А. Баровської – К. : НІСД, 2016. – 109 с.

4.Правила захисту інформації про користувачів сайту VK.com [Електронний ресурс]. – Режим доступу: http://vk.com/privacy

5.Рейтинг популярних сайтів за квітень 2016: Facebook.com випередив Wikipedia.org [Електронний ресурс]. – Режим доступу: https://tns-ua.com/news/reyting-populyarnih-saytiv-za-kviten-2016-facebook-com-viperediv-wikipedia-org

6.Bobbie Johnson. Facebook information should be regulated, survey says // The Guardian. –5 June 2008. https://www.theguardian.com/technology/2008/jun/05/privacy.socialnetworking?gusrc=rss&feed=technologyfull

Селезньова О. М.
завідувач кафедри професійних та спеціальних правових дисциплін ПВНЗ «Буковинський університет», доктор юридичних наук, доцент

ТЕОРЕТИКО-МЕТОДОЛОГІЧНЕ ТРАКТУВАННЯ ОКРЕМИХ ЗАСАДНИЧИХ КАТЕГОРІЙ ІНФОРМАЦІЙНОГО ПРАВА

На сьогоднішній день наука інформаційного права перебуває на тому етапі свого розвитку, коли відбувається активне формування своєрідного понятєво-категоріального апарату. Такий процес може характеризуватись фрагментарністю, неточністю, вузькістю розуміння, розрізненістю та суперечливістю, однак це не можна називати його недоліками, а лише – похідними наукового і творчого пошуку необхідних соціуму розумінь термінів, які з'являються та мають місце у сучасному суспільстві, що усе більше набуває рис інформаційного. Актуальність подальшого вияснення сутності різноманітних понять, що використовуються в

інформаційному праві, не викликає сумнівів, адже їх адекватне розуміння сприяє гармонізації інформаційних відносин, нормалізує інформаційну діяльність та забезпечує її належну правову регламентацію, створює базиси для формування якісного інформаційного законодавства, урегульовує постійно виникаючі технічні та технологічні ситуації у нормативному полі тощо. Разом з тим, особливої наукової уваги у теоретико-методологічній розробці потребують засадничі категорії інформаційного права, оскільки саме вони є основою для побудови усього поняттєво-категоріального апарату науки інформаційного права, а проте тут і спостерігаємо найбільшу плутанину у трактуваннях. Становище ускладнюється ще й тим, що багато існуючих понять не закріплені законодавчо або вживаються без пояснення їхнього змісту.

Відмітимо, що з різних ракурсів окреслену тематику дослідження розглядали у своїх працях такі українські вчені, як: Арістова І. В., Баранов О. А., Бєляков К. І., Брижко В. М., Бурило Ю. П., Калюжний Р. А., Копан О. В., Коваленко Л. П., Кормич Б. А., Кохановська О. В., Марущак А. І., Новицький А. М., Олійник О. В., Панова І. В., Пилипчук В. Г., Цимбалюк В. С., Яременко О. І. та інші. Беручи до уваги наукові досягнення у спробі розв'язання проблеми неузгодженості та суперечливості поняттєво-категоріального апарату науки інформаційного права, варто все-таки констатувати той факт, що багато аспектів цієї проблеми залишаються відкритими та потребують свого вирішення.

Метою даної статті є спроба узагальнити існуючі наукові погляди на такі засадничі категорії науки інформаційного права, як «інформаційна сфера», «інформаційний простір» та «інформаційне середовище», визначити їх сутність та нетотожність, взаємозв'язок і взаємовідношення, та сформулювати їхні поняття.

Починаючи наше дослідження, необхідно насамперед оговорити той момент, що досить часто у літературі категорії «інформаційна сфера», «інформаційний простір» та «інформаційне середовище» ототожнюються і/або трактування одного терміну здійснюється через вживання іншого (наприклад, О. В. Логінов розглядає інформаційну сферу

України як «єдиний інформаційний простір, який формується державними органами, громадськими, політичними та соціальними організаціями, а також громадянами й функціонує з урахуванням правових, організаційних, науково-технічних, економічних, фінансових, методичних, гуманітарних та моральних засад з урахуванням вимог та завдань національної інформаційної безпеки України» [1, с.9], ототожнюючи при цьому категорії «інформаційна сфера» і «інформаційний простір», та звужуючи обсяг поняття «сфера» до обсягу поняття «простір», застосувавши територіальне обмеження). Такі позиції, на нашу думку, є в своїй основі невірними, оскільки кожна із вищевказаних категорій має своє тлумачення. Більше того, навіть в інформаційному законодавстві визнається їх нетотожність. Зокрема, п.8 ч.1 ст.3 Закону України «Про інформацію» вказує, що одним з основних напрямів державної політики є сприяння міжнародній співпраці в інформаційній сфері та входження України до світового інформаційного простору [2].

Категорія «інформаційна сфера» є найбільш широким поняттям, оскільки володіє рядом характерних ознак, а саме:

1) є частиною ноосфери.

Термін «інформаційна сфера» складається з двох слів, причому одне з них вказує на галузеву особливість, а інше – на приналежність до соціального буття. Вживання слова «сфера» у даному випадку обумовлює знаходження вказаного терміну на одному щаблі з такими загальновідомими філософськими категоріями, як «біосфера» та «ноосфера».

Якщо звернутися до відповідної літератури, то стає зрозумілим, що у сучасній науці розрізняють два поняття ноосфери: як сфери виникнення й існування розуму, що виникає з біосфери, та як сфери взаємодії суспільства і природи, у якій домінуюча роль належить розуму, діяльності людини [3, с.233]. Такі позиції дають підстави вважати ноосферу (у будь-якому випадку, сферу розуму) подальшим витком розвитку планетарної історії. Поряд з тим, така сфера за своєю внутрішньою природою є комплексним різностороннім явищем і далеко не останню роль у ньому відіграє такий його елемент, як інформаційна сфера. Остання представляє собою

багатовекторне активне утворення, яке включає до свого складу усі види інформаційної діяльності фізичних і юридичних осіб, державних органів та інших суб'єктів цієї діяльності, а також самих суб'єктів інформаційної діяльності; сукупність інформації у будь-якій матеріальній і нематеріальній формі, інформаційних ресурсів, інформаційних технологій та інших інформаційних розробок; існуючу інформаційну інфраструктуру, з наявними у ній інформаційними послугами, інформаційною продукцією, інформаційними макро- і мікрокліматом.

Як бачимо, інформаційна сфера найтіснішим чином пов'язана з іншими сферами суспільної діяльності, але водночас вона характеризується галузевою приналежністю, що визначає її автономність серед інших сфер. Звідси випливають ще дві ознаки інформаційної сфери:

2) комплексність внутрішньої природи інформаційної сфери, яка зумовлюється інформаційною приналежністю;

3) дуалістичність функціональних характеристик, що проявляється у своєрідній автономії та нерозривному зв'язку з іншими сферами суспільної діяльності.

Розвиваючи думку про характерні ознаки інформаційної сфери варто відмітити той факт, що набуває популярності позиція, згідно якої «всі складові інформаційної сфери, незалежно від наявності чи відсутності її узагальнюючої дефініції, потребують державного управління, в якому повинні брати участь всі ланки виконавчої влади» [4, с. 15]. Звичайно, для юридичної науки та практики неабияке значення відіграє можливість управлінського впливу не тільки на інформаційну, але й на будь-яку іншу сферу суспільної діяльності. Роль держави та права, правових інституцій зростає із збільшенням об'єктів, на які можна спрямувати пряму чи опосередковану дію. А проте В. П. Семиноженко слушно зауважує, що «інформаційна сфера сьогодні стала, мабуть, самою ліберальною сферою суспільних відносин, тому роль держави в цих процесах повинна бути не контролюючою, а стимулюючою» [5], і до цієї думки варто прислухатись та знайти (розробити) відповідні механізми й важелі оптимального керування (винятками, звісно, є ті сегменти інформаційної сфери, що володіють певними суспільно-значимими рисами та

потребують посиленої уваги з боку держави – інформаційна безпека, інформаційна політика та інше).

Розглядаючи даний аспект, варто підтримати і думку О. А. Баранова, який пише, що «інформаційне сфера як важлива та розгалужена сфера соціуму потребує відповідного соціального регулювання» [6, с.23].

Багатопрофільність сегментів інформаційної сфери зумовлює існування цілої сукупності різних явищ, об'єднаних інформаційною приналежністю. Це дозволяє виділити таку ознаку інформаційної сфери, як:

4) множинність внутрішньої природи інформаційної сфери, яка включає до свого складу інформацію та інформаційні відносини (первинні/базисні конструкції інформаційної сфери), інформаційну діяльність та інформаційну інфраструктуру, інформаційну культуру, суб'єктів інформаційної діяльності. Надбудовчим рівнем перелічених елементів є державне управління інформаційною сферою, інформаційне право та інформаційне законодавство.

Терміни «інформаційний простір» та «інформаційне середовище» є значно вужчими за своїм розумінням порівняно з терміном «інформаційна сфера», оскільки обидва обмежуються територією поширення.

Так, інформаційний простір можна визначити як частину інформаційної сфери, що обмежується територією держави, союзу держав або віртуальним суспільством. Тобто інформаційний простір може бути територіальним (інформаційний простір держави, європейський інформаційний простір, світовий інформаційний простір) або віртуальним інформаційним простором.

Інформаційний простір не можна вважати самою «територією поширення інформації за допомогою конкретних компонентів системи інформації і зв'язку» [7, с.9], оскільки тоді воно переходить у розряд явищ геополітичної природи і віддаляється від сфери розуму (ноосфери), частиною якої його можна цілком сміливо вважати, адже територія – це лише фактор обмеження визначеної частини інформаційої сфери.

Вважаємо також помилковою думку про те, що «у центрі інформаційного простору стоїть суб'єкт, який у процесі своєї

діяльності створює, накопичує, передає, зберігає інформацію. Таким суб'єктом може бути як людина чи соціальна група, так і компанія чи навіть державний орган» [8, с.189]. Ядром інформаційного права є саме сукупність суб'єктів, що здійснюють інформаційну діяльність. Окрема людина або державний орган є центром інформаційного середовища – обмеженого певними рамками (територією, часом тощо) оточення, спрямованого на виробництво, копіювання, поширення чи знищення інформації.

Іншими словами, інформаційне середовище характеризується своєрідним мікрокліматом, певними інформаційними умовами, що створюють можливість здійснення інформаційної діяльності суб'єктами інформаційних відносин. Це може бути інформаційне середовище колективу, установи, науково-дослідного інституту, державного органу тощо. Воно проявляється і на елементарному рівні – в процесі взаємодії людини і комп'ютера, автора і його твору тощо.

Проведене дослідження дозволяє зробити наступні висновки, в яких запропонувати трактування таких термінів:

1) інформаційна сфера – це частина ноосфери, яка характеризується інформаційною приналежністю та множинністю внутрішньої природи, що обумовлює її автономію серед інших сфер суспільства, але забезпечує їх постійний взаємозв'язок при реалізації своєї функціональної сутності;

2) інформаційний простір – це частина інформаційної сфери, обмеженої матеріальною та нематеріальною територією поширення, центром якої є сукупність суб'єктів, що здійснюють інформаційну діяльність, а її складовими – інформація та інформаційні відносини, інформаційна наука та інформаційна культура, інформаційна діяльність та інформаційна інфраструктура, інформаційне право та інформаційне законодавство.

Беручи до уваги значення для України, інформаційний простір може поділятися за критерієм території поширення: а) інформаційний простір держави (України) – на нього поширюється юрисдикція однієї держави; б) європейський інформаційний простір – підлягає юрисдикції союзу держав; в) світовий інформаційний простір – міжнародний термін для

організованої співпраці всіх країн світу, спрямованої на позитивний розвиток інформаційного суспільства;
г) віртуальний інформаційний простір – проявляється в межах віртуального (комп'ютерного) суспільства;

3) інформаційне середовище – це частина інформаційного простору, що характеризується мінімальною територією поширення та обмеженою кількістю суб'єктів інформаційної діяльності, а також обумовлюється своєрідним інформаційним мікрокліматом, що включає сукупність способів, прийомів, заходів та умов безпосереднього здійснення інформаційної діяльності.

Список літератури

1.Логінов О. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : автореф. дис. на здобуття наук. ступеня кандидата юрид. наук : спец. 12.00.07 «Теорія управління; адміністративне право і процес; фінансове право; інформаційне право» / Олександр Володимирович Логінов. – К., 2005. – 23 с.

2.Про інформацію : Закон України в редакції від 13 січня 2011 р. № 2938-VI з наступними змінами та доповненнями : [електорнний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2657-12

3.Філософія : навч. посібник / за ред. І. Ф. Надольного. – К. : Вікар, 2005. – 455 с.

4.Яременко О. І. Правовий статус Кабінета Міністрів України як суб'єкта державного управління інформаційною сферою / О. І. Яременко // Інформація і право. – 2015. – № 2 (14). – С. 13-19.

5.Семиноженко В. П. «Інформаційна хвиля» суспільного розвитку: глобальні виклики і національні перспективи : [Електорнний ресурс] / В. П. Семиноженко. – Режим доступу : http://www.semynozhenko.net/documents/14/

6.Баранов О. А. Теоретико-методологічні основи правового забезпечення інформаційної сфери України : автореф. дис. на здобуття наук. ступеня доктора юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Олександр Андрійович Баранов. – Харків, 2015. – 40 с.

7.Буньківська О. В. Інформаційний простір: соціокультурна сутність, стан та проблеми функціонування в Україні : автореф. дис. на здобуття наук. ступеня кандидата культурології : спец. 26.00.01 «Теорія та історія культури» / Оксана В'ячеславівна Буньківська. – К., 2009. – 22 с.

8.Біловус Л. І. Український інформаційний простір: сьогодення та перспективи / Леся Іванівна Біловус / Український інформаційний простір : науковий журнал Інституту журналістики і міжнародних відносин КНУКІМ / гол. ред. М. С. Тимошик. – Число 1. – У 2-х ч. – Ч. 1. – К., 2013. – С. 188-191.

Сірант О.Р. –
аспірант кафедри адміністративного права
Інституту права ім. князя Володимира Великого МАУП

ВІДКРИТІСТЬ ІНФОРМАЦІЇ ОДНА З УМОВ РОЗВИТКУ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА В УКРАЇНІ

Угода про асоціацію України і Європейського Союзу передбачає гарантування реалізації вільного потоку інформації та ідей. Це є визнанням принципу, що державні органи володіють інформацією в інтересах суспільства та від його імені. У зв'язку з цим при обмеженні доступу до інформації суспільні інтереси повинні бути головним критерієм для органів державної влади та місцевого самоврядування, їх посадових осіб, що володіють цією інформацією на законних підставах.

Поряд з цим поняттям існує поняття інформаційної відкритості органів державної влади, яке отримало назву транспарентність. Під нею розуміється така організація діяльності органів державної влади, при якій громадянам, їх об'єднанням, комерційним структурам, іншим державним і місцевим органам забезпечується змога отримувати необхідну та достатню інформацію про діяльність, прийняті рішення та іншу суспільно значиму інформацію при дотриманні обмежень, встановлених законами.

Принцип інформаційної відкритості закріплений у Законах України «Про Кабінет Міністрів України», «Про центральні органи виконавчої влади», «Про місцеве самоврядування в Україні», «Про доступ до публічної інформації» і інших нормативних актах [1-4].

Цей принцип виражається в доступності для громадян інформації, що становить суспільний інтерес або зачіпає особисті інтереси громадян; систематичному інформуванні громадян про передбачувані або прийняті рішеннях; здійсненні громадянами контролю за діяльністю державних органів, організацій і підприємств, громадських об'єднань, посадових осіб та прийнятими ними рішеннями, пов'язаними з дотриманням, охороною і захистом прав і законних інтересів громадян.

Специфіка діяльності органів влади полягає у постійному зверненні за інформацією, що одержується із зовнішніх джерел, і безпосередньо в її створенні.

Сучасне суспільство зацікавлене в розвитку прозорості та відкритості державного управління. Широкий доступ до інформації про державні і місцеві органи розширює змогу оцінювати їх діяльність.

Доступність інформації про діяльність органів влади спрямована на забезпечення особистих інтересів індивідуума, пов'язаних зі змогою реалізувати свої права та свободи, на його участь у справах суспільства та держави. Доступ фізичних і юридичних осіб до інформації про діяльність органів влади є основою здійснення громадського контролю над діяльністю державних органів, органів місцевого самоврядування, громадських, політичних та інших організацій.

Особливого значення доступність інформації для громадян має у сферах економіки, екології.

У переважній більшості випадків об'єктом правовідносин у контексті відкритості влади виступає інформація про діяльність того чи іншого суб'єкта публічної влади. Практично жодний суспільний інтерес не обходиться без інформаційної взаємодії учасників.

Нормами міжнародного права встановлюється презумпція розкриття інформації державою як гарантія права на інформацію. Це означає обов'язок гарантувати право на інформацію, введення реальних і ефективних механізмів для його реалізації.

Право на інформацію є ключовим інструментом для боротьби з корупцією та неправомірними діями органів державної влади, органів діяльність яких регулюється корпоративними нормативними актами.

Такий підхід дає змогу розширити систему стримувань і противаг адміністративній владі за допомогою права на інформацію та громадський контроль, який це право активізує. Підвищення відкритості органів виконавчої влади дозволяє досягти відразу декількох цілей:

– зробити державу більш демократичною, інформаційно відкритою для громадян;

– підвищити ефективність діяльності державного апарату;

– встановити громадський контроль над владою.

Відкритий доступ до інформації дозволяє підвищити відповідальність державних службовців і службовців органів місцевого самоврядування, позитивно впливає на ефективність боротьби з корупцією, зі зловживанням службовим становищем.

Хоча відкритість не може бути абсолютною, вона повинна бути необхідною і достатньою. Для підтримки балансу принципово важливо дотримуватися деяких обмежень, тобто обмеження доступу до інформації, наприклад, для поваги прав і репутації інших осіб, а також для охорони державної безпеки, громадського порядку, здоров'я населення.

Специфіка інформації про діяльність державних органів і органів місцевого самоврядування полягає у тому, що ці органи є власниками значного обсягу суспільно важливої інформації, що викликає підвищений суспільний інтерес в силу свого впливу на всі сфери людської діяльності.

Право на доступ до інформації є ключовим елементом розвитку громадянського суспільства і є дієвим механізмом боротьби з негативними соціальними явищами.

Умови, при яких значна частина інформації про діяльність органів влади залишається недоступною для суспільства, створюють сприятливий ґрунт для неефективного державного управління.

Важливим елементом громадянського суспільства є забезпечення державою змоги для громадян ознайомиться з тією інформацією, яка була підставою для прийняття органами влади того чи іншого рішення. В умовах формування суспільства, в якому інформація стає головною цінністю, неминуче повинна відбуватися переоцінка і прав, і обов'язків органів влади та громадян в інформаційній сфері.

Список літератури

1. Про Кабінет Міністрів України: Закон України від 27.02.2014 р. № 794-VII // Відомості Верховної Ради України. – 2014. – № 13. – Ст. 222.

2. Про центральні органи виконавчої влади: Закон України від 17.03.2001 р. // Відомості Верховної Ради України. – 2011. – № 38. – Ст. 385.

3. Про місцеве самоврядування в Україні: Закон України від 21.05.1997 р. № 280/97-ВР // Відомості Верховної Ради України. – 1997. – № 24. – Ст. 170.

4. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 314.

Тацишин І.Б. –
доцент кафедри адміністративного та інформаційного права
Навчально-наукового інституту права та психології
Національного університету «Львівська політехніка»,
кандидат юридичних наук, доцент

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ПРАВА КОНТРОЛЮЮЧИХ ОРГАНІВ НА ПИСЬМОВИЙ ЗАПИТ ПРО ПОДАННЯ ІНФОРМАЦІЇ ЗГІДНО ПОДАТКОВОГО КОДЕКСУ УКРАЇНИ

Відповідно до ч. 2 ст. 19 Конституції України органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України.

Згідно п.п. 20.1.4 п. 20.1 ст. 20 Податкового кодексу України (далі по тексту – ПК України), контролюючі органи мають право проводити відповідно до законодавства перевірки і звірки платників податків (крім Національного банку України), у тому числі після проведення процедур митного контролю та/або митного оформлення.

Відповідно до п. 75.1 ст. 75 ПК України, контролюючі органи мають право проводити камеральні, документальні (планові або позапланові; виїзні або невиїзні) та фактичні перевірки.

Підпунктом 75.1.2 п. 75.1 ст. 75 ПК України передбачено, що документальною перевіркою вважається перевірка, предметом якої є своєчасність, достовірність, повнота нарахування та сплати усіх передбачених цим Кодексом податків та зборів, а також дотримання валютного та іншого законодавства, контроль за дотриманням якого покладено на контролюючі органи, дотримання роботодавцем законодавства щодо укладення трудового договору, оформлення трудових відносин з працівниками (найманими особами) та яка проводиться на підставі податкових декларацій (розрахунків), фінансової, статистичної та іншої звітності, регістрів податкового та бухгалтерського обліку, ведення яких

передбачено законом, первинних документів, які використовуються в бухгалтерському та податковому обліку і пов'язані з нарахуванням і сплатою податків та зборів, виконанням вимог іншого законодавства, контроль за дотриманням якого покладено на контролюючі органи, а також отриманих в установленому законодавством порядку контролюючим органом документів та податкової інформації, у тому числі за результатами перевірок інших платників податків.

Документальна позапланова перевірка не передбачається у плані роботи контролюючого органу і проводиться за наявності хоча б однієї з обставин, визначених Податковим Кодексом України.

Документальною виїзною перевіркою вважається перевірка, яка проводиться за місцезнаходженням платника податків чи місцем розташування об'єкта права власності, стосовно якого проводиться така перевірка.

Статтею 78 ПК України встановлено особливості проведення документальної позапланової перевірки.

Відповідно до п.п. 78.1.1 п. 78.1 ст. 78 ПК України, в редакції, що діяла на час спірних правовідносин, документальна позапланова перевірка здійснюється за наявності хоча б однієї з таких обставин: отримано податкову інформацію, що свідчить про порушення платником податків валютного та іншого не врегульованого цим Кодексом законодавства, контроль за дотриманням якого покладено на контролюючі органи, якщо платник податків не надасть пояснення та їх документальні підтвердження на обов'язковий письмовий запит контролюючого органу, в якому зазначаються порушення цим платником податків відповідно валютного та іншого не врегульованого цим Кодексом законодавства, контроль за дотриманням якого покладено на контролюючі органи, протягом 10 робочих днів з дня отримання запиту.

Пунктом 78.4 ст. 78 ПК України визначено, що про проведення документальної позапланової перевірки керівник органу державної податкової служби приймає рішення, яке оформлюється наказом.

Право на проведення документальної позапланової перевірки платника податків надається лише у випадку, коли

йому до початку проведення зазначеної перевірки вручено під розписку копію наказу про проведення документальної позапланової перевірки.

Відповідно до п. 73.3 ст. 73 ПК України контролюючі органи мають право звернутися до платників податків та інших суб'єктів інформаційних відносин із письмовим запитом про подання інформації (вичерпний перелік та підстави надання якої встановлено законом), необхідної для виконання покладених на контролюючі органи функцій, завдань, та її документального підтвердження.

Такий запит підписується керівником (заступником керівника) контролюючого органу і повинен містити: 1) підстави для надіслання запиту відповідно до цього пункту, із зазначенням інформації, яка це підтверджує; 2) перелік інформації, яка запитується, та перелік документів, які пропонується надати; 3) печатку контролюючого органу.

Запит про надання інформації може бути надісланий платнику у зв'язку з виявленням обставин, визначених абзацом 3 п.п. 73.3 ст. 73 ПК України, відповідно до яких письмовий запит про подання інформації надсилається платнику податків або іншим суб'єктам інформаційних відносин за наявності хоча б однієї з таких підстав:

1) за результатами аналізу податкової інформації, отриманої в установленому законом порядку, виявлено факти, які свідчать про порушення платником податків податкового, валютного законодавства, законодавства у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму та іншого законодавства, контроль за дотриманням якого покладено на контролюючі органи;

2) для визначення рівня звичайних цін на товари (роботи, послуги) під час проведення перевірок та в інших випадках, передбачених статтею 39 цього Кодексу;

3) виявлено недостовірність даних, що містяться у податкових деклараціях, поданих платником податків;

4) щодо платника податків подано скаргу про ненадання таким платником податків:

податкової накладної покупцю або про допущення продавцем товарів/послуг помилок при зазначенні обов'язкових реквізитів податкової накладної, передбачених пунктом 201.1 статті 201 цього Кодексу, та/або порушення продавцем/ покупцем граничних термінів реєстрації в Єдиному реєстрі податкових накладних податкової накладної та/або розрахунку коригування;

акцизної накладної покупцю або про порушення порядку заповнення та/або порядку реєстрації акцизної накладної;

5) у разі проведення зустрічної звірки;

6) в інших випадках, визначених цим Кодексом.

Запит вважається врученим, якщо його надіслано поштою листом з повідомленням про вручення за податковою адресою або надано під розписку платнику податків або іншому суб'єкту інформаційних відносин або його посадовій особі.

Аналогічні положення містить в п. 10 Порядку періодичного подання інформації органам державної податкової служби та отримання інформації зазначеними органами за письмовим запитом, затвердженим постановою Кабінету Міністрів України від 27.12.2010 року № 1245. Так у відповідності до вказаного пункту запит щодо отримання податкової інформації від платників податків та інших суб'єктів інформаційних відносин оформляється на бланку органу державної податкової служби та підписується керівником (заступником керівника) зазначеного органу. При цьому, у запиті мають бути обов'язково зазначені: посилання на норми закону, відповідно до яких орган державної податкової служби має право на отримання такої інформації; підстави для надіслання запиту; опис інформації, що запитується, та в разі потреби перелік документів, що її підтверджують.

З положень наведеної норми вбачається, що запит податкового органу в обов'язковому порядку повинен містити викладення визначених Податковим кодексом України підстав отримання інформації.

Контролюючі органи надсилаючи інформаційні запити, як правило посилаються на акти перевірок інших контролюючих органів, що порушує п. 10 Порядку періодичного подання інформації органам державної податкової служби та отримання

інформації зазначеними органами за письмовим запитом, фактично не визначивши підстави для надіслання запиту позивачу.

Відповідно до абз. 5 п. 86.7 ст. 86 ПК України, контролюючим та іншим державним органам забороняється використовувати акт перевірки як підставу для висновків стосовно взаємовідносин платника податків з його контрагентами, якщо за результатами складення акта перевірки податкове повідомлення-рішення не надіслано (не вручено) платнику податків або воно вважається відкликаним відповідно до статті 60 цього Кодексу.

У відповідності до п.п. 78.1.1 п. 78.1 ст. 78 ПК України, у податкового органу відсутнє право на отримання від платника податків пояснень з підстав порушення податкового законодавства, а також наявності для податкового органу заборони щодо використання акту перевірки, як підставу для висновків стосовно взаємовідносин платника податків з його контрагентами, а також враховуючи відсутність за результатами складеного акту перевірки прийнятих податкових повідомлень – рішень, слід прийти до висновку, що у контролюючого органу відсутні правові підстави для використання актів перевірки інших контролюючих органів, як податкової інформації в розумінні п.п. 78.1.1 п. 78.1ст. 78 ПК України.

Згідно п. 73.3 ст. 73 ПК України, а також враховуючи абз. 5 п.86.7 ст. 86 ПК України у разі коли запит складено з порушенням вимог, викладених в абзацах першому та другому цього пункту, платник податків звільняється від обов'язку надавати відповідь на такий запит.

Хомишин І.Ю. –
доцент кафедри адміністративного та інформаційного права
Навчально-наукового інституту права та психології
Національного університету «Львівська політехніка»,
кандидат юридичних наук

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

Відомо, що сфера освіти відчуває вплив культури, науки, економіки, політики і техніки в процесі розвитку. Особливо помітний вплив інтегральних політико-економічних, соціально-культурних і науково-технічних факторів, які проявляють себе у вигляді певних тенденцій. Стрімка глобалізація проявляється як в лібералізації світової економіки, взаємозалежності економіки і безпеки всіх країн так само і в глобальній інформатизації суспільства.

У Контексті предмета нашого дослідження особливий інтерес становить інформатизація суспільства, яка ініціює формування інформаційно-комунікативної сфери, роблячи доступною інформацію будь-якого виду для кожної людини планети. Забезпечується така можливість засобами інформаційних технологій, завдяки яким людина здатна накопичувати, зберігати інформацію, працювати з будь-якою інформацією, застосовувати її в професійній діяльності.

В основі соціально-економічного розвитку інформаційного суспільства лежить не матеріальне виробництво, а виробництво інформації та знань. Для будь-якої країни ступінь її економічного і технологічного розвитку, добробуту суспільства пропорційні середньому рівню знань, умінь, навичок і кваліфікацій її активного населення [1, с.5].

З розвитком інформаційних технологій зростає їх роль та використання у сфері освіти. Світовим трендом у сфері освіти стають відкриті онлайн-курси MOOCs і медіа-освіта. Автори наголошують на тому, що впровадження нових технологій навчання та досконале оволодіння ними вимагають певної внутрішньої готовності як викладачів, так і здобувачів вищої освіти до серйозних перетворень, що відповідають умовам швидкозмінного інформаційного суспільства [2, с. 50].

З 2010 року в Україні набула чинності Концепція впровадження медіаосвіти Україні, що має на меті «сприяння розбудові в Україні ефективної системи медіа-освіти заради забезпечення всебічної підготовки дітей і молоді до безпечної та ефективної взаємодії із сучасною системою медіа, формування у них медіа-обізнаності, медіа-грамотності і медіа-компетентності відповідно до їхніх вікових та індивідуальних особливостей» [3]. Онлайн-курси стали сьогодні дуже популярним засобом навчання, Така форма навчання дає змогу інтерактивного спілкування студентів та викладачів, а також прийому іспитів в режимі онлайн. Це одна із найновіших форм дистанційного навчання, яка активно розвивається у світовій освіті.

Використання в освітній практиці технологій, пов'язаних з Інтернетом, дозволяє реалізувати принцип безперервної освіти – «навчання впродовж усього життя», перейти від догматичного заучування до діяльнісного та компетентного підходу – підготовки фахівців, здатних в умовах сучасного виробництва вирішувати наявні проблеми в нетривіальних умовах. Інформаційно-комунікаційні технології мають великі можливості для особистісного розвитку людини, розкриття її потенціалу, тому на сучасному етапі значну роль відіграють дистанційні форми та технології навчання й виховання. Сьогодні без широкого застосування дистанційного навчання навчальні заклади не можуть перемагати в конкурентній боротьбі на ринку освітніх послуг та забезпечувати підготовку кваліфікованих фахівців на сучасному рівні.

Основні принципи дистанційного навчання – це встановлення інтерактивного спілкування між студентом та викладачем без забезпечення їх безпосередньої зустрічі і самостійне освоєння певного масиву знань і навичок за обраним курсом при використанні певних інформаційних технологій [4, с. 167].

В Україні у 2013 році пройшли перші МООС на базі Київського національного університету імені Тараса Шевченка – «Університет онлайн». Перший масовий онлайн-курс, ініційований Іваном Примаченком, стосувався бренд-менеджменту та зібрав понад 9 тисяч учасників.

Весною 2014 року стартував проект інтерактивної онлайн-освіти EdEra, − який створює онлайн-курси та освітній контент широкого спектра з використанням IT. Мета проекту зробити освіту в країні доступною та якісною на зразок західних найкращих освітніх ініціатив.

Звичайно таке онлайн навчання має як переваги так і певні недоліки. До переваг ми відносимо:

− доступ до програм найкращих університетів і викладачів світу;

− найновіша інформація, технології, теорії;

− безкоштовне або доступніше за ціною, ніж денне навчанням в університеті;

− можливість навчатись будь-де і будь-коли.

Але сучасний студент зіштовхується і з труднощами у самомотивації, і з недостатньою кількість спеціалізованих матеріалів вищого рівня складності (більшість матеріалів вступного рівня − для того, щоб охопити якомога більшу аудиторію). Ще одним недоліком онлайн навчання ми вважаєм це ілюзія компетенції, тобто важко оцінити знання чи їх відсутність.

Отже, дистанційна форма навчання це сучасна платформа для отримання знань. І хоча Україна значно відстає від країн зарубіжжя з питань дистанційної освіти, але ми вже бачимо перші кроки які вітчизняна освіта робить у даному напрямі.

У країні не має відповідних програм загальнодержавного та регіонального рівнів. Невисокий рівень комп'ютеризації суспільства та системи освіти зокрема, низьке освоєння навчальними закладами сітьових інформаційних технологій, несформованість національного освітнього простору в Web-середовищі та ін. не дають змоги в даний час реалізувати значні потенційні можливості дистанційного навчання.

Список літератури

1.Триндаде А.Р. Информационные и коммуникационные технологии и развитие человеческих ресурсов // Дистанционное образование. – 2000. – № 2. – С. 5-9

2.Абдалова О. И. Использование технологий электронного обучения в учебном процессе / О. И. Абдалова, О. Ю. Исакова // Дистанц. и виртуал. обучение. – 2014. – № 12. – С. 50–55

3.Концепція впровадження медіа-освіти в Україні // Інститут соціальної та політичної психології Національної академії педагогічних наук України [Електронний ресурс]. – Режим доступу: http://www.ispp.org.ua/news_44.htm

4.Гозман Л. Я. Дистанционное обучение на пороге XXI века / Гозман Л. Я., Шестопал Е. Б. – Ростов-н/Д. : Мысль, 1999. 368 с.

Цьвок М.С. –
асистент кафедри адміністративного та інформаційного права
Навчально-наукового інституту права та психології
Національного університету «Львівська політехніка»

РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЗАБЕЗПЕЧЕННІ ПОРЯДКУ ВІЛЬНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ В ЗАРУБІЖНИХ КРАЇНАХ

Ефективність державного управління в зарубіжних країнах значною мірою пов'язана з широким використанням інформаційно-комунікаційних технологій, які забезпечують вільний доступ та поширення інформації щодо діяльності органів влади, що значною мірою підвищує рівень правової обізнаності громадян та зміцнює їх довіру до владних структур. Інформаційно-комунікаційні технології є також засобом отримання однакового обсягу інформації та знань різними людьми і стимулюють не тільки плідну співпрацю із державними органами, але й розвиток громадянського суспільства.

Право доступу до інформації та належних документів прямо закріплене ст.ст. 11, 42 Хартії основних прав Європейського Союзу від 7 грудня 2000 р Зокрема, статтею 42 визначено, що «кожний громадянин або громадянка Європейського Союзу, чи будь-яка інша фізична або юридична особа, яка проживає або має офіційне зареєстроване місцеперебування в одній з держав-членів, має право доступу до документів інституцій, органів, установ і агентств Союзу, незалежно від носія, на якому вони зафіксовані» [1].

Право на доступ до інформації, що перебуває в розпорядженні державних органів закріплено в Рекомендації Ради Європи N R (2002)2 «Про доступ до офіційних

документів» від 21 лютого 2002 року. Зокрема в ст. 3 зазначено, що «держави-члени повинні гарантувати кожній особі, після здійснення нею запиту, право доступу до офіційних документів, які є в розпорядженні органів державної влади. Цей принцип має застосовуватися без жодної дискримінації, у тому числі й за ознакою державної належності». [2]

Важливе місце серед міжнародних актів у галузі інформаційних технологій посідає Окінавська хартія глобального інформаційного суспільства, яку підписали 8 країн: Великобританія, Німеччина, Італія, Канада, Російська Федерація, США, Франція, Японія. Вони слушно зазначили, що «питання подолання електронно-цифрового розриву всередині держав і між ними посіло важливе місце в національних дискусіях. Кожна людина повинна мати можливість доступу до інформаційних і комунікаційних мереж» (п. 9 Окінавської хартії). Також ці країни визначили, що «інформаційно-комунікаційні технології (ІТ) є одним із найбільш важливих факторів, що впливають на формування суспільства у XXI столітті. Їх революційний вплив стосується способу життя людей, їх освіти та роботи, а також взаємодії уряду та громадянського суспільства. ІТ швидко стають життєво важливим стимулом розвитку світової економіки...» (п. 1 Окінавської хартії) [3];

Очевидно, що ефективне інформаційне забезпечення нерозривно пов’язане з використанням сучасних інформаційних технологій, комп’ютерних мереж та засобів телекомунікації.

Впровадження комп’ютерних технологій в процес державного управління докорінно змінило порядок надання державних послуг, замінивши собою чимало традиційних урядових механізмів. Комп’ютерні технології та прикладні програми електронного врядування поступово проникли в управлінську сферу та допомогли знайти рішення багатьох задавнених проблем, з якими боролися уряди всього світу. Відповідно змінилися й засоби надання інформації, відкривши простір застосуванню мережевих інструментів як кращих і швидших каналів спілкування між урядом і громадянами [4, с. 265].

В зарубіжних країнах громадянам забезпечено вільний доступ до чинного законодавства у сфері інформації через урядові сайти та інші ресурси, що забезпечує прозорість та відкритість роботи уряду.

Зокрема в Австрії вільний доступ до законів забезпечує створена урядом федеральна онлайн-система законодавчої інформації, яка дає громадянам можливість ознайомлюватися з новими законодавчими актами з моменту набрання ними чинності.

З 2001 року одним із головних каналів інформаційного обміну між австрійськими органами влади та громадянами є веб-портал «Help» (http://help.gv.at), який надає інформацію з майже двохсот різних тем, пов'язаних з офіційними процедурами, в тому числі про необхідні документи, розміри державного мита за різні послуги, строки подання документів, онлайн-форми та шаблони. Портальна технологія забезпечує цілодобовий інтерфейс між державними органами та громадянами. За час, що минув з відкриття порталу, він забезпечує виконання дедалі більшої кількості різних процедур у режимі онлайн. Він надає інформацію про всі справи, які громадянин може вести з державними органами (реєстрацію новонароджених, укладання шлюбу, житлові чи паспортні питання) і дає можливість виконувати деякі з цих процедур в електронному режимі. Контент вебсайту розподілений на чотири головні секції, призначені для різних груп населення: фізичних осіб, бізнесменів, молоді та осіб старшого віку. Всі ці сервіси побудовані на основі єдиних критеріїв: прозорість, комплексний характер, ясність інформації та зосередження уваги на основних фактах. [4, с. 267].

Британський уряд створив онлайн-платформу, яка служить для громадян єдиним пунктом доступу до інформації та послуг державного сектора. Портал (www.direct.gov.uk) використовується як центр надання інформації, онлайн-послуг і опитування громадської думки з питань, винесених урядом на широке обговорення. П'ять секцій порталу надають додаткову інформацію, призначену для окремих груп населення – молоді, британців, які проживають за кордоном, батьків, осіб з

обмеженими можливостями та осіб, які за кимось доглядають. [4, с. 270].

В Болгарії у 2000 році з метою підвищення прозорості процесу прийняття рішень, надання громадянам можливості приймати поінформовані рішення і водночас контролювати хід реалізації державних програм. був прийнятий Закон про доступ до публічної інформації Закон наділяє всіх громадян правом доступу до будь-якої інформації, наявної в усіх державних установах. Інформаційний запит може бути поданий також із використанням Інтернет-технологій. Крім того, деякі державні установи запровадили додаткові ініціативи, спрямовані на підвищення прозорості. Це, зокрема, прямі онлайн-трансляції засідань муніципальної ради Софії. Дебати, що відбуваються на цих засіданнях, потім архівуються і розміщуються на веб-сторінці столичного муніципалітету. У 2009 році з метою підвищення прозорості та надання громадянам можливості «ближче придивитися» до дискусій, які відбуваються на міністерських засіданнях, уряд створив нову електронну систему, в якій розміщені повні тексти протоколів і рішень, прийнятих під час урядових засідань. Ці матеріали публікуються у спеціальній секції урядового вебсайту того ж дня, коли відбулася та чи інша дискусія. Так само були проскановані й розміщені в мережі урядові рішення, які приймалися починаючи з 1990 року. Таким чином засоби масової інформації та громадяни мають змогу стежити за розробкою політичного курсу, дізнаватися про причини прийняття/відхилення того чи іншого рішення, контролювати процес їх виконання і притягати міністрів до відповідальності. [4, с. 272].

Вважаємо, що для України цінним є міжнародний досвід щодо використання інформаційно-комунікаційних технологій в процесі державного управління. Доцільно для врегулювання цього питання створити окремий законодавчий акт на основі міжнародного досвіду, беручи до уваги загальноприйняті світові законодавчі норми щодо інформатизації та інноваційної діяльності.

Список літератури

1. Хартія Основних прав Європейського Союзу: Міжнародний документ від 07 грудня 2000 р. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_524.

2. Рекомендації Ради Європи № R (2002)2 від 21 лютого 2002 р. «Про доступ до офіційних документів»: Рада Європи, Комітет Міністрів Ради Європи; Рекомендації, Міжнародний документ від 21 лютого 2002 р. № R(2002)2 [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/994

3. Окінавська хартія глобального інформаційного суспільства: Великобританія, Німеччина, Італія [...]; Хартія, Міжнародний документ від 22 липня 2000 р. // Дипломатический вестник. – 2000. – № 8. – С. 51 – 56.

4. Національні та міжнародні механізми фінансування громадянського суспільства. Міжнародні заходи зміцнення довіри між державою та громадянським суспільством. – К.: Фенікс, 2011. – 336 с.

Yudkova K.V.
graduate student, Scientific and Research Institute of Informatics and Law NALS of Ukraine,
deputy vice-rector for international collaboration NTUU «KPI»

INFORMATION TECHNOLOGIES IN A FRAMEWORK OF HUMAN RIGHTS PROTECTION

We live in a world where information and communication technologies (hereafter referred to as IT) and extensive flow of information have become the natural and unmistakable features of modern life.

Today, human rights in the information sphere (concerning to usage the Internet), in fact, include:

– The right of access to the Internet;

– The right to a full life with the use of the Internet;

– The right to a balanced use of the Internet in everyday life;

– The right to freedom of speech and expression within the Internet.

– The right to education, knowledge and communication through the Internet.

Mentioned rights give rise to the main areas of organizational and technical complexities and challenges that must be addressed. Said direction can be classified into the following groups:

1) «End user» – respect the rights of a specific person, the protection of his honor and dignity, and other non-property rights associated with the human personality;

2) «Legal frameworks» - the fact that legal regulation has low level of dynamic of development than process of the formation of new public relations;

3) «Jurisdictional complexity» – here we mean the cross-regional dissemination of information in general and separate informational flows. That is, as a result of the absence of de facto borders and boundaries for the dissemination of information the necessity to the permanent coordination of the national law of the various states arise worldwide. It is also important process of integration of the specific local (state) law in international practice;

4) «Technological complexity» – high speed high speed and turnover of the progress and of the development of new technologies with the unpredictable, often negative, consequences for human rights;

5) B2B and B2G relations – relations in the framework «business to business» and «business to government» in the field of human rights.

Many companies are already taking strong steps to share the IT more wider within the global audience. For example, Unilever's company has partnered with Facebook company under the direction by Internet.org alliance, to understand how to provide Internet access to millions of people across rural India (currently, only about 12% of the Indian population has access to the Internet [1]).

Informatively: Internet.org Alliance - a global partnership between leaders in technology, non-profit organizations, local communities and experts who work together to «Expanding access to the Internet aimed to bring the Internet up to two-thirds of the world's population that does not have it» [2]. The founders and partners: Ericsson, Facebook, Mediatek, Nokia, Opera, Qualcomm and Samsung.

Another example of both B2B and B2G relations is a project created by Amnesty International. Thus, the company has developed

a «panic button». Mentioned mobile application has an intuitive interface and implementation in the form of a standard tool - which allows users to secretly send a notification to pre-selected contacts by quickly pressing the phone's power button (or any another button on the external casing). One of among other objectives pursued: to provide journalists who are attacked or detained, the ability to report it to the competent persons (authorised bodies). Described situation of journalists inability to protect themselves took place in just a few years ago. And today, any mobile gadgets equipped by such button.

However, development of B2B and B2G relations in the field of human rights has also a number of negative aspects. Thus, in many countries, Internet companies are faced with requirements to restrict access to Web sites, delete user-generated content or provide personal information to law-enforcement agencies or other government agencies. Risks to human rights, freedom of expression and privacy are relevant to the whole chain of IT usage (from technological issues to organizational matters). For example, the introduction of IT usage monitoring system during the elections in Iran caused serious public debate and has attracted the attention of a number of human rights organizations. Another one example - revealing disparity to the state requirements of telecommunication service providers (as a result - its vulnerability) in Egypt led to the mass closure of such providers.

Thus, there are several «risk drivers»:

1) Telecommunications Services (for example, the state requirements to disclose the privacy information aimed to assist law-enforcement agencies or other government agencies);

2) Mobile phones and other mobile devices (the risks of breaches of confidentiality, which are caused by the possibility of a hidden location determination);

3) Internet services (possibility of a legally or illegally gain access to the contents of the filter, to remove, block or disable individual user accounts, as well as significant risks of information storage using a so-called cloud resource (often vulnerable);

4) Home appliances (Smart Electronics) (risks of installed special software to covert surveillance and recording information).

In the interconnection between human rights, business, government, law-enforcement agencies or other government

agencies, as well as the interests of national security it is important to clarify some of the specific features of such relations. Named specificity can be accurately described by the statement that perfectly expressed in 2008, the Special Representative of the Secretary-General of the United Nations on business and human rights: all the States must protect human rights, and companies are responsible for the lack of respect for human rights [3].

It is necessary to designate two pitfalls in mentioned relationships:

at first, there are legitimate reasons for the state (law-enforcement agencies or other government agencies) and various companies to restrict the free flow of information (for example, the removal of images of violence) or, on the contrary, allow access to personal information (such as the fight against fraud, terrorism). In this context, can we talk about the positive intervention, since the main purpose is to protect human rights;

secondly, while the said activity (justified interference) in the examples carried out with positive aims, however, there is always a risk that an external organization (public or private entities) require to translate privacy in public - for its protection, transparency etc. That is, to create a legal basis for intervention. In this case it would be appropriate to specify as an example of informational reservation of North Korea.

The contrast between these features of the relationship is great. Therefore, the most correct approach is to keep the balance:

– Transparency of legal regulation;

– The consistency of national law and international norms and practices;

– Practice of justified intervention;

– Individual and situational approach.

References

1. Data of International Telecommunication Union : http://www.itu.int/en
2. Official web Internet.org : https://info.internet.org/en/
3. Data of The Office of the United Nations High Commissioner for Human Rights (OHCHR) : http://www.ohchr.org

Секція 2.

ПРИВАТНО-ПРАВОВІ ПРОБЛЕМИ СФЕРИ ІТ

Вінник О.М. –
професор кафедри господарського, повітряного та космічного права Юридичного інституту Національного авіаційного університету, доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України

ПРАВОВІ ЗАСАДИ ЕЛЕКТРОННОГО БІЗНЕСУ

Електронна комерція, віртуальний офіс, електронна форма договору і цінних паперів, веб-сайт компанії, на якому розміщується інформація про її діяльність, в т.ч. вироблені нею/пропоновані до продажу товари/роботи/послуги, – ось неповний перелік нових понять, що характеризують сучасне підприємництво, яке вже неможливо уявити без електронних засобів ведення бізнесу. Своєю чергою, це передбачає відповідне закріплення в законодавстві таких способів здійснення підприємницької діяльності. Проте в прийнятому 2015 р. Законі «Про електронну комерцію» поняття електронна комерція трактується вузько: як відносини, спрямовані на отримання прибутку, що виникають під час вчинення правочинів щодо набуття, зміни або припинення цивільних прав та обов'язків, здійснені дистанційно з використанням інформаційно-телекомунікаційних систем, внаслідок чого в учасників таких відносин виникають права та обов'язки майнового характеру [1, п. 1 ч. 1 ст. 3]. Тобто це поняття охоплює лише одну складову ведення бізнесу, а саме: відносини щодо реалізація товарів, робіт, послуг за плату.

Разом з тим, термін «комерція» традиційно визначається як підприємницька діяльність, тобто діяльність щодо виробництва зазначених благ з метою їх реалізації за прибуткову плату, що має забезпечити самофінансування суб'єкта підприємництва. Тому в країнах з дуалістичною системою приватного права кодекси, що регулюють відносини у сфері підприємництва, іменуються комерційними (Франція [2]), або торговими (Німеччина [3], Японія [4]). Відтак, електронну комерцію можна розглядати і в додатковому ракурсі, як функціонування суб'єктів підприємництва та використання ними в процесі вищезгаданої діяльності електронних засобів зв'язку. З огляду на ці обставини обґрунтованим видається використання поняття електронного бізнесу (**E-business**) як ведення будь-якої бізнес-діяльності у глобальних телекомунікаційних мережах, зокрема в мережі Інтернет [5].

Проте в чистому вигляді такий бізнес ще не став переважаючим, хоча його елементами пронизана майже вся підприємницька діяльність та функціонування її суб'єктів, що знайшло віддзеркалення в нормативно-правових актах, серед який не лише Закон «Про електронну комерцію» [1] , що встановлює порядок вчинення електронних правочинів із застосуванням інформаційно-телекомунікаційних систем та визначає права і обов'язки учасників відносин у сфері електронної комерції, а й прийняті задовго до нього акти, зокрема:

- Господарський кодекс України [6], в якому нещодавно було закріплено положення про оприлюднення державними (в т.ч. казенними) та комунальними підприємствами, господарськими товариствами, що контролюються державою або органом місцевого самоврядування, інформації про свою діяльність, крім випадків, встановлених законом, шляхом розміщення її на власній веб-сторінці/веб-сайті) або на офіційному веб-сайті суб'єкта управління об'єктами державної/комунальної власності, що здійснює функції з управління підприємством, у строки та порядку, встановлені Урядом (щодо господарських організацій, контрольованих державою) чи відповідною місцевою радою (щодо комунальних підприємств та господарських товариств з переважаючою

часткою територіальної громади в статутному капіталі); при цьому доступ до таких веб-сторінок та веб-сайтів має бути цілодобовим і безоплатним [6, статті 73, 75, 77, 78, 79, 90];

- Закон «Про акціонерні товариства» [7], який передбачає: (а) розміщення на власному веб-сайті акціонерного товариства інформації про проведення загальних зборів акціонерів (ст. 35), а також про можливість надання акціонерам для ознайомлення в *електронній формі* документів, на підставі яких прийматимуться рішення на загальних зборах (ст. 36); (б) бездокументарну форму акцій [7, ч. 2 ст. 20] як виду цінного паперу, що існує у формі електронного документа [8, ч. 3 ст. 3];
- Закон «Про публічні закупівлі» [9], в якому закріплено визначення понять (ст. 1): *авторизований електронний майданчик* (авторизована Уповноваженим органом інформаційно-телекомунікаційна система, яка є частиною електронної системи закупівель та забезпечує реєстрацію осіб, автоматичне розміщення, отримання і передання інформації та документів під час проведення процедур закупівель, користування сервісами з автоматичним обміном інформацією, доступ до якого здійснюється за допомогою мережі Інтернет), *веб-порталу Уповноваженого органу* з питань закупівель (інформаційно-телекомунікаційна система, до складу якої входять модуль електронного аукціону і база даних, та який є частиною електронної системи закупівель та забезпечує створення, зберігання та оприлюднення всієї інформації про закупівлі, проведення електронного аукціону, автоматичний обмін інформацією і документами та користування сервісами з автоматичним обміном інформацією, доступ до якого здійснюється за допомогою мережі Інтернет), *електронної системи закупівель* (інформаційно-телекомунікаційна система, що забезпечує проведення процедур закупівель, створення, розміщення, оприлюднення та обмін інформацією і документами в електронному вигляді, до складу якої входять веб-портал Уповноваженого органу, авторизовані електронні майданчики, між якими забезпечено автоматичний обмін інформацією та документами), *інформаційного ресурсу Уповноваженого органу* (сайт, наповнення якого здійснює

Уповноважений орган та на якому надаються безоплатні консультації з питань закупівель, доступ до якого здійснюється через мережу Інтернет), а також положення про *оприлюднення інформації про закупівлі на веб-сайтах замовника* (у разі наявності) або веб-сайтах відповідних органів влади, органів місцевого самоврядування (ст. 10);

- Закон України «Про державне регулювання ринку цінних паперів в Україні» [10], що містить положення щодо розміщення інформації про призначення тимчасового адміністратора у день його призначення на офіційному веб-сайті Національної комісії з цінних паперів та фондового ринку (ст. 11-1).

Аналіз лише вищезгаданих положень господарського законодавства свідчить про обов'язкову наявність у суб'єктів господарювання, які мають певну організаційно-правову форму (АТ, зокрема), контролюються носієм публічних інтересів (державою/органом місцевого самоврядування) або є *уповноваженим* (на певному ринку/щодо певних аспектів ведення бізнесу) органом *власного веб-сайту*, на якому має розміщуватися обов'язкова для оприлюднення інформація. Однак зазначені положення є неповними, оскільки не містять норм про обов'язковість своєчасного оновлення розміщеної на сайті інформації та наслідки невиконання/неналежного виконання такого обов'язку.

Найближчим часом мають бути внесені зміни до законодавства щодо *усунення адміністративних бар'єрів для експорту послуг з використанням електронних засобів зв'язку* [11; 12]. Проте положення щодо ведення бізнесу з використанням таких засобів потребує консолідації в одному акті законодавства, яким може стати розширена (порівняно з нині чинною) редакція Закону «Про електронну комерцію» [1], в якому мають визначатися основні засади ведення бізнесу з використанням електронних ресурсів, включно з електронною комерцією у вузькому розумінні (як реалізація за плату результатів підприємницької діяльності). Відповідно, мають бути визначені пов'язані з цим обов'язки суб'єктів підприємництва та уповноважених органів, включно з наявністю у них власного веб-сайту (веб-сторінки) для розміщення

інформації, що підлягає оприлюдненню, вчасному внесенню змін до такої інформації, відповідальність та інші наслідки за порушення такого обов'язку (в т.ч. можливість визнання недійсними договорів, що були укладені на підставі несвоєчасно оновленої на веб-сайті/веб-сторінці інформації, тобто такої, що ввела в оману контрагента). Це дозволить забезпечити прозорість і зрозумілість правового регулювання ***Е-бізнесу*** для пересічних його учасників та споживачів, які не мають можливості часто звертатися до недешевих послуг бізнес-юристів, а відтак – відповідатиме соціальному спрямуванню економіки України, що має забезпечуватися державою відповідно до положень Конституції України [13, ч. 4 ст. 13] та Національної стратегії сприяння розвитку громадянського суспільства в Україні на 2016 – 2020 роки, спрямованої на створення належних умов для ефективної взаємодії держави, громадянського суспільства та бізнесу задля модернізації України, підвищення добробуту і створення рівних можливостей для всіх [14].

Список літератури

1.Закон від 03.09.2015 р. «Про електронну комерцію» // Відомості Верховної Ради України (ВВР), 2015 р., № 45, ст. 410.

2.Коммерческий кодекс Франции / Перевод с французского, пред., доп., коммен. и справ. аппарат В.Н. Захватаева. М. : Волтерс Клувер, 2010. – 672 с.

3.Торговое уложение Германии. Закон об акционерных обществах. Закон об обществах с ограниченной ответственностью. Закон о производственных и хозяйственных кооперативах / пер. с нем. Е.А. Дубовицкая ; сост. В. Бергман. – М. : Волтерс Клувер, 2005. – 596 с.

4.Торговый кодекс Японии. Пер. с япон. А. А. Лыхо / Под общ. ред. Тэцуо Сато.- М.: МИКАП, 1993.- С. 17-166.

5.Борецька І.Ю. Марєєв С.В. Степова С. В. Електронна комерція як складова частина електронного бізнесу [Електронний ресурс] // Режим доступу: // http://www.rusnauka.com/15_APSN_2010/Informatica/67272.doc.htm (дата доступу 07.11.2016 р.). – Назва з екрана.

6.Господарський кодекс України від 16.01.2003 // Відомості Верховної Ради України (ВВР), 2003, № 18, № 19-20, № 21-22, ст.144

7.Закон від 17.09.2008 р. «Про акціонерні товариства» // Відомості Верховної Ради України (ВВР), 2008, N 50-51, ст.384

8.Закон від 23.02.2006 р. «Про цінні папери та фондовий ринок» // Відомості Верховної Ради України (ВВР), 2006, N 31, ст.268

9.Закон від 25.12.2015 р. «Про публічні закупівлі» // Відомості Верховної Ради (ВВР), 2016, № 9, ст.89

10. Закон України від 30.10.1996 р. «Про державне регулювання ринку цінних паперів в Україні» // Відомості Верховної Ради України (ВВР), 1996 р., № 51, ст. 292.

11. А. Пасютина. Украинским айтишникам решили облегчить экспорт услуг. Но вряд ли это побудит их легализоваться [Електронний ресурс] // Режим доступу: // http://strana.ua/articles/analysis/38924-ukrainskie-frilansery-smogut-zaklyuchat-mezhdunarodnye-dogovora-po-email.html (дата звернення 08.11.2016 р.). – Назва з екрана.

12. Проект Закону про внесення змін до деяких законодавчих актів України (щодо усунення адміністративних бар'єрів для експорту послуг) № 4496 від 21.04.2016 [Електронний ресурс] // Режим доступу: // http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=58833 (дата звернення 09.11.2016 р.). – Назва з екрана.

13. Конституція України від 28.06.1996 р. // Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141.

14. Указ Президента України від 26.02.2016 р. № 68/2016 «Про сприяння розвитку громадянського суспільства в Україні»[Електронний ресурс] // Режим доступу: http://www.president.gov.ua/documents/682016-19805 (дата звернення 09.11.2016 р.). – Назва з екрана.

Гарасимів Т. З. –
заступник директора
Навчально-наукового інституту права та психології
Національного університету «Львівська політехніка»,
професор кафедри теорії та філософії права
Навчально-наукового інституту права та психології
Національного університету «Львівська політехніка»,
доктор юридичних наук, професор

РЕГУЛЯЦІЯ ПОВЕДІНКИ ОСОБИ У ВІРТУАЛЬНОМУ СЕРЕДОВИЩІ

З початку XXI ст. впровадження сучасних інформаціних технологій буквально в усі сфери людського життя кардинально трансформує суспільство. Особливо інтенсивно на тлі бурхливого прогресу цих технологій виділяється всесвітня глобальна мережа Інтернет, яка змінює умови формування особистості. Інтернет як соціальний інститут має цілу низку специфічних характеристик, що визначають процес соціалізації особи, що відрізняється від традиційних соціальних інститутів (сім'ї, громадські організації, освітні, релігійні установи тощо).

Він являє собою соціокультурне середовище, яка відрізняється локалізацією в кіберпросторі, особливими можливостями задоволення і/або квазізадоволенням численних потреб сучасної людини; потенціалом трансформації структури самосвідомості особистості в процесі трансляції культурних цінностей, норм і правил поведінки в Інтернеті. Такі безперечні переваги Інтернету, як доступність, мобільність, оперативність, анонімність, свобода самовираження, здатні активно впливати як на позитивні, так і на негативні аспекти в процесі соціалізації особи.

Мічіо Кайку у книзі «Фізика майбутнього» зазначає, що «мета повсюдної комп'ютеризації – вселити комп'ютер у наш світ: умістити чіпи всюди» [1, с. 50]. Науковець передбачає, що «до середини сторіччя ми житимемо у повністю функціональному кіберсвіті, що поєднуватиме реальний світ зі зображеннями комп'ютера» [1, с. 60].

Особливо актуально знати, як впливають ці особливості на формування моральної сфери особистості. І перша особливість, про яку слід пам'ятати, це те, що віртуальна реальність, в якій сьогодні перебуває іноді більша частина життя і дозвілля особи, ніяк не пов'язана з моральним законом і моральними нормами спільного існування людей саме в силу автономності, анонімності та повної свободи від будь-яких обмежень інтернет-середовища.

Сьогодні вже слід говорити про постлюдину – гіпотетичний образ майбутньої людини, яка відмовляється від традиційної людської подоби на користь впровадження інформаційних, біотехнологічних, медичних інноваційних технологій в своє тіло і психіку [2]. Якщо зовсім недавно цей образ вживався тільки в науковій фантастиці, то сьогодні активно формується позитивне і раціональне ставлення до можливостей так званого «покращення» людини [2], які спрямовані на подолання страхів, пов'язаних з переглядом традиційного антропологічного образу людини.

С. Хоружий, аналізуючи практичні технології, що ведуть до постлюдини, зазначає, що вихід в кіберпростір, «віртуальна кіборгізація» – це віртуальна практика, яка представляє собою один з типів граничних антропологічних практик, технологій

трансформації людини. І якщо перебування у віртуальному світі домінуватиме над традиційними сферами життєдіяльності, то це призведе до евтаназії. Стане практикою припинення життя людини [3]. Фактично це означає, що якщо людина перестає бути носієм морального закону, який зосереджений в її совісті, вона перестає бути людиною за своєю природою, перестає бути особистістю в традиційному розумінні і стає таким собі іншим видом живих істот або скоріше гібридом людини з інноваційними технічними засобами майбутнього. Відбуватиметься трансформація людської природи через усунення традиційного механізму виховання та формування мотиваційних структур і відповідних причинних схем, відповідальних за моральну поведінку.

Стрімкий розвиток інтернет-середовища, створює очевидні труднощі, які будуть виникати в процесі морального життя особистості. По-перше, в ситуаціях, коли віртуальна реальність є основною життєвою реальністю, в якій особа шукає ідеали для самоідентифікації, не формуються причинні схеми, що визначають статус особистості як суб'єкта моральних дій. По-друге, ситуація необмеженої свободи дій у віртуальній реальності створює ілюзію вседозволеності, яка часто переноситься на поведінку в реальному житті. По-третє, транзитна ідентичність не забезпечує самототожності особистості в часі, що загрожує психічними розладами. По-четверте, існування у віртуальної реальності часто направлено на порушення будь-яких норм, в тому числі і моральних, що фактично деформує свідомість, позбавляє її чутливості у процесі морального вибору.

Список літератури

1.Мічіо Кайку. Фізика майбутнього. / Переклала з англ. Анжела Кам'янець. – Львів: Літопис, 2013. – 432 с.

2.Прайд В. Модификация человека в XXI веке [Електронний ресуср]. – Режим доступу: http://rutracker. org/forum/viewtopic.php?t=1378178

3.Сергей Хоружий. О мутантах и Клонах [Електронний ресуср]. – Режим доступу: http://rumagic. com/ru_zar/sci_philosophy/horujiy/m/j2.html

Довгань Ю. –
здобувач кафедри адміністративного права
Інституту права ім. князя Володимира Великого МАУП

ІНФОРМАЦІЯ ПРО ЯКІСТЬ ПРОДУКТІВ ХАРЧУВАННЯ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ПРАВ СПОЖИВАЧІВ

Захист прав громадянина як споживача є однією з найважливіших ознак демократичного суспільства та напрямом захисту конституційних прав громадян. Науково-технічний прогрес і пов'язаний із цим економічний розвиток актуалізували необхідність оновлення юридичних механізмів захисту прав споживачів від недоброякісних товарів, результатів робіт та послуг. Це завдання вимагає об'єднаних зусиль науки і практики, удосконалення державної політики.

В Україні право на захист прав споживачів закріплено в Основному Законі – Конституції України, стаття 42 якої передбачає, що держава захищає права споживачів, здійснює контроль за якістю й безпечністю продукції та всіх видів послуг і робіт, сприяє діяльності громадських організацій споживачів [1].

Одним із важливих завдань у цьому контексті є забезпечення права громадян-споживачів на вільний доступ до інформації про якість харчових продуктів.

Слід зауважити, що право споживача на повну і достовірну інформацію про товари є пріоритетним у всьому світі. У науковій юридичній літературі теж висвітлюється це питання. Вчені-правознавці намагаються розглянути юридичні підстави для забезпечення такого права людини [1].

Стаття 15 Закону України «Про захист прав споживачів» [2] зазначає, що споживач має право на одержання необхідної, доступної, достовірної та своєчасної інформації про продукцію, що забезпечує можливість її свідомого компетентного вибору. Уявляється, що інформація про продукцію повинна містити, у тому числі позначку про наявність у її складі генетично модифікованих компонентів. Відповідно до ст. 1 Закону України «Про якість та безпеку харчових продуктів і продовольчої сировини» [3] безпека харчових продуктів — це відсутність загрози шкідливого впливу харчових продуктів, продовольчої

сировини та супутніх матеріалів на організм людини. Тим самим визнається, що харчові продукти можуть бути небезпечні для громадян. Тому важливим є можливість отримання достовірної інформації про якість продукту та його склад.

Організація Об'єднаних Націй оголосила нинішнє століття століттям біотехнології. Це пов'язано з тим, що останнім часом з'явилися певні досягнення у галузі генної інженерії, які в багатьох країнах набули пріоритетного значення.

У 2000 р. у Монреалі (Канада) був підписаний Картахенський протокол із біобезпеки, який став першим міжнародним документом, що регламентує торговельні відносини між країнами у сфері генно- модифікованих організмів. У 2002 р. Україна приєдналася до цього міжнародного документа.

Аналіз норм цього акту (зокрема, преамбули) дозволяє зробити висновок, що міжнародна спільнота визнає, що в результаті генної інженерії відбувається шкідливий вплив на біологічне розмаїття, а також на здоров'я людини, але в той же час стверджує, що сучасна біотехнологія відкриває неабиякі можливості для підвищення добробуту людей.

Отже, Україна зробила декілька кроків у правовій регламентації вказаного питання.

Так, приєднання до Картахенського протоколу для країни створює передумови для утворення національної системи біобезпеки. Угодою про Технічні бар'єри в торгівлі визнається, що в жодній країні не може бути заборонено вжиття заходів, необхідних для захисту її інтересів безпечності та безпосередньо не забороняється введення маркування продукції, виготовленої з ГМО, а також заходів, які є необхідними для забезпечення якості її експорту чи захисту життя або здоров'я людини, тварин чи рослин, захисту навколишнього середовища, або для запобігання шахрайським діям на тому рівні, який така країна вважає за потрібне, за умови дотримання вимог про те, що такі заходи не мають застосовуватися у спосіб, що являв би собою засіб свавільної або невиправданої дискримінації між країнами, де переважають такі ж умови або приховане обмеження міжнародної торгівлі, та відповідати іншим положенням цієї Угоди.

Верховна Рада України прийняла Закон України «Про державну систему біобезпеки при створенні, випробуванні, транспортуванні та використанні генетично модифікованих організмів» [4]. У ньому визначена державна політика в галузі поводження з ГМО, врегульовано питання поводження з ГМО та генно-інженерної діяльності у замкненій та відкритій системах, використання, транспортування, зберігання та утилізації ГМО. Проте навіть встановлення цих правил не дає гарантії щодо унеможливлення розповсюдження таких організмів у природне середовище. До того ж на сьогодні державні органи не мають реєстру генетично модифікованих організмів – увезених, вироблених тощо.

Список літератури

1. Ізотова Л. Право на інформацію як чинник якості життя / Л. Ізотова // Унів. наук. зап. – 2007. – № 2 (22). – С. 308-311; Пунда О. О. Право на безпеку харчових продуктів та предметів побуту у правовій системі України: цивільно-правовий аспект / О. О. Пунда // Життя і право. – 2004. – № 3. – С. 45-50.
2. Рабінович П.М. Права людини і громадянина у Конституції України (до інтерпретації вихідних конституційних положень) / П.М. Рабінович. – Х., 1997. – С. 7.
3. Відомості Верховної Ради. – 1991. - № 30. – Ст. 379.
4. Відомості Верховної Ради. – 2002. - № 48. – Ст. 359.
5. Відомості Верховної Ради. – 2007. - № 35. – Ст. 484.

Еннан Р. Є.,
доцент кафедри права інтелектуальної власності Національного університету «Одеська юридична академія», старший науковий співробітник НДІ інтелектуальної власності НАПрН України, кандидат юридичних наук, доцент

ПРАВОВЕ РЕГУЛЮВАННЯ ВІДНОСИН У МЕРЕЖІ ІНТЕРНЕТ

Інтернет є глобальною телекомунікаційною мережею, яка з початку виникла як засіб зв'язку для вузького кола фахівців (основними користувачами мережі у 60-х – 70-х рр. XX ст. були

службовці Міністерства оборони США), проте з часом швидко перетворилася в масове соціальне явище. Від інших глобальних мереж Інтернет відрізняється як за змістом інформації, так і за умовами доступу. На відміну від інших комп'ютерних мереж, єдиних правил доступу до інформації в Інтернеті не існує. На відміну від будь-якого іншого соціального середовища мережа Інтернет не є територіально відокремленою і централізовано керованою системою, що дозволяє розглядати її як якісно нове явище з новими правилами взаємодії [1, с. 58].

Інтернет – це всесвітня інформаційна мережа загального доступу, яка логічно пов'язана глобальним адресним простором та базується на Інтернет–протоколі, визначеному міжнародними стандартами. Інтернет зазвичай характеризують як «комп'ютерну мережу», «інформаційну мережу», «телекомунікаційну мережу» і застосовують до неї такі терміни: «віртуальність», «віртуальний простір», «віртуальне середовище», «кіберпростір». Отже, *Інтернет* – це інформаційна система, тобто сукупність телекомунікаційних мереж і засобів для накопичення, оброблення, зберігання і передавання даних.

Інтернет є екстериторіальним інформаційним простором, що має глобальний, міжнародний характер. *Інтернет* – це єдиний інформаційний простір, в якому відбуваються глобальні процеси соціальних комунікацій та якому притаманний всесвітній загальний характер доступу.

При цьому Інтернет у цілому *не є суб'єктом права*, оскільки це не міжнародна організація або юридична особа чи взагалі будь-яка інша організована структура. Інтернет у цілому *не є об'єктом права*, тому що не існує єдиного конкретного власника мережі, і взагалі не існує суб'єкта, який би управляв чи контролював значну частину цієї мережі. Крім того, Інтернет в цілому *не є засобом масової інформації*, оскільки власник інформаційного ресурсу не робить жодних активних дій щодо доставки інформації до споживача [2, с. 26].

До основних *ознак мережі Інтернет* можна віднести такі: 1) Інтернет як технологічна система, що забезпечує обмін інформацією між комп'ютерами є різновидом мережі електрозв'язку – телекомунікаційної мережі; 2) Інтернет як

система інформаційного зв'язку регулює суспільні відносини з приводу обміну даними; 3) глобальний, екстериторіальний, міжнародний характер Інтернету; 4) Інтернет відкритий для використання всіма фізичними та юридичними особами, тобто є мережею зв'язку загального користування; 5) мережа Інтернет призначена для передачі (обміну) електронних даних.

Розглядаючи види інформаційної діяльності, які проводяться в межах або за допомогою мережі Інтернет, слід звернути уваги на їх неоднорідність. Саме тому необхідно приділити увагу *правовідносинам, пов'язаним з функціонуванням мережі Інтернет* (*Інтернет–відносинам*), які, зокрема, стосуються таких питань: регулювання змісту (контенту – інформаційного наповнення Інтернет-ресурсів); запобігання кіберзлочинності; захист конфіденційної інформації та персональних даних; захист прав інтелектуальної власності; електронна комерція (торгівля); захист прав споживачів; захист прав людини [3, с. 7].

Правовідносини, що виникають з приводу функціонування мережі Інтернет (*Інтернет–відносини*), характеризуються такими *ознаками*: 1) обмін інформації відбувається відбувається в електронній цифровій формі; 2) віддаленість суб'єктів цих відносин у просторі; 3) наявність суб'єктів, які не ініціювали ці відносини, проте мали організаційно-технічну можливість здійснити вплив на них; 4) використання програмного забезпечення, технічних стандартів і протоколів; 5) схильність цих відносин до саморегуляції; 6) технологічна складність мережі Інтернет; 7) поширені можливості порушення інформаційних прав суб'єктів цих відносин; 8) технічний, культурний та освітній ценз суб'єктів цих відносин.

Суспільні відносини, що виникають у зв'язку з використанням глобальних комп'ютерних мереж, є особливими інформаційними відносинами, спрямованими на організацію руху інформації у суспільстві. Інтернет-відносини обумовлені інформаційною природою комунікацій інформаційного суспільства, бути учасниками яких можливо лише за допомогою ЕОМ, підключеної до комп'ютерної мережі.

Особливістю цих відносин також є наявність технічного компоненту, інформаційне наповнення, особливий суб'єктний склад. Це суспільні відносини, що існують в електронно-цифровій формі у кіберпросторі. Варто також зазначити, що суб'єкти цих відносин можуть знаходитися у різних країнах, а їх діяльність регулюватися законодавствами різних країн. Інтернет-відносини не можуть існувати без використання інформаційно-телекомунікаційних технологій і мереж. Ці відносини мають інформаційне наповнення, тобто складаються щодо інформації в Інтернеті [4, с. 255].

Інтернет-відносини можна класифікувати за такими ознаками:

1) *в залежності від суб'єктів*: між розробниками інформаційних мереж та їх партнерами; між спеціалістами, які створюють (виробляють) і розповсюджують інформацію в Інтернеті; між інформаційними провайдерами, що надають ліцензії на здійснення он-лайнових послуг; між громадянами, організаціями, фірмами та іншими споживачами (користувачами);

2) *в залежності від державної приналежності фізичних і юридичних осіб*: між вітчизняними та іноземними провайдерами; між іноземними провайдерами та вітчизняними користувачами; між вітчизняними юридичними особами та іноземними громадянами; між вітчизняними та іноземними розробниками мереж; між фахівцями;

3) *в залежності від мети виникнення відносин та інформаційного впливу*: внутрішні відносини (відбуваються у кіберпросторі); зовнішні відносини (пов'язані з наданням зовнішніх інформаційних послуг).

Отже, *Інтернет-відносини* це суспільні відносини у кіберпросторі, учасники яких є носіями суб'єктивних прав та обов'язків у мережі Інтернет. *Інтернет-відносини* – це особливі суспільні відносини, які виникають у результаті впливу норм інформаційного, комп'ютерного, міжнародного та інших галузей права, міжнародних договорів на поведінку суб'єктів цих відносин. Інтернет-відносини – це новий тип суспільних відносин, що виникають, змінюються та припиняються у кіберпросторі. Це не лише правові, фактичні, етичні відносини,

це складні соціальні зв'язки особливої правової, інформаційної та технічної природи [20, с. 50].

Правове регулювання Інтернет–відносин це цілеспрямований вплив на процеси у цифровому середовищі мережі Інтернет правовими засобами з метою їх впорядкування та розвитку. Це також плив на поведінку суб'єктів права за допомогою норм права, що забезпечує їх нормальну роботу. Інтернет формує особливу інформаційну сферу (Інтернет-сферу), пов'язану з оборотом цифрової інформації. Таким чином, *Інтернет-відносини* – це суспільні відносини, що пов'язані з соціально-правовим регулюванням віртуального простору, тобто з регулюванням цього простору за допомогою норм права, моралі, етики та інших засобів.

Структура Інтернет-відносин містить такі складові: суб'єкти, об'єкти, суб'єктивні права та обов'язки, інформація, технічні засоби. Щодо *суб'єктів* цих відносин необхідно зазначити, що в даному випадку йдеться про таких суб'єктів – учасники інформаційних контактів і процесів, учасники зв'язку та інформаційної взаємодії. В інформаційному просторі і процесах діє безліч посередників – провайдерів або операторів в системі мережі Інтернет та інших суб'єктів, що надають різноманітні види послуг. Одним з важливих факторів в сфері Інтернет є «віртуалізація» суб'єктів і віртуалізація відносин в системі глобальної інформаційної взаємодії різних структур. До суб'єктів правовідносин в Інтернеті зазвичай відносять: операторів зв'язку; постачальників послуг доступу в Інтернет; постачальників інформації; користувачів [6, с. 44].

Розглядаючи окремі види інформаційної діяльності, які відбуваються в межах або за допомогою Інтернет, необхідно виділити їх неоднорідність. Окрім необхідності запровадження певної класифікації як самих правовідносин щодо мережі Інтернет, пропонується виділяти суб'єктів цих правовідносин, які діють в мережі Інтернет.

Суб'єктами Інтернет-відносин є: 1) оператори та провайдери телекомунікацій, які забезпечують функціонування мережі Інтернет як інформаційної системи; 2) виробники, власники і розповсюджувачі інформації та інформаційних ресурсів, які створюють інформаційне наповнення мережі

Інтернет; 3) суб'єкти, які надають специфічні послуги з укладання електронних (мережевих) угод (договорів) за допомогою мережі Інтернет, тобто все те, що охоплюється терміном «електронна комерція (торгівля)»; 4) споживачі (користувачі) телекомунікаційних послуг.

Перша група суб'єктів Інтернет-відносин надає такі основні види інформаційних послуг: підключення (забезпечення доступу до мережі); адміністрування (забезпечення функціонування технічних засобів підтримки адресного простору Інтернет); хостинг (розміщення інформаційних ресурсів замовника на веб-серверах і забезпечення доступу до цих ресурсів); послуги з навігації в мережі (створення веб-порталів, що полегшують пошук і доступ до інформаційних ресурсів мережі). Друга група суб'єктів створює електронні інформаційні ресурси, володіє правами на них, забезпечує функціонування цих ресурсів і задовольняє інформаційні потреби користувачів. До третьої групи суб'єктів належать Інтернет-магазини, Інтернет-казино, Інтернет-аукціони тощо. До четвертої групи суб'єктів належать фізичні та юридичні особи, які потребують, замовляють, отримують телекомунікаційні послуги для власних інформаційних потреб [7, с 40].

В Інтернеті не принципово, чи є користувач мережі фізичною або юридичною особою або чи зареєстрований оператор мережевих послуг в якості платника податків. Причому це стосується не тільки таких суб'єктів правовідносин, як фізичні та юридичні особи. Як суб'єкти правовідносин можуть виступати і органи державної влади, а також органи місцевого самоврядування. Оскільки доступ в Інтернет в даний час є анонімним, то в ряді випадків визначення приналежності суб'єкта до традиційних в реальному фізичному світі видається складним [10, с. 17].

Розміщення в мережі Інтернет інформації, доступ до цієї інформації, а також «внутрішньо-мережевий» обмін інформацією здійснюється за участю спеціалізованих організацій – постачальників послуг Інтернет (послуг). При цьому сам «Інтернет» як сукупність інформаційних ресурсів непідконтрольний якійсь конкретній особі держави або міжнародній організації. По-перше, кожен провайдер має

можливість контролювати інформацію, яка передається в мережу або виходить з мережі при користуванні його послугами. У цьому сенсі кожен провайдер має потенційну можливість встановлювати певні стандарти користування мережею для своїх клієнтів [24, с. 80]. По-друге, держава має можливість регулювати і контролювати діяльність провайдерів, що надають послуги на його території, за допомогою різних юридичних інститутів. По-третє, режим інформаційного обміну з використанням мережі Інтернет може бути предметом міжнародно-правового регулювання.

Отже, будь-які відносини, що виникають у зв'язку з використанням мережі Інтернет, можуть бути предметом правового регулювання, причому як на внутрішньодержавному, так і на міжнародному рівні. Водночас такі відносини безумовно мають свою специфіку, яка вимагає певної адаптації юридичних інститутів. Технічне розміщення інформації в мережі Інтернет і отримання інформації з мережі можуть здійснюватися на анонімній основі. При цьому анонімно може діяти конкретний користувач мережі (тобто клієнта провайдера, який розмістив або отримав певну інформацію, визначити неможливо), проте в мережі Інтернет можна встановити факт поширення інформації певним постачальником або отримання інформації за допомогою послуг певного провайдера [15].

Об'єктами правовідносин у мережі Інтернет є: 1) телекомунікаційні мережі та інше технічне обладнання; 2) комп'ютерне програмне забезпечення; 3) інформація, інформаційні ресурси, інформаційні продукти, інформаційні послуги; 4) доменні імена; 5) права та свободи в сфері інформації; 6) інформаційна безпека.

При всьому різноманітті об'єктів відносин в Інтернеті потрібно зазначити, що *основним об'єктом відносин, що складаються в мережі, є інформація* (технічна, економічна, соціальна, юридична та ін.). Сьогодні інформація стирає грані між продуктом і послугою, що знаходить своє втілення в сучасних технологіях, які об'єднують інформаційні продукти і послуги в єдине ціле.

Правові норми, що регулюють діяльність у мережі Інтернет мають змішаний приватно-публічний характер, тобто

з одного боку у мережі превалює приватна ініціатива та договірне регулювання (а також саморегулювання) її учасників, а тому певна частина норм права щодо мережі Інтернет має диспозитивний характер, водночас, з іншого боку у електронно-цифровому середовищі мережі Інтернет також діють імперативні норми права, які характеризуються детальністю регламентації правил поведінки суб'єктів права. Це свідчить про складний характер правового регулювання відносин у цій сфері, що поєднує диспозитивні та імперативні засади.

Отже, під правовідносинами в Інтернеті також часто розуміють громадські зв'язки, що утворюються на основі використання мережі Інтернет та інших інформаційно-комунікаційних технологій (наприклад, програмного забезпечення) між постачальниками послуг з доступу в Інтернет, постачальниками інформації та користувачами, які утворюються на засадах взаємного визнання даними суб'єктами волі та формальної рівності.

Крім того, правовідносини в мережі Інтернет можуть бути класифіковані на такі види: загальні; організаційні (управлінські); інформаційні; предметні.

До загальних правовідносин в Інтернеті відносяться ті правовідносини, які здійснюються за допомогою (при використанні) ресурсів (служб) мережі Інтернет, які «протиставляються» правовідносинам, місцем вчинення яких є реальна дійсність, а не кіберпростір. Так, В.Б. Наумов, досліджуючи питання про правове регулювання Інтернету, відзначає ряд загальнотеоретичних і спеціальних проблем. До загальнотеоретичних проблем він відносить такі: юрисдикція мережі (або проблеми компетенції, екстериторіальності в Інтернеті); правосуб'єктність осіб, що представляють, розповсюджують і споживають інформацію в мережі Інтернет (або визначення правосуб'єктності всіх учасників правовідносин в Інтернеті); визначення часу і місця дії в мережі Інтернет [17].

До організаційних (управлінських) правовідносин в Інтернеті відносяться такі відносини, які спрямовані на взаємодію або протидію між учасниками соціальних відносин в Інтернеті, об'єктом яких є соціальна чи технічна природа (інфраструктура) Інтернету. До організаційних відносин можна

віднести відносини з делегування доменних імен, міжнародної стандартизації електронного документообігу і т. ін. *Інформаційні правовідносини* в Інтернеті є відносини, що регулюються відповідними нормами права, в галузі виробництва, перетворення і споживання інформації [9, с. 54]. *До предметних правовідносин* можна віднести ті, які регулюються окремими (спеціальними) нормами права. У даний перелік входять відносини, що регулюються нормами конституційного права, цивільного права, адміністративного права; відносини, що регулюються нормами законодавства про засоби масової інформації, і т. ін.

Необхідно зазначити, що серед фахівців (насамперед в технічній сфері) існує вкрай негативне ставлення до самої ідеї правового регулювання відносин, що виникають в Інтернет – середовищі. У мережі навіть була поширена «Декларація незалежності кіберпростору» (автор – Джон Барлоу) [27], в якій проголошувалося право на свободу Інтернет – простору та принцип невтручання держав у регулювання Інтернет – відносин.

Пріоритетними методами та способами правового регулювання суспільних відносин, що виникають з приводу використання всесвітньої комп'ютерної мережі Інтернет, є публічно-правовий та приватно-правовий методи (метод юридичної рівності сторін), позитивне зобов'язання та дозвіл, оскільки вони є засобами юридичного стимулювання поведінки учасників згаданих суспільних відносин [8, с. 125].

Правовідносини у віртуальному середовищі виступають юридичною формою взаємодії користувачів мережі Інтернет з приводу обміну різноманітною інформацією, мають вольовий характер та у сукупності складаються з комплексу абсолютних і відносних, регулятивних і охоронних правовідносин. Потрібно зауважити, що багато вчених, відносини у мережі Інтернет називають інформаційними відносинами, а це дає змогу зробити висновок, що відносини у мережі Інтернет є різновидом інформаційних відносин. Головною особливістю цих правовідносин є те, що суб'єктивні права в них, в першу чергу, розкриваються через власні дії користувачів мережі Інтернет, які спричиняють виникнення, припинення або зміну прав та

обов'язків інших учасників мережі Інтернет, а не тільки через обов'язки третіх осіб (інформаційних провайдерів та власників Інтернет-сайтів).

Список літератури

1. Акопов Г.Л. Информационное право / Г.Л. Акопов. – М.: Феникс, 2008. – 348с.
2. Андреев Б.В. Право и Интернет / Б.В. Андреев, Е.А. Вагонова. – М., 2001. – 48с.
3. Бабкин С.А. Право, применяемое к отношениям, возникающим при использовании сети Интернет / С.А. Бабкин. – М.: ЮрИнфоР, 2003. – 69с.
4. Бачило И.Л. Информационное право / И.Л. Бачило. – М.: Юрайт, 2009. – 454с.
5. Голоскоков Л.В. Теория сетевого права / Л.В. Голоскоков. – М.: МПСУ, 2012. – 216с.
6. Городов О.А. Информационное право / О.А. Городов. – М.: Проспект, 2009. – 256с.
7. Дашян М.С. Право информационных магистралей / М.С. Дашян. – М.: Волтерс Клувер, 2007. – 288с.
8. Жилінкова І. Правове регулювання Інтернет – відносин / І. Жилінкова // Право України. – 2003 – № 5. – С. 124-128.
9. Загурський Я.М. Регулювання і саморегулювання мережі Інтернет / Я.М. Загурський // Інформаційне суспільство. – 2000. – № 4. – С. 54-59.
10. Интернет – технологии в экономике знаний / Под ред. Н.М. Абдикеева. – М.: Инфра-М, 2010. – 448с.
11. Калятин В.О. Право в сфере Интернета / В.О. Калятин. – М.: Норма, 2004. – 480с.
12. Ковалева Н.Н. Информационное право / Н.Н. Ковалева. – М.: Дашков и К, 2009. – 352с.
13. Леанович Е. Проблемы правового регулирования Интернет-отношений [Електронний ресурс] // http://www.russianlaw.net/law/doc/al02.htm
14. Малахов С.В. К проблеме содержания понятия Интернет в юридической науке [Електронний ресурс] // http://www.conf3.parkmedia.ru/any_r.asp?URL=mala.asp
15. Мелюхин И. Интернет и правовое регулирование [Електронний ресурс] // http://www.medialaw.ru/publications/zip/28/melukhin_2.html
16. Наумов В.Б. Право и Интернет: очерки теории и практики / В.Б. Наумов. – М., 2002. – 432с.
17. Наумов В.Б. Особенности правового регулирования сети Интернет / В.Б. Наумов // http://www.russianlaw.net/law/doc/a08.htm
18. Попов Л.Л. Информационное право / Л.Л. Попов, Ю.И. Мигачев, С.В. Тихомиров. – М.: Норма, 2010. – 496с.
19. Правовое обеспечение информационной безопасности / Под ред. С.Я. Казанцева. – М.: Академия, 2005. – 240с.
20. Рассолов И.М. Интернет – право / И.М. Рассолов. – М.: Юнити, 2004. – 143с.

21. Рассолов И.М. Информационное право / И.М. Рассолов. – М.: Юрайт, 2012. – 444с.
22. Синеокий О.В. Основы информационного права и законодательства в области высоких технологий и ИТ – инноваций / О.В. Синеокий. – Х.: Право, 2011. – 592с.
23. Серго А.Г. Интернет и право / А.Г. Серго. – М., 2003. – 272с.
24. Харчук В. Запровадження правового регулювання відносин у глобальній мережі Інтернет / В. Харчук // Юридичний журнал. – 2010.– № 12. – С. 80-82.
25. Черкес М.Е. Правовое регулирование деятельности в Интернете / М.Е. Черкес. – О.: Латстар, 2002. – 88с.
26. Якушев М.А. Интернет и право / М.А. Якушев. – М., 2002. – 45с.
27. John Perry Barlow A Declaration of the Independence of Cyberspace [Електронний ресурс] // https://projects.eff.org/~barlow/Declaration-Final.html

Зеров К.О. –
аспірант кафедри інтелектуальної власності юридичного факультету Київського національного університету ім. Т. Шевченка, молодший науковий співробітник Науково-дослідного інституту інтелектуальної власності Національної академії правових наук України

ОСОБЛИВОСТІ ВІДПОВІДАЛЬНОСТІ ІНТЕРНЕТ-ПОСЕРЕДНИКІВ ЗА ПОРУШЕННЯ АВТОРСЬКИХ ПРАВ НА ТВОРИ, РОЗМІЩЕНІ В МЕРЕЖІ ІНТЕРНЕТ

При розгляді питання захисту авторських прав на твори, розміщені в мережі Інтернет, вбачається неможливим недооцінити роль інтернет-посередників[2] – суб'єктів, чиїми послугами користуються кінцеві користувачі (одержувачі послуг) мережі Інтернет при здійсненні своєї діяльності, оскільки:

[2] Враховуючи відсутність єдиного визначення зазначеної категорії суб'єктів в світовій практиці (intermediary service providers (ISP) в країнах ЄС, service provider в США, інформаційний посередник в РФ тощо), в цілях цього Дослідження ми будемо використовувати термін "інтернет-посередник", який ототожнюємо з "постачальником посередницьких послуг" відповідно до ст.244 Угоди про асоціацію між Україною, з однієї сторони, та Європейським союзом і його державами- членами, з іншої сторони (надалі за текстом - Угода) [2].

1) Надаючи свої послуги інтернет-посередники здійснюють зберігання, обробку та передачу інформації (в тому числі – об'єктів авторського права у цифровій формі), що створюється, модифікується і отримується користувачами мережі Інтернет, та взагалі - доступ кінцевих користувачів до мережі Інтернет без їх участі є неможливим.

2) Звісно, за певних умов окремі дії як користувачів, так і самих інтернет-посередників можуть порушувати авторські права. Тобто, інтернет-посередник може бути суб'єктом як прямого, так і непрямого порушення авторських прав. Наприклад, пряме порушення авторського права, на думку Seagull Haiyan Song, буде у випадку розміщення твору контент-провайдером на власному сервері через мережу Інтернет без дозволу правоволодільця.[1, с. 7]. Українській судовій практиці вже відомі випадки притягнення до відповідальності інтернет-посередників (а саме – провайдерів доступу) за пряме порушення *суміжних* прав[3].

[3] Так, у постанові по справі № 910/28372/14 від 17.05.2016 р. Київський апеляційний господарський суд зазначив, що Товариство (відповідач -1) здійснює ретрансляцію передач/програм, що транслюються позивачем на телеканалах "ФУТБОЛ 1" та "ФУТБОЛ 2" для абонентів, що користуються послугами зв'язку (інтернетом), наданих ФОП ОСОБА_4 (відповідач -2). Товариство та ФОП ОСОБА_4 здійснюють свою діяльність під логотипом "ІНФОРМАЦІЯ_1", використовують один сайт ІНФОРМАЦІЯ_2 та надають однакові послуги з підключенням користувачів до мережі Інтернет з одночасним наданням можливості перегляду телевізійних каналів […]. Відмовляючи в задоволенні таких вимог, судом першої інстанції в змісті мотивувальної частини оскарженого рішення було зазначено, що вимоги до цих осіб ґрунтуються на тому, що перегляд ретрансляцій програм, здійснених ТОВ "Корбіна Телеком", стало можливим завдяки використанню отриманого обладнання - IPTV приставки, наданої ФОП ОСОБА_5, маючи доступ до мережі Інтернет, наданий ФОП ОСОБА_4, проте, останні як при наданні доступу до мережі Інтернет, так і при продажу приставки IPTV не порушували будь-яких прав позивача у справі, а лише здійснювали власну господарську діяльність, яка не заборонена законом.

Однак, ретрансляція сигналу здійснювалась виключно з IP адрес НОМЕР_1 та НОМЕР_2, які належать відповідачу-1, які, в свою чергу, у вказаній мережі Інтернет *не перебувають в загальному доступі* і отримання сигналу ретрансляції передбачає використання відповідного технічного обладнання, продаж якого (з використанням логотипів "ІНФОРМАЦІЯ_3", ІНФОРМАЦІЯ_2 і т.ін.), разом з пакетом послуг доступу вказаного

3) На інтернет-посередників не покладається обов'язків відслідковувати, контролювати (відносини з «активного моніторингу») своїх користувачів.

4) Як справедливо зазначає *Н. І. Федоскіна*, роль інтернет-посередників в механізмі захисту авторських і суміжних прав визначається ще й можливістю присікти незаконну діяльність в мережі шляхом відмови в доступі користувачам – порушникам [3, с.39].

При підготовці цієї публікації враховані підходи, висловлені українськими та російськими вченими Н.І. Федоскіною, О. Мацкевич, М.А. Хатаєвовю, А.К. Жаровою та О. М. Ліпкесом, а також останні правові позиції Європейського суду справедливості (англ. Court of Justice of the European Union, CJEU) (надалі за текстом – ЄСС).

Метою дослідження у цій публікації є класифікація інтернет-посередників та встановлення випадків звільнення них від відповідальності за порушення авторських прав на твори, розміщені в мережі Інтернет.

В літературі розрізняють такі види інтернет-посередників:

1) провайдер доступу / просто посередник (англ. «Mere conduit») – забезпечує доступ до мережі, в тому числі підключення до мережі Інтернет кінцевих користувачів.

обладнання до мережі Інтернету, зокрема, здійснювали відповідач-2 та відповідач-3. […]За таких обставин, вбачається обґрунтованим висновок, що відповідач-2 разом з відповідачем-3 безпосередньо і пов'язані із вчиненим порушенням суміжних прав позивача. Створення можливості вчинення порушення (авторських) суміжних прав, безпосередньої загрози порушення прав позивача, яке згідно з ч. 1 ст. 52 Закону України «Про авторське право і суміжні права» позивач в праві вимагати припинити, та саме по собі порушення вказаних прав, згідно з наведеними вище нормами Закону є підставою судового захисту порушених прав позивача шляхом застосовування компенсаційних заходів, з урахуванням загальних засад цивільного законодавства (справедливості, добросовісності, розумності і т.ін.). Враховуючи викладене вище, колегія суддів суду апеляційної інстанції вбачає позовні вимоги ТОВ "Телерадіокомпанія "Україна" про стягнення з ФОП ОСОБА_4, ФОП ОСОБА_5 компенсації за порушення суміжних прав […] обґрунтованими, підтвердженими наявними в матеріалах справи доказами та не спростованими належним чином та у встановленому законом порядку, а відтак такими, що підлягають задоволенню[4].

2) хостинг-провайдер (англ. – «Hosting») – надає інформаційні ресурси, що належать третій особі та забезпечує їх доступність. Особливим різновидом хостинг – провайдеру є контент-провайдер (постачальник контенту), який надає послуги щодо зберігання інформації, яка надається одержувачем послуги, в тому числі об'єктів авторського права та суміжних прав та забезпечує їх доступність. Окремі науковці, зокрема О. Мацкевич, М.А. Хатаєва відносять контент-провайдера до самостійного виду інтернет-посередників [5, с.54; 6, с.105];

3) Кеш-провайдер (англ. – «Caching») – провайдер, що забезпечує автоматичне проміжне тимчасове зберіганні матеріалу в системі чи Інтернеті, що контролюється чи керується провайдером;

Доцільно також погодитись з А.К. Жаровою та О.М. Ліпкесом, які вважають, що посередник, який виконує декілька функцій, може відноситись до декількох категорій (наприклад, якщо він забезпечує доступ до даних в Інтернеті і в той же час пропонує свій зміст з власного серверу)[7, с.62; 8, с.98].

Вбачається, що діяльність кожного із вказаних видів інтернет-посередників потребує спеціального правового регулювання, в т.ч. і спеціальних умов настання юридичної відповідальності, оскільки одні і ті ж самі правовідносини можуть породжувати для різних інтернет-посередників різні правові наслідки.

В іноземній практиці існує декілька підходів до питання відповідальності інтернет-посередників.

Згідно законодавства країн Близького Сходу, інтернет – провайдер несе відповідальність за всі дії користувачів, не залежності від наявності у нього відомостей про скоєні дії [6, с. 107].

Особливості обмеження відповідальності (англ. «limitations on liability relating to material online», які ще прийнято називати «safe harbor») інтернет-посередників містить закон США H.R.2281 Digital Millennium Copyright Act (надалі за текстом – DMCA), а саме – в §512 розділу 202 DMCA.

Так, імунітет інтернет-посередника можливий у таких випадках:

(a) коли інформація міститься в тимчасових цифрових повідомленнях, які передаються через систему або мережі провайдера;

(b) коли інформація збережена (кешована);

(c) коли інформація постійно зберігається в системах або мережах за вказівкою користувачів;

(d) коли інтернет-посередник використовує різні посилання або з'єднання, використовуючи інструментарій визначення місцезнаходження інформації, включаючи довідники, каталоги, посилання, покажчики, на інформаційні ресурси, що містять нелегальний контент або проводять незаконну діяльність[9].

При цьому для звільнення від відповідальності у випадку коли інформація постійно зберігається в системах або мережах за вказівкою користувачів, такий інтернет-посередник не повинен мати фактичного знання (а за його відсутності він не має бути обізнаний про обставини, з яких було б очевидним визначити незаконний матеріал або діяльність) про протиправний статус контенту; повинен зареєструвати DMCA-агента; повинен розробити, довести до відома клієнтів (передплатників) і розумно застосовувати правила розміщення контенту та недопущення подальших порушень; повинен протягом встановленого строку реагувати на скарги; не повинен отримувати фінансову вигоду, безпосередньо пов'язану з незаконною діяльністю, коли він має право і можливість контролювати таку діяльність; повинен дотримуватися і не перешкоджати стандартним технічним засобам, що їх використовують правоволодільці для ідентифікації та захисту охоронюваних творів[10].

Особливості відповідальності інтернет-посередників в країнах – членах Європейського Союзу визначені в ст.ст. 12-15 Директиви 2000/31/ЄС «Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку» («Директива про електронну комерцію») [11], які відображені в ст.ст. 245-247 Угоди [2]. Вбачається, що саме детальний аналіз європейського підходу до відповідальності інтернет-посередників є доцільним в контексті

гармонізації українського законодавства до законодавства європейського співтовариства.

Зауважимо, що в основі положень Директиви 2000/31/ЄС та Угоди покладений принцип обмеження відповідальності не певних видів інтернет-посередників, а відповідальності за здійснення певного роду діяльності. Положення цієї Директиви не гармонізують проблеми відповідальності чи визначення порушення, а лише випадки звільнення від відповідальності.

При цьому звільнення від відповідальності, що передбачені в Директиві 2000/31/ЄС та Угоді, поширюються лише на випадки, коли:

1) діяльність інтернет-посередників обмежена технічним процесом дії та наданням доступу до мережі передачі даних;

2) інформація, що стає доступною для третіх сторін, передається чи тимчасово зберігається з єдиною метою - зробити передачу більш ефективною;

3) ця діяльність має просту технічну, автоматичну та ***пасивну*** (виділено – К. Зеров) сутність, яка передбачає, що постачальник інформаційних послуг не має ні знань, ні може контролювати інформацію, що передається чи зберігається[11, п. 42; 2, ст. 244].

Отже, в Директиві 2000/31/ЄС та Угоді визначені наступні випадки звільнення від відповідальності інтернет-посередників:

1.Відповідальність постачальників посередницьких послуг: «Просто посередник» (ст. 12 Директиви 2000/31/ЄС; ст. 245 Угоди). Якщо надаються інформаційні послуги, які складаються з передачі інформації, що надається одержувачем послуг, всередині мережі зв'язку або надання доступу до мережі зв'язку, сторони гарантують, що постачальник послуг не несе відповідальності за інформацію, що передається, за умови, що постачальник: a) не ініціює передачу; b) не вибирає одержувача передачі; і c) не вибирає або модифікує інформацію, що міститься в передачі.

Необхідно відзначити, що згідно практики ЄСС (справа C-484/14) «просто посередником» може визнаватися в тому числі власник публічної Wi-Fi мережі. Зазначений суб’єкт за умови відповідності його діяльності положенням ст. 12 Директиви 2000/31/ЄС, не несе відповідальності за порушення авторських

прав, що скоєні користувачами, які під‘єднались до його мережі[12].

При цьому зазначені вище положення не впливають на можливість вимагати через суд або адміністративний орган від постачальника послуг припинити або попередити порушення авторських прав. Так, у Великобританії з прийняттям Digital Economy Act у 2010 р. (DEA), інтернет-посередник не повинен самостійно оцінювати правомірність дій своїх абонентів, але лише оперативно реагувати на претензії правоволоділців і виконувати приписи закону [13]. За невиконання ж означених приписів до інтернет-посередника можуть бути застосовані фінансові санкції. Рішенням цивільної палати Апеляційного Суду Англії та Уєльсу 03 червня 2012 року у справі BT Plc and TalkTalk Telecom Group Plc проти Secretary of State for Culture, Olympics, Media and Sport та інших ([2012] EWCA Civ 232) встановив, що DEA не суперечить ст. 12 Директиви 2000/31/ЄС, яка забороняє покладати на інтернет-посередників доступу відповідальність за передані користувачами дані, оскільки вона дозволяє вимагати від посередників прийнятті заходів щодо припинення або запобігання порушень авторських прав. А фінансові санкції можуть бути накладені на посередників не за вчинення ними порушень авторських прав, а за невиконання основних зобов'язань за Кодексом провайдера або технічних зобов'язань, встановлених Управлінням зв’язку Великобританії [14, 47-60].

2.Відповідальність постачальників посередницьких послуг: «Хостинг» (англ. – «Hosting») (ст. 14 Директиви 2000/31/ЄС; ст. 247 Угоди). Так, умовами звільнення від відповідальності інтернет-посередника хостингу передбачені випадки, коли:

a) йому фактично не відомо про незаконну діяльність або інформацію і, стосовно позову про відшкодування збитків, і не відомо про факти або обставини, з яких випливає незаконна діяльність або інформація; або

b) він, після одержання таких відомостей, діє оперативно, щоб зняти або зробити неможливим доступ до інформації.

Значення вказаного виду обмеження від відповідальності набирає все більшої актуальності через розміщення на веб-сайтах користувацького (англ. - user-generated) контенту.

Принагідним є той факт, що діяльність контент-провайдерів здебільшого не може підпадати під обмеження відповідальності провайдерів хостингу, що визначені в Угоді та Директиві 2000/31/ЄС. Згідно рішення ЄСС по справі С- 324/09 від 12 липня 2011 р. Статтю 14 (1) Директиви 2000/31 / ЄС слід тлумачити як таку, яку можна застосовувати до посередника, де цей посередник **не відігравав активної ролі**, що дозволяє йому мати знання або контроль над даними, що зберігаються. Посередник грає таку роль, коли він надає допомогу, яка тягне за собою, зокрема, оптимізацію подання *[кінцевим користувачам –прим К.З.]* пропозицій про продаж або їх просування. Навіть коли інтернет-посередник не відіграє такої активної ролі і, відповідно, послуга, що надається, підпадає під дію пункту 1 статті 14 Директиви 2000/31/ЄС, він все-таки не зможе – у ситуації, що погрожує винесенням рішення про відшкодування збитків – послатися на виняток з відповідальності, передбачений цією статтею, якщо, незважаючи на те, що йому були відомі факти чи обставини, на підставі яких добросовісний суб'єкт господарської діяльності повинен був би зрозуміти, що відповідні пропозиції є незаконними, він не вжив негайних заходів відповідно до підпункту «b» пункту 1 статті 14 Директиви 2000/31/ЄС. (наприклад внаслідок власного розслідування чи повідомлень, в яких міститься досить точна і адекватно обґрунтована інформація про порушення авторських прав)[15].

Контент-провайдер, який надає послуги по зберіганні інформації, яка надається одержувачем послуги, здебільшого відіграє саме активну роль, яка може виражатись, на думку автора, зокрема у наступному: персоналізації виводу інформації на основі дії кінцевих користувачів щодо перегляду веб-сайту; організації та категоризації об'єктів, що розміщені на його веб-сайті; контент – провайдер займається інтенсивною рекламною діяльності шляхом розміщення рекламних банерів різних типів та форматів, вивід яких залежить від поведінки кінцевих користувачів веб-сайту; зміст реклами змінюється в залежності

від географічного розташування чи дій кінцевого користувача; контент-провайдер за замовчуванням пропонує обмежений перегляд об'єктів, що розміщені на його веб-сайті, однак, якщо кінцевий користувач придбає оплатну підписку, то отримає необмежений доступ тощо.

3.Відповідальність постачальників посередницьких послуг: «Кешування» (ст. 13 Директиви 2000/31/ЄС; ст.246 Угоди)**.** Особливості звільнення від відповідальності інтернет-посередників за кешування, на думку автора, необхідно розглядати через призму діяльності пошукових сервісів. (сервісів інтернет-агрегаторів)**.** Таку діяльність необхідно розглядати в трьох площинах:

1) розміщення результатів рекламних оголошень у вигляді гіперпосилань, шо можуть містити у своїй структурі (а саме - описовій (інформаційній) частині гіперпосилання) твори – через умови звільнення відповідальності за хостинг[4];

2) розміщення результатів пошуку у вигляді гіперпосилань, шо можуть містити у своїй структурі (а саме - описовій (інформаційній) частині гіперпосилання) твори – відповідно до положень національних законодавств щодо захисту прав видавництв (т. зв. «податок на Google»)[5];

[4] Так, згідно рішення ЄСС по справі C-236/08 Google France SARL and Google Inc. V Louis Vuitton Malletier SA and Others умови звільнення від відповідальності, передбачені ст. 14 Директиви 2000/31/ЄС розповсюджуються на інтернет-посередника з розміщення посилань за умови, якщо він не грав активної ролі, яка б надавала б йому знання або контроль над даними, що зберігаються у нього. За такої умови на нього не може бути покладена відповідальність за дані, зберігання яких він забезпечував на запит рекламодавця, за виключенням випадків, коли він отримав знання про протизаконний характер цих даних чи діяльності цього рекламодавця та невідкладно не видалив такі дані чи не обмежив до них доступ [16].

[5] Наприклад в Німеччині 22 березня 2013 р. були прийняті зміни до закону "Про авторське право" (нім. - *Urheberrechtsgesetz*), ст.ст. 87F, 87G і 87H якого передбачають виключне право видавництв на комерційне використання їхнього контенту протягом одного року від дня публікації, тим самим обмежуючі пошукові системи від безоплатного показу уривків у гіперпосиланнях з газетних статей. Однак оплата не передбачається за відображення окремих слів або короткі текстові фрагменти. Тим не менш, в законі не зазначається необхідна кількість символів для безоплатного використання [17].

3) індексація та кешування[6] змісту веб-сайтів та інших об'єктів. авторського права (зокрема, літературних творів) як акт відтворення.

Станом на листопад 2016 р. законодавство України не містить положень щодо обмежень майнових прав правоволоділців стосовно кешування/тимчасових копій творів, а відтак – діяльність пошукових сервісів щодо створення кешованих копій веб-сторінок можна кваліфікувати як використання творів способом їх відтворення без відповідних правових підстав.

В країнах Європейського Союзу згідно положень ст. 13 Директиви 2000/31/ЄС інтернет-посередник з кешування звільняється від відповідальності за порушення авторських прав за сукупності певних умов, а саме якщо:

1) кешування є автоматичним, проміжним і тимчасовим;

2) здійснюється з єдиною метою – зробити більш ефективною наступну передачу інформації;

3) постачальник не модифікує інформацію;

4) постачальник виконує умови доступу до інформації;

5) постачальник виконує правила, що стосуються оновлення інформації, які визначені способом, що широко визнаний і використовується в промисловості;

6) постачальник не перешкоджає законному використанню технологій, які широко визнаються і використовуються в промисловості, щоб одержати дані стосовно використання інформації;

7) постачальник вдається до швидких дій з метою усунення можливості доступу чи відключення доступу до інформації, яку він зберігав, після того як він узнає, що інформація на початковій стадії передання була видалена з мережі або доступ до неї був відключений, чи суд або адміністративний орган наказав здійснити таке усунення чи відключення [11].

[6] Кешування підвищує продуктивність мережі Інтернет, що дозволяє пошуковим системам можливість швидкого отримання кешованної копії на своєму сервері замість того, щоб постійно отримувати таку копію з віддалених серверів. Кешування також корисне коли веб-сторінка недоступна через проблеми інтернет-трафіку або перевантаження веб-сайту[18].

Проаналізувавши досвід в інших іноземних юрисдикціях щодо кваліфікації дій з індексації та кешування творів сервісами-пошуковими інтернет – агрегаторами, зокрема в США, то слід зауважити, що такі дії визнаються судами правомірними згідно доктрини добросовісного використання (англ. – *fair use*) (Наприклад, справа Blake A. Field VS. Google Inc.) [19].

Наголосимо також, що згідно ст. 278 Угоди (в основі якої відображено зміст ст. 15 Директиви 2000/31/ЄС) Україна не повинна покладати на інтернет-посередників (в тому числі і контент-провайдерів як «активних» хостинг-провайдерів) ні загального зобов'язання при наданні послуг здійснювати моніторинг інформації, яку вони передають або зберігають, ні загального зобов'язання активно шукати факти або обставини, які вказують на незаконну діяльність. Зазначений обов'язок підтверджується також на рівні європейської судової практики[7]. Однак це не стосується зобов'язань по відслідковуванню в особливому випадку та, зокрема, не впливає на розпорядження, які можуть бути видані національними органами влади відповідно до законодавства.

Згідно положень ст. 246 Угоди [2] положення щодо відповідальності постачальників посередницьких послуг мають бути імплементовані до українського законодавства впродовж 18 місяців з дати набрання чинності Угоди.

Відповідно до чинного законодавства України, а саме положень ч. 4 ст. 40 Закону України «Про телекомунікації» «оператори, провайдери телекомунікацій не несуть відповідальності за зміст інформації, що передається їх мережами»[22, 40], а згідно норм законопроекту №3081-Д «Про

[7] Наприклад в судових справах С-70/10 та С‑360/10 ЄСС встановив, що судове рішення, що зобов'язує інтернет посередника запровадити фільтраційну систему, зобов'яже такого постачальника здійснювати активний моніторинг усіх даних кожного із своїх клієнтів із метою уникнення будь-якого майбутнього порушення прав інтелектуальної власності. Відповідно, таке судове рішення зобов'яже цього постачальника послуг із зберігання даних здійснювати загальний моніторинг, заборонений положеннями частини 1 статті 15 Директиви 2000/31 ЄС [20, п.40; 21, 38].

державну підтримку кінематографії в Україні» [23] до Закону України «Про електронну комерцію» вносяться положення щодо звільнення від відповідальності провайдерів доступу та хостингу, які в цілому відповідають положенням Угоди.

Вважаємо за необхідне також наголосити, що обмеження відповідальності інтернет-посередників не впливають на можливість застосування щодо них тих способів захисту, які не пов'язані з відповідальністю. Так, відповідно до положень ст.ст. 12-14 Директиви 2000/31/ЄС (та, відповідно, ст. ст. 245-247 Угоди) випадки обмеження відповідальності постачальників посередницьких не впливають на можливість для судового або адміністративного органу, відповідно до правових систем Сторін, вимагати від постачальник послуг припинити або *попередити* порушення[2] (*тобто застосування заходів захисту – К.З.).*

Згідно положень ч.3. ст. 8 Директиви 2001/29/ЄС[24] та ст. 11 Директиви 2004/48/ ЄС [25] правоволодільці мають право подати заяву про **судову заборону** (англ. injunction) проти посередників, чиї послуги використовуються третьою стороною з метою порушення права інтелектуальної власності. Така заборона не залежить від характеру поведінки посередника (дія чи бездіяльність). Зазначена норма знайшла своє відображенні і в ст. 238 Угоди [2, 238]. Наприклад такою забороною може бути веб-блокування, яке хоча прямо і не зазначається в тексті вказаних директив та Угоди, але розглядається і застосовується в судовій практиці країн-членів ЄС саме в якості судової заборони. Втім, питання застосування веб-блокування як способу захисту авторських прав потребує окремого ґрунтовного дослідження.

Отже, в контексті гармонізації українського законодавства до законодавства європейського співтовариства обмеження відповідальності інтернет-посередників доцільно розглядати через здійснення ними певного роду діяльності: просто посередник, хостинг, кешування. При цьому такі обмеження можуть бути застосовані виключно у випадках коли 1) діяльність інтернет-посередників обмежена технічним процесом дії та наданням доступу до мережі передачі даних; 2) інформація, що стає доступною для третіх сторін, передається

чи тимчасово зберігається з єдиною метою - зробити передачу більш ефективною; 3) ця діяльність має просту технічну, автоматичну та пасивну сутність, яка передбачає, що постачальник інформаційних послуг не має ні знань, ні може контролювати інформацію, що передається чи зберігається. Крім того, такі обмеження не повинні впливати на можливість застосування щодо них тих способів захисту, які не пов'язані з відповідальністю.

Список літератури

1. Song S. A Comparative Copyright Analysis of ISP Liability in China Versus the United States and Europe / Seagull Haiyan Song. // The Computer & Internet Lawyer. – 2010. – №7. – P. 7–24.

2. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [Електронний ресурс] – Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/show/984_011.

3. Федоскина Н. И. Условия гражданско-правовой ответственности интернет- провайдеров за нарушение авторских и смежных прав [Электронный ресурс] / Н. И. Федоскина – Режим доступа: http://www.center-bereg.ru/h1624.html .

4. Рішення Київського апеляційного господарського суду від 17 травня 2016 р. по справі № 910/28372/14 [Електронний ресурс] – Режим доступу до ресурсу: http://reyestr.court.gov.ua/Review/57788681.

5. Мацкевич О. Загальні підходи до визначення юридичної відповідальності провайдерів за порушення авторських і суміжних прав у мережі Інтернет / О. Мацкевич. // Теорія і практика інтелектуальної власності. – 2012. – №1. – С. 54–62.

6. Хатаева М. А. Дифференциация ответственности интернет-провайдеров за нарушение интеллектуальных прав на результаты интеллектуальной деятельности в интернете / М. А. Хатаева. // Журнал зарубежного законодательства и сравнительного правоведения. – 2010. – №1. – С. 103–111.

7. Жарова А. К. О необходимости правовой классификации операторов сети интернет / А. К. Жарова. // Бизнес-Информатика. – 2011. – №3. – С. 60–65.

8. Липкес А. М. Правовые вопросы использования авторских произведений в Интернете : дис. канд. юр. наук : 12.00.03 / Липкес Александр Михайлович – М., 2006. – 146 с.

9. https://www.gpo.gov/fdsys/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf

10. Как работает DMCA? Удаление контента по требованию правообладателя, и его восстановление. [Электронный ресурс] – Режим доступа: http://lexdigital.ru/2013/078/ .

11. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [Electronic resource]. – Access mode: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32000L0031.

12. Court of Justice of the European Union. Press Release № 99/16. Judgment in Case C-484/14. Tobias Mc Fadden v Sony Music Entertainment Germany GmbH [Electronic resource]. – Access mode: http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-09/cp160099en.pdf .

13. Калятин В. О. О некоторых тенденциях развития законодательства об ответственности интернет-провайдеров [Электронный ресурс] / В. О. Калятин – Режим доступа: http://www.center-bereg.ru/b3284.html .

14. BT Plc and TalkTalk Telecom Group Plc -v- Secretary of State for Culture, Olympics, Media and Sport and others. In The Court of Appeal (Civil Division) on appeal from the High Court of Justice (Queen's Bench Division) Administrative Court. Neutral Citation Number: [2012] EWCA Civ 232 [Electronic resource]. – Access mode: https://www.judiciary.gov.uk/wp-content/uploads/JCO/Documents/Judgments/r-bt-and-talktalk-v-ss-for-culture-and-others.pdf .

15. Judgment of the European Court of Justice (Grand Chamber) of 12 July 2011.L'Oréal SA and Others v eBay International AG and Others (C-324/09) [Electronic resource]. – Access mode: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0324 .

16. Judgment of the European Court of Justice (Grand Chamber) of 23 March 2010. Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08). [Electronic resource]. – Access mode: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62008CJ0236.

17. Rosati E. The German 'Google Tax' law: groovy or greedy? Electronic resource] / Eleonora Rosati – Access mode: http://jiplp.blogspot.co.uk/2013/06/the-german-google-tax-law-groovy-or.html .

18. What is proxy cache? A Webopedia Definition [Electronic resource]. – Access mode: http://www.webopedia.com/TERM/P/proxy_cache.html .

19. Field v. Google, Inc. - Stanford Copyright and Fair Use. Docket Number: 2:2004cv00413 [Electronic resource]. – Access mode: http://fairuse.stanford.edu/case/field-v-google-inc/ .

20. Judgment of the European Court of Justice (Third Chamber) of 24 November 2011. Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). Reference for a preliminary ruling: Cour d\'appel de Bruxelles - Belgium. Case C-70/10. [Electronic resource]. – Access mode: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0070 .

21. Judgment of the European Court of Justice (Third Chamber) of 16 February 2012. Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV. Reference for a preliminary ruling: Rechtbank van

eerste aanleg te Brussel - Belgium. Case C-360/10. [Electronic resource]. – Access mode: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0360

22. «Про телекомунікації», Закон України від 18.11.2003 № 1280-IV // Відомості Верховної Ради України (ВВР), 2004, N 12, ст.155 (зі змінами).

23. «Про державну підтримку кінематографії в Україні», проект закону №3081-д від 27.11.2015 [Електронний ресурс] – Режим доступу до ресурсу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=57258 .

24. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 On the harmonisation of certain aspects of copyright and related rights in the information society [Electronic resource]. – Access mode: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:EN:PDF .

25. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [Electronic resource]. – Access mode: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:195:0016:0025:EN:PDF .

Карпенко О.І. –
старший викладач кафедри цивільно-правових дисциплін
Харківський національний університет ім. В.Н. Каразіна,
кандидат юридичних наук

ЩО ТАКЕ І ЯК ПРАЦЮЄ ПЛАТФОРМА ODR ЄВРОПЕЙСЬКОГО СОЮЗУ?

Врегулювання суперечок в мережі Інтернет зараз є дуже актуальною темою. Це пов’язано з розвитком і необхідністю регулювання специфічних суспільних відносин в інформаційному суспільстві. Для вирішення спорів саме в галузі електронної комерції, необхідні фахівці, знання та інструменти саме з цієї галузі. Чи не кожен суддя має знання і навички IT технологій і тому судовий розгляд може перетворитися на суцільну експертизу. Отже, сторони цих суперечок і почали все частіше звертатися безпосередньо до експертів з вирішення суперечок в даній галузі [11, с. 241].

Для початку необхідно прояснити ситуацію з терміном «онлайн» врегулювання суперечок. Фахівці в області IT під терміном онлайн (online) розуміють безпосереднє «живе» спілкування. Більш широко під цим терміном розуміється розгляд спору в мережі Інтернет в електронній формі [11, с. 241-242].

Поняття альтернативного вирішення спорів (Alternative Dispute Resolution, далі – ADR) незнайоме вітчизняній правовій системі, адже навіть перелік позасудових способів розгляду і вирішення спорів обмежений (третейські суди, засоби досудового врегулювання і т.п.). Тому, можуть бути запозичені ті правові концепції, які вже розроблені і діють в інших країнах.

Спочатку положення про застосування ADR для вирішення цивільних і торговельних суперечок були врегульовані в Європейському Союзі (далі – ЄС) на рівні так званого «м'якого права»: в зелених книгах і рекомендаціях Європейської Комісії (далі – Єврокомісія) [5, с. 119].

Одним з різновидів альтернативного вирішення спорів є онлайн вирішення спорів (Online Dispute Resolution, далі – ODR). ODR – це сукупність методів врегулювання спорів (конфліктів) із застосуванням Інтернет-технологій. Онлайн вирішення спорів (ODR) є ADR процедурою, яка проводиться повністю в режимі онлайн. Впровадження інноваційних технологій, включаючи Інтернет-технології, дозволяє значно розширити можливості цих традиційних процедур [9].

Наприклад, коли у споживачів виникають проблеми з трейдером щодо товару або послуги, які вони купили, вони можуть врегулювати свій спір поза судом за альтернативною процедурою врегулювання спорів.

Такі процедури є альтернативою вирішення спорів до суду і, отже, називаються альтернативним вирішення спорів (ADR). Коли ця процедура відбувається в Інтернеті, вона називається онлайн вирішенням спорів (ODR).

Вирішення спорів через ADR набагато простіше, швидше і дешевше, ніж вирішення спорів в суді. В Європейському Союзі процедури ADR можуть приймати різні форми і мають різні назви, наприклад, посередництво, примирення, арбітраж, омбудсмен, дошки скарг.

З метою прискорення та спрощення вирішення спорів за участю споживачів в травні 2013 року були прийняті два документи: Директива № 2013/11 / ЄС Європейського Парламенту та Ради ЄС «Про альтернативному вирішенні спорів за участю споживачів» (далі – Директива № 2013/11 / ЄС) [1] і Регламент № 524/2013 Європейського Парламенту та Ради ЄС

«Про врегулювання спорів за участю споживачів онлайн» (далі – Регламент № 524/2013) [2].

Директива № 2013 / 11 / ЄС складається з п'яти глав: 1) загальні положення; 2) доступ до інформації і вимоги, що пред'являються до процедури ADR і установи, які здійснюють процедури ADR; 3) інформація про співпрацю; 4) роль компетентних органів і Єврокомісії; 5) прикінцеві положення.

У ст. 1 Регламенту ЄС № 524/2013 визначено його мету: «Шляхом досягнення високого рівня захисту прав споживачів внести свій вклад в належне функціонування внутрішнього ринку ЄС шляхом створення європейської платформи онлайн-вирішення спорів (ODR platform)». Положення Регламенту ЄС № 524/2013 передбачають також сприяння державам-членам ЄС у створенні прозорої та ефективної системи альтернативного вирішення спорів між споживачами та онлайн-продавцями [2].

У ст. 2 Регламенту ЄС № 524/2013 зафіксована сфера його застосування. Регламент застосовується до розгляду і вирішення спорів з договірних зобов'язань, що виникли з договорів онлайн-продажів між споживачами – мешканцями країни-члена ЄС і онлайн-продавцями, на платформі ODR. Держави-члени ЄС повинні інформувати Єврокомісію про те, чи дозволяє їхнє законодавство розглядати суперечки між споживачами і онлайн-продавцями в режимі онлайн [2].

У ст. 5 передбачені основні умови створення платформи ODR. Її створення, підтримку, а також технічне обслуговування, фінансування і забезпечення безпеки комп'ютерних даних повинна забезпечувати Єврокомісія. Платформа ODR повинна бути єдиною точкою входу для громадян-споживачів і онлайн-продавців. Передбачається можливість використання даного веб-сайту безкоштовно і на всіх мовах ЄС [2].

Отже, що таке онлайн вирішення спорів – ODR?

Якщо споживачі мають претензії з приводу товару або послуги, які вони купили, то замість того, щоб йти до суду, вони можуть вибрати альтернативне врегулювання спорів (ADR). Термін ADR включає в себе всі шляхи вирішення скарг, які не пов'язані зі зверненням до суду.

Як правило, споживачі просять нейтральну третю сторону виступити в якості посередника між ними і трейдером; ця

нейтральна третя сторона називається установою ADR. Уповноважена особа ADR може потім запропонувати рішення або просто зібрати обидві сторони разом, щоб обговорити, як знайти рішення.

Що таке і як працює платформа ODR Європейського Союзу?

Платформа ODR є веб-платформою, яка була розроблена Європейською комісією. Відповідно до чинного законодавства, Комісія підготувала платформу до терміну 9 січня 2016 р. Проте, вона стала доступна для використання з 15 лютого 2016 року для забезпечення максимального географічного та галузевого охоплення всієї території Європейського Союзу.

Її мета полягає в тому, щоб допомогти споживачам і онлайн-продавцям вирішити свої договірні суперечки з приводу покупок товарів і послуг поза судом, за низькою ціною, простим і швидким способом.

Це дозволяє споживачам представляти на розгляд свої суперечки онлайн на будь-якій з 23 офіційних мов Європейського Союзу. Держави-члени повинні створити національний контактний пункт для надання допомоги користувачам платформи ODR. Перелік цих національних контактних пунктів розміщений на платформі ODR.

Це відбувається наступним чином. Споживач заповнює електронну форму скарги. Потім скарга направляється відповідному онлайн-продавцю, який пропонує установа ADR споживачеві. Після того, як споживач і онлайн-продавець домовляються про установу ADR, яка вирішить їх суперечку, платформа ODR автоматично передає скаргу даній установі. Уповноважена особа ADR обробляє випадок повністю онлайн і досягає результату протягом 90 днів.

Які переваги ODR?

Завдяки ODR, споживачі і трейдери будуть більш впевнені в торгівлі в Інтернеті. Таким чином, споживачі і трейдери будуть знати, що вони зможуть врегулювати свої суперечки без суду, простим, швидким і недорогим способом. Крім того, ODR сприятиме розвитку нової культури outof-court (поза судом), примирливого вирішення спорів між споживачами та онлайн-продавцями в ЄС. Споживачі будуть домагатися відшкодування

навіть при здійсненні малоцінних покупок і забезпечення дотримання їх прав. Трейдерам в ЄС це також принесе користь. В даний час близько 60% Інтернет-продажів не здійснюється через передбачувані труднощів вирішення проблем, що випливають з такого продажу. ODR дозволить заощадити на дорогих судових розглядах, а також дозволить підтримувати ділову репутацію і хороші відносини з клієнтами.

Яке законодавство знаходиться в основі ODR платформи?

Положення ODR встановлює на всій території ЄС платформу для сприяння онлайн дозволу договірних суперечок між споживачами і трейдерами ЄС за покупки, здійснені в мережі Інтернет. Ця платформа ODR пов'язує всі установи ADR, нотифіковані державами-членами відповідно до ADR Директиви № 2013/11 / ЄС. Відповідно до нового законодавства, трейдери повинні також надати посилання на платформу ODR на своєму сайті. Директива № 2013/11 / ЄС забезпечує правову основу для ADR в цілому. Це гарантує, що споживачі ЄС можуть звернутися до уповноваженої особи ADR для вирішення всіх своїх договірних суперечок практично у всіх секторах економіки з онлайн-продавцями, незалежно від того, де (всередині країни або за її кордоном) і як (онлайн / оффлайн) покупка була зроблена [3].

Зобов'язання для онлайн-продавців надати посилання на платформу ODR.

Компаніям, створеним в ЄС, які продають товари або послуги для споживачів в мережі Інтернет, необхідно дотримуватися законодавства ADR / ODR. Онлай-продавці, які здійснюють продаж в мережі Інтернет, зобов'язані використовувати ADR і при цьому повинні інформувати споживачів про можливість вирішення спорів такою установою ADR. Вони повинні робити це на своїх веб-сайтах. Вони зобов'язані надати наступне посилання http://ec.europa.eu/odr з їх сайту на платформу ODR. Для вказівки на ODR платформу, трейдери також можуть використовувати інтерактивні веб-банери (http://europa.eu/youreurope/promo/odr-banners/index_en.htm), які доступні на різних мовах ЄС.

У главі ІІІ Регламенту ЄС № 524/2013 «Прикінцеві положення» передбачено, що до 9 липня 2018 року Єврокомісія повинна надати звіт про застосування положень Регламенту ЄС № 524/2013 в державах-членах ЄС.

Впровадження в практику нового способу вирішення спорів за участю громадян-споживачів у ЄС – онлайн вирішення спорів на спеціальному веб-сайті платформи ODR – заслуговує найпильнішої уваги і вивчення, оскільки відкриває нові можливості електронного правосуддя.

Таким чином, в зв'язку зі зростаючою кількістю суперечок щодо надання та отримання Інтернет-послуг вважаємо найбільш перспективними шляхами вирішення цієї проблеми в Україні: а) впровадження інституту онлайн вирішення спорів – ODR, з належним чином регламентованою ODR платформою; б) виділення і законодавче закріплення певної категорії справ, які підлягають розгляду шляхом електронного вирішення спору; в) імплементація вже існуючого законодавства і практики Європейського Союзу в правову сферу регулювання цих відносин в Україні.

Список літератури

1.Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) № 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR). [Электронный ресурс]. – Режим доступа: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0063:0079:EN:PDF

2.Regulation (EU) № 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) № 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR). [Электронный ресурс]. – Режим доступа: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0001:0012:EN:PDF

3.Settling consumer disputes online [Электронный ресурс]. – Режим доступа: http://ec.europa.eu/consumers/solving_consumer_disputes/docs/adr-odr.factsheet_web.pdf

4.Uniform Mediation Act [Электронный ресурс]. – Режим доступа: http://www.uniformlaws.org/shared/docs/mediation/uma_final_03.pdf

5.Берлингуэр Альдо. «Мягкое право» против «жесткого права» в Европейском Союзе // Современное право. – 2012. – №12. – С. 119.

6.Ермакова Е.П., Ивановская Н.В Онлайн-разрешение споров с участием потребителей в Европейском союзе: документы 2013 года. [Электронный ресурс]. – Режим доступа: http://xn----7sbbaj7auwnffhk.xn--p1ai/article/1887

7.Карпенко О. І. Інтернет-послуга як об’єкт цивільно-правових відносин [Текст]: дис. ...канд. юрид. наук: 12.00.03 / О. І. Карпенко; Харківський національний університет імені В. Н. Каразіна. – Х., 2015. – 207 с.

8.Конвенция о признании и приведении в исполнение иностранных арбитражных решений (Нью-Йорк, 1958 год) [Электронный ресурс]. – Режим доступа:
http://www.uncitral.org/uncitral/ru/uncitral_texts/arbitration/NYConvention.html

9.Онлайн-врегулювання спорів [Электронный ресурс]. – Режим доступа: http://www.wikipage.com.ua/Internet/onlayn-vregulyuvannya_sporv.html

10. Онлайн-разрешение споров с участием потребителей в Европейском Союзе: документы 2013 года / Е. П. Ермакова, Н. В. Ивановская // Современное право. – 2014. – №8. – С. 128–132.

11. Полатай В. Ю. Вирішення спорів у мережі Інтернет. Альтернативний спосіб / В. Ю. Полатай // Актуальні проблеми сучасного міжнародного права: зб. наук. ст. за матеріалами І Харк. міжнар.-прав. читань, присвяч. пам’яті проф. М. В. Яновського і В. С. Семенова, Харків, 27 листоп. 2015 р. : у 2 ч. – Харків, 2015. – Ч. 1. – С. 241-247.

Кохановська О.В. –
професор кафедри цивільного права
Київського національного університету ім. Т. Шевченка
доктор юридичних наук, професор

ПРИВАТНО-ПРАВОВЕ РОЗУМІННЯ ІНФОРМАЦІЙНИХ ВІДНОСИН В УКРАЇНІ

У вітчизняній доктрині права на сьогодні сформувалося декілька теорій щодо поняття, змісту і місця інформаційних відносин у системі права і системі законодавства України. Їх становлення відбувалося починаючи із середини XX століття і продовжується в наш час. Перш за все, вражає різноманітністю спектр поглядів на інформацію як об’єкт правовідносин, особливості суб’єктного складу інформаційних правовідносин, дискусії щодо предмету і методу, принципів цих відносин. Це, а також значна кількість сфер інформаційних відносин, починаючи від права на інформацію як особистого немайнового права і закінчуючи інформаційними відносинами у журналістській, архівній, творчій тощо діяльності породили різні, інколи протилежні підходи до розуміння місця і правової природи масиву норм, присвячених правовому регулюванню відносин у названій сфері.

Поряд із концепцією інформаційного права як галузі права в Україні, особливо після прийняття Цивільного кодексу України 2003 р.[1] (далі – ЦК України), актуальності набула теорія інформаційних прав як цивільно – правового інституту. Закріплення інформації в якості окремого об'єкта цивільних прав у ст..200 ЦК України і права на інформацію як одного із найважливіших особистих немайнових прав фізичної особи у ряді статей Книги другої ЦК України надало поштовх для все більш інтенсивного пошуку у цьому напрямі.

Усвідомлення інформації, перш за все, як нематеріального, неекономічного, тісно пов'язаного з особою блага відкрило широкі можливості для ефективної охорони і захисту інформаційних прав усіма цивільно – правовими засобами. Саме завдяки застосуванню усього інструментарію цивільного права фізична особа має право вільно збирати, зберігати, використовувати і поширювати інформацію.

Так само завдяки глибоким теоретичним розробкам у сфері зобов'язального права знаходить своє логічне пояснення інформація як товар.

Серед двох теорій, які мають найбільше послідовників – теорія інформаційного права як окремої галузі права (ІТ – права) і приватно – правова концепція інформаційних відносин як інституту цивільного права і комплексного інституту законодавства України. Особливо вражаючими можна визнати темпи розвитку теорії інформаційного права як окремої галузі права в ряді зарубіжних пострадянських країнах але не менш активно розвивається в останні десятиліття вітчизняна теорія інформаційних прав як інституту цивільного права. Про останнє свідчать численні роботи українських авторів – цивілістів.

У даних тезах ми зазначимо більш детально про Концепцію інформаційних прав як приватно – правового інституту, оскільки вона, на нашу думку, не тільки за своєю суттю теоретично вірна, але і практично витребувана сучасним суспільством. Крім того, саме з цією теорією, яка ґрунтується на основних засадах приватного права, гармонійно пов'язується майбутнє усього людства за умови обрання ним цивілізованих і гуманних шляхів розвитку.

Інформаційні цивільні права розглядаються також у даній теорії як основа інституту комплексного інформаційного законодавства, які мають визначальний вплив на їх регулювання в цілому. Найбільш повно дана теорія знайшла своє втілення у доктринальному обґрунтуванні і пропозиціях по доповненню ЦК України новою Главою «Загальні положення про інформаційні права»[2].

Якщо вести мову про інформаційне право із зазначених позицій, то це право фізичної особи створювати, виробляти, одержувати, знати, фіксувати, використовувати, поширювати та зберігати інформацію у порядку, передбаченому ЦК України та іншими законами. Юридичні особи також мають відповідні інформаційні права, які не пов'язані з особливостями людини як живої істоти. При цьому інформаційні права мають бути закріплені саме у законах.

Інформаційні права становлять: особисті немайнові інформаційні права, включаючи право на інформацію, та (або) майнові інформаційні права, в тому числі на інформаційні продукти, ресурси, документи, зміст яких щодо певних об'єктів інформаційних прав визначається, перш за все, Конституцією України і ЦК України, а також іншими законами.

Самі поняття «інформаційні права», «право на інформацію» слід розуміти як правову фікцію, оскільки подібні вирази стосовно інформаціє є вельми умовними, а також розрізняти їх за змістом як категорії.

Крім того, інформаційні правовідносини – як особисті немайнові, так і майнові, мають приватноправову природу і не потребують штучного обмеження і безмежного контролю, а права на повагу до інформації як особистого немайнового блага фізичної особи слід дотримуватися ще до моменту народження людини, навіть до того, як вона набуде статусу суб'єкта права. Фактично право на повагу до інформації, яка є сутністю людини разом із матерією, в якій вона уособлюється, яку несуть, зокрема, гени, слід визначити у законодавстві так само як право на повагу до життя зачатої дитини - тобто з моменту зачаття.

Інформаційне право є непорушним. Ніхто не може бути позбавлений інформаційних прав чи обмежений у їх здійсненні, крім випадків, передбачених законом.

Слід особливо підкреслити, що інформаційне право та право власності на річ (документ, продукт, ресурс) в якій інформація втілена, не залежать одне від одного. При цьому перехід права на інформацію, як на об'єкт інформаційного права, не означає переходу права власності на форму, в якій вона уречевлена (на документ, продукт, ресурс тощо). В свою чергу, перехід права власності на документ (продукт, ресурс тощо), як на річ, не означає переходу прав на інформацію. Інформація, як відомості, зафіксовані на матеріальному носії (документована інформація) ототожнюється з цим носієм для зручності обігу в разі легального закріплення такого поєднання визначеними способами і у відповідності із законодавством України.

До об'єктів інформаційного права належать: інформація як немайнове благо; відкрита інформація та інформація з обмеженим доступом (в тому числі усі види таємниць); інформаційні продукти (ресурси), документи тощо в різних сферах інформаційної діяльності; інформаційні системи (мережі, в тому числі Інтернет); об'єкти права інтелектуальної власності, які не мають кваліфікуючих ознак і не визнані такими у встановленому законом порядку; відкриття; інформація, яка набуває юридичного значення в момент і за умови фіксації її впливу на людину. Для того, щоб пояснити запропонований перелік об'єктів інформаційних прав, необхідно врахувати одне з основних положень теорії інформаційних прав, а саме те, що інформація як об'єкт цивільного права розглядається нами у таких її проявах: 1) як особисте немайнове благо у комплексі благ, перерахованих у Книзі другій ЦК України; 2) як результат творчої інтелектуальної діяльності, тобто як об'єкт виключних прав, врегульованих у ст.199 і Книзі 4 ЦК України; як інформаційний продукт, ресурс, документ, тобто об'єкт, який може бути інформаційним товаром і предметом будь – яких правочинів, договорів з урахуванням особливостей і специфіки як об'єкту особливого роду.

Інформація, як результат інтелектуальної творчої діяльності і інформація, як особисте немайнове, не пов'язане з майновими, благо, є об'єктами інформаційного права і регулюються нормами відповідної глави ЦК України у тій

частині, в якій вони не врегульовані Книгою 2 і Книгою 4 ЦК України.

Суб'єктами інформаційного права є: будь – які фізичні та (або) юридичні особи, в тому числі: фізичні особи, які мають право на інформацію як особисте немайнове право з моменту народження і юридичні особи, які мають право на інформацію з моменту утворення; творець (творці) інформації; виробник (виробники) інформації; володілець інформаційного продукту (ресурсу, документу тощо); володілець інформаційної системи, мережі тощо; особа, яка використовує, споживає, знає інформацію та інші особи, яким належать особисті немайнові та (або) майнові інформаційні права відповідно до ЦК України, іншого закону чи договору.

Згідно з теорією інформаційних прав інформаційні права виникають в результаті народження фізичної особи, чи утворення юридичної особи, створення чи (або) вироблення інформації, а також набуваються з підстав, встановлених ЦК України, іншим законом чи договором.

Особистими немайновими інформаційними правами є: 1) право на інформацію (достовірну, актуальну, повну тощо), доступ особи до інформації про неї (персональні дані) та інші особисті немайнові, не пов'язані з майновими права, передбачені Книгою 2 ЦК України; 2) право на визнання людини творцем об'єкта інформаційного права, в тому числі, передбачене Книгою 4 ЦК України; 3) право перешкоджати будь – якому посяганню на інформаційне право, в тому числі, здатному завдати шкоди честі чи репутації її творця (виробника) об'єкта інформаційного права; 4) право отримувати, знати, поширювати інформацію та інші особисті немайнові інформаційні права, встановлені законом.

Особисті немайнові інформаційні права належать фізичній, юридичній особі як право на інформацію, тобто особисте немайнове, не пов'язане з майновим, право; творцеві об'єкта інформаційного права; фізичній особі, яка знає інформацію. У випадках, передбачених законом, особисті немайнові інформаційні права можуть належати іншим особам.

Особисті немайнові інформаційні права не залежать від майнових інформаційних прав і не можуть відчужуватися

(передаватися) ні за яких умов, якщо вони є правом на інформацію, тобто особистим немайновим, не пов'язаним з майновими, правом, передбаченим Книгою 2 ЦК України і не можуть відчужуватися (передаватися), якщо вони є особистими немайновими, пов'язаними з майновими, правами, передбаченими ЦК України, за винятками, встановленими законом.

Щодо майнових інформаційних прав, то серед них можна назвати право на вироблення інформації; право на доступ і використання інформації; право дозволяти використання об'єкта інформаційного права; право перешкоджати неправомірному використанню і поширенню об'єкта інформаційного права, в тому числі забороняти таке використання; інші майнові інформаційні права, встановлені законом.

Право на інформацію та інші інформаційні права, передбачені Книгою 2 ЦК України не мають майнового еквівалента, неекономічні і не можуть визнаватися майновими ні за яких умов.

Законом при цьому можуть бути встановлені винятки та обмеження в майнових інформаційних правах за умови, що такі обмеження та винятки не створюють істотних перешкод для нормальної реалізації майнових інформаційних прав та здійснення законних інтересів суб'єктів цих прав. При цьому майнові інформаційні права можуть відповідно до закону бути вкладом до статутного капіталу юридичної особи, предметом договору застави та інших зобов'язань, а також використовуватись в інших цивільних відносинах.

Інформаційними правами отримувати, знати, поширювати тощо інформацію, включаючи право на інформацію, як особистими немайновими, не пов'язаними з майновими, правами фізична особа володіє довічно, а юридична особа – безстроково відповідно до Книги 2 ЦК України; особистими немайновими, пов'язаними з майновими, інформаційними правами особи володіють відповідно до Книги 4 ЦК України, а майнові інформаційні права є чинними протягом строків, встановлених ЦК України, іншим законом чи договором. Майнові інформаційні права можуть бути припинені достроково у спеціально встановлених законом чи договором випадках.

Специфікою відзначається використання об'єкта інформаційного права. Способи використання об'єкта інформаційного права визначаються ЦК України, главою, присвяченою інформаційним правам, Книгою 4 та іншими законами. При цьому особа, яка має право (в тому числі виключне) дозволяти використання об'єкта інформаційного права, може використовувати цей об'єкт на власний розсуд, з додержанням прав інших осіб. Використання об'єктів, які складають відкриту інформацію здійснюється будь – якою особою вільно, крім випадків, які передбачені законом. Використання об'єктів, які складають інформацію з обмеженим доступом іншою особою здійснюється з дозволу особи, яка має право дозволяти використання об'єкта інформаційного права, крім випадків правомірного використання без такого дозволу, передбачених ЦК України та іншим законом. Умови надання дозволу на використання об'єкта інформаційного права (як відкритої інформації, так і інформації з обмеженим доступом), можуть бути визначені інформаційним договором, який укладається з додержанням вимог ЦК України та іншого закону.

В теорії інформаційних прав, крім того, досліджуються питання передання майнових інформаційних прав та здійснення інформаційного права, яке належить декільком особам, особливості права на інформаційний об'єкт, створений або вироблений у зв'язку з виконанням трудового договору, права на інформаційний об'єкт, створений у зв'язку з виконанням трудового договору та інформаційні права на інформаційний об'єкт, створений або вироблений на замовлення; наслідки порушення інформаційних прав та захист інформаційних прав судом.

На сьогоднішній день дану теорію в Україні підтримують у своїх роботах такі вчені, як Т.І. Бегова, Ю.О. Борисова, Б.М. Гоголь, О.А. Джуринський, А.О. Кодинець, А.Г. Дідук, Ю.В. Носік та ряд інших[3; 4; 5; 6;7; 8; 9].

Неоціненний внесок у створенні передумов виникнення і подальший розвиток розглянутої теорії був зроблений видатним вітчизняним правознавцем В.І. Жуковим, законодавче закріплення інформація як об'єкт цивільних прав отримала завдяки розробникам чинного ЦК України, особливо цивілістам

А.С. Довгерту, Н.С. Кузнєцовій, О.А. Підопригорі, які заклали підвалини для розвитку інформаційних правовідносин саме в дусі приватного права на принципах цивільного права і основних засадах цивільного законодавства, гармонійно поєднавши предмет і основний метод регулювання цивільних та інформаційних відносин.

Другий підхід заснований на розумінні інформаційного права як галузі права, яка регулює суспільні відносини в інформаційній сфері. Обгрунтуванню таких підходів присвячена значна кількість широко відомих для спеціалістів ІТ – права робіт ряду авторів. В цих тезах ми не наводимо їх, оскільки вони виходять далеко за межі заявленої теми.

Слід звернути увагу і на те, що виокремився з часом і третій підхід, який являє собою ще більш вузьке розуміння інформаційного права, за якого вважається, що його можна застосовувати тільки для регулювання відносин, які виникають при обробці документованої інформації чи при обробці інформації у системі телекомунікацій тощо.

Сучасні представники теорії інформаційного права, такі як Л.Л. Попов, Ю.І. Мігачов, С.В. Тихомиров вважають, що інформаційне право являє собою одну з найскладніших галузей права, що, на їх думку, обумовлено предметом даної галузі права – суспільними відносинами в інформаційній сфері, тобто відносинами, пов'язаними з інформацією, використанням інформаційних технологій і захистом інформації і які виникають при здійсненні інформаційних процесів – виробництва, збору, обробки, накопичення, зберігання, пошуку, передачі, поширення і споживання інформації [10, с.9].

Так само як і В.О. Копилов, сучасні прибічники теорії інформаційного права розглядають «інформаційне право» у трьох значеннях: як галузь права, що регулює певну групу суспільних відносин, як науку, яка вивчає правові проблеми в інформаційній сфері, і як учбову дисципліну і вважають, що воно регулює інформаційну діяльність у всіх сферах життя суспільства [11, с.13].

Таким чином, ключовим поняттям у визначенні інформаційного права є для теоретиків інформаційного права відносини в інформаційній сфері: інформаційне право – як

сукупність юридичних норм, які регулюють суспільні відносини в інформаційній сфері, пов'язані з виробництвом, передачею, поширенням, пошуком і отриманням інформації, застосуванням інформаційних технологій, а також захистом інформації [10, с. 31].

Провідні вітчизняні дослідники теорії інформаційного права обґрунтовують концепцію формування галузі інформаційного права так само – як групи правових норм, які регулюють суспільні відносини, що виникають з приводу встановлення режимів та параметрів суспільного обігу інформації, правового статусу, поведінки та зв'язків суб'єктів інформаційних процесів [12, с. 88].

Вважається, що «за природою правового походження, як комплексна галузь національного права України, інформаційне право має приватно – правову і публічно – правову природу. Тобто, норми інформаційного права формуються як на публічному (державному), так і на приватному рівнях суспільних відносин» [12, с. 89].

З цього приводу варто зауважити, що вказівка на подвійну правову природу правового походження галузі, завжди призводить до плутанини, яка не сприяє виявленню важливих закономірностей і особливостей галузі, фактично не виявляє її дійсної правової природи, її основоположного методу і принципів, а протиставляння державного і приватного інтересу, з точки зору цивілістики, ускладнюється тим, що держава щодо інформаційних відносин має так само «приватні», власні інтереси, як і будь – який інший суб'єкт цих відносин. Держава в ідеалі повинна керуватися у такому випадку «власними інтересами» членів суспільства на їх суспільну користь. Між тим, у незаангажованості інтересу держави в останні десятиліття доводиться все більше сумніватися, оскільки часто інтереси держави збігаються не із суспільним інтересом її громадян, а з невеликою групою осіб, які «приватизують» ці інтереси і трактують їх на свою, знов – таки, «приватну» користь. Тому незайвим буде ще раз підкреслити, що інформаційні відносини мають приватно – правову природу їх походження, а комплексність цих відносин пояснюється наявністю ряду виключень, в тому числі і суттєвих, щодо реалізації і захисту

інформаційних прав, які здійснюються за допомогою інструментарію інших галузей права. Немає потреби доводити наявність нової галузі, якщо вже існуючі ефективно справляються з формуванням необхідної і достатньої системи регулювання інформаційних відносин, охороною і захистом прав усіх учасників таких відносин.

Надзвичайно важливо, між тим, пам'ятати, що переваги інформаційного суспільства завжди залишаються поруч з його проблемами і ризиками, інформаційне суспільство також є недосконалим, тому і наслідки застосування його механізмів цілком залежить від ціннісних орієнтирів і політичних рішень того чи іншого суспільства, держави.

Сучасні автори називають предметом інформаційного права суспільні відносини, пов'язані з виробництвом, переданням, поширенням, пошуком і отриманням інформації, застосуванням інформаційних технологій, а також захистом інформації; методом інформаційного права вважають усі прийоми, способи і засоби впливу права на суспільні відносини, які дозволяють визначити сферу правового регулювання. Виходячи із останньої тези прибічники теорії інформаційного права відносять до методів інформаційного права методи припису, заборони і дозволу в усій їх сукупності. Крім того, на їх думку, методи правового регулювання інформаційних відносин поділяються на адміністративно – правовий і цивільно – правовий, які мають, на їх думку, однаково особливе значення для регулювання інформаційних відносин.

З точки зору цивілістів режим правового регулюванні інформаційних відносин не завжди заснований на рівності їх учасників, але останнє має бути пріоритетним, виходячи із правової природи інформаційних відносин і враховуючи, що все інше – це завжди виключення із цього найважливішого правила.

Має свої недоліки і твердження про те, що «в інформаційному і цивільному праві існує ряд міжгалузевих інститутів, наприклад, інститут інтелектуальної власності, оскільки його коріння знаходиться у системі цивільного права, але забезпечується він нормами як цивільного, так і інформаційного права» [10, с.32]. Ми притримуємося позиції, що право інтелектуальної власності є складовою міжгалузевого

інституту інформаційних відносин (або інформаційних прав), коріння якого знаходяться у системі цивільного права. Права інтелектуальної власності, таким чином, є за своєю суттю інформаційними правами, які характеризуються творчим або іншим спеціально обумовленим елементом і у зв'язку з цим їх суб'єкти отримують додаткові специфічні засоби і способи охорони і захисту своїх прав.

Особливо слід звернути увагу на те, що для пояснення теорії інформаційного права як галузі права автори досліджують питання предмету, методу, принципів інформаційного права, що, на нашу думку, яскраво виявляє як особливості цієї теорії, так і ряд помилок, які впливають не лише на доктринальний рівень проблеми, але породжують недоліки у правовому регулюванні інформаційних відносин і пошуку ефективних шляхів реалізації, заходів, засобів і способів захисту інформаційних прав.

Додамо також, що у спектрі теорій, які висуваються представниками правової науки обґрунтовуються також підходи до інформаційних відносин як галузевих і як інституту комплексного галузевого законодавства, але значних заперечень з точки зору аргументів, які ними висуваються, з боку представників двох основних теорій вони не викликають, а слугують лише в якості доповнення. Осторонь залишається проприєтарна теорія, яка у сфері інформаційних відносин розглядає інформацію та інші об'єкти інформаційних прав з точки зору права власності на них, між тим, в теорії права вона в останнє десятиліття все більше втрачає свої переваги.

Список літератури

1.Цивільний кодекс України від 16.01.2003 р. №435 – IУ/ Відомості Верховної Ради України (ВВР). – 2003. - №40 – 44. – Ст. 356.

2.*Кохановська О.В.* Теоретичні проблеми інформаційних відносин у цивільному праві. Монографія. – К.: Виробничо – поліграфічний центр «Київський університет», 2006. – 463 с.

3.*Бєгова Т.І.* Поняття ноу – хау та договір про його передачу: Автореферат дис…..канд. юрид. наук: 12.00.03/ Національна юридична академія імені Ярослава Мудрого. – Харків., 2008. – 19с.

4.*Борисова Ю.О.* Цивільно – правове регулювання відносин у сфері електронної комерції: Автореферат дис….анд.юрид.наук: 12.00.03/ Київський національний університет імені Тараса Шевченка. – К.,2012. – 19с.

5.*Дідук А.Г.* Правовий режим конфіденційної інформації: цивільно-правовий аспет: Авторе. Дис….канд. юрид. наук: 12.00.03/Харківський національний університет внутрішніх справ. – Х., 2008. – 21с.

6.*Джуринський О.А.* Захист від недобросовісної конкуренції (цивільно-правовий аспект: Автореф. … дис. канд. юрид. наук: 12.00.03/ Київський національний університет імені Тараса Шевченка. – К., 2010. – 18с.

7.*Гоголь Б.М.* Право на інформацію в цивільному праві України: Автореф. Дис..канд.юрид.наук: 12.00.03/ НАН України. Інститут держави і права імені В.М.Корецького. – К., 2010. – 16 с.

8. *Кодинець А.О.* Цивільно – правове регулювання зобов'язальних інформаційних відносин: монографія. / А.О.Кодинець. – К.: Алерта, 2016. – 582с.

9.*Носік Ю.В.* Права на комерційну таємницю в Україні (цивільно-правовий аспект): автореф. … дис. канд. юрид. наук: 12.00.03. – К., 2006. – 18с.

10. *Попов Л.Л., Мигачев Ю.И., Тихомиров С.В.*. Информационное право. Учебник. – НОРМА. Инфра – М. Москва, 2010. – 496 с.

11. *Копылов В.А.* Информационное право; Учебник. – 2-е изд., перераб. и доп. – М.:Юристъ, 2003. – 512 с.

12. *Марущак А.І.* Інформаційне право: Доступ до інформації: Навчальний посібник. – К.: КНТ, 2007. – 532 с.

Кохановський В.О. –
аспірант кафедри цивільного права
Київського національного університету ім. Т. Шевченка

ІНФОРМАЦІЯ ЯК ОДИН ІЗ ОСНОВНИХ ЕЛЕМЕНТІВ У ВИЗНАЧЕННІ ЗМІСТУ, ФОРМИ І УМОВ ДОГОВОРУ ПРО НАДАННЯ ТУРИСТИЧНИХ ПОСЛУГ

Значний інтерес у приватному праві являє собою аналіз змісту, форми та умов договору про реалізацію туристичного продукту.

Надзвичайно важливу роль у розумінні і наповненні цих елементів договірної сфери у туризмі в останні роки відіграє інформація, яка значною мірою визначає як зміст, так і форму відповідних договорів, а надання об'єктивної, достовірної, повної інформації є важливою умовою їх укладання.

Теоретично зміст договору як юридичного факту, як відомо, являє собою сукупність умов, за якими досягнуто згоду сторін. Чіткість і визначеність змісту договору передбачає

особливості прав і обов'язків, які виникають, можливість належного виконання сторонами зобов'язань, наслідки їх порушення.

В літературі немає єдиної точки зору з питання класифікації умов договору. Більшість вчених поділяє їх на три групи умов: істотні, звичайні і випадкові. Навпаки, М.І. Брагінський переконаний, що немає підстав для виокремлення, як це пропонується у більшості джерел, крім істотних, ще й звичайних і випадкових умов, оскільки всі умови, за якими досягнуто згоду, і є суттєві, і жодних інших умов, крім істотних, в договорі не може бути [1, с.211 - 212]. На нашу думку, це найбільш обґрунтований підхід.

Цивільний кодекс розкриває переважно зміст істотних умов, тобто таких, які необхідні і достатні для визнання договору укладеним. Відповідно до ч. 1 ст. 628 Цивільного кодексу України [2] (Далі – ЦК України) зміст договору становлять умови (пункти), визначені на розсуд сторін і погоджені ними, та умови, які є обов'язковими відповідно до актів цивільного законодавства.

Предметом договору про надання туристичних послуг є надання комплексу послуг, які входять у туристичний продукт. Істотні умови у договорі на туристичне обслуговування закріплені у ч. 4 ст. 20 Закону України «Про туризм» [3] (далі – Закон):

1) строк перебування у місці надання туристичних послуг із зазначенням дат початку та закінчення туристичного обслуговування;

2) характеристика транспортних засобів, що здійснюють перевезення, зокрема їх вид та категорія, а також дата, час і місце відправлення та повернення (якщо перевезення входить до складу туристичного продукту);

3) готелі та інші аналогічні засоби розміщення, їх місце розташування, категорія, а також строк і порядок оплати готельного обслуговування;

4) види і способи забезпечення харчування;

5) мінімальна кількість туристів у групі (у разі потреби) та у зв'язку з цим триденний строк інформування туриста про те, що туристична подорож не відбудеться через недобір групи;

6) програма туристичного обслуговування;

7) види екскурсійного обслуговування та інші послуги, включені до вартості туристичного продукту;

8) інші суб'єкти туристичної діяльності (їх місцезнаходження та реквізити), які надають туристичні послуги, включені до туристичного продукту;

9) страховик, що здійснює обов'язкове та/або добровільне страхування туристів за бажанням туриста, інших ризиків, пов'язаних з наданням туристичних послуг;

10) правила в'їзду до країни (місця) тимчасового перебування та перебування там;

11) вартість туристичного обслуговування і порядок оплати;

12) форма розрахунку.

Уся зазначена інформація, як можна зробити висновок, є істотною і такою, що лише за наявності її у договорі, його можна бути вважати укладеним.

При цьому у ч. 5 ст. 20 Закону уточнюється, що зміна ціни туристичного продукту після укладення договору на туристичне обслуговування допускається лише у разі необхідності врахування зміни тарифів на транспортні послуги, запровадження нових або підвищення діючих ставок податків і зборів та інших обов'язкових платежів, зміни курсу гривні до іноземної валюти, в якій виражена вартість туристичного продукту.

Втім зазначений перелік істотних умов слід визнати дещо обтяжливим для сторін, оскільки законодавець значно розширив вимоги щодо інформації, яка має міститися у договорі, збільшуючи коло істотних умов. Їх аж дванадцять, отже, цей перелік визначає скоріше склад і кількість таких умов, але не їх зміст.

До істотних повинні відноситися тільки ті умови, які виражають природу договору – характерні риси відповідного договірного типу, без узгодження яких договір неможливо виконати. Крім того, недобросовісний контрагент нерідко заявляє про «неукладеність» договору, тож будь-яке невиправдане розширення кола істотних умов погіршує стан сторони, яка добросовісно виконує свої обов'язки за договором,

і крім того, не сприяє стабільності договірних зв'язків. Можливе і умисне не включення у договір істотних умов з наміром заявити про його недійсність («неукладеність») у подальшому, якщо це буде вигідно з будь-яких причин недобросовісній стороні договору.

В теорії вважається, що проникнення публічно-правових елементів у приватноправові відносини – визнаний факт, однак віднесення до істотних умов таких умов, у погодженні яких у сторін немає необхідності, можна розцінювати як невиправдане введення публічно-правового елементу, який обмежує свободу договору. Немає необхідності, наприклад, включати в якості істотних умов умови про фінансові гарантії. Отже, слід визначити, що є дійсно істотними умовами договору надання туристичних послуг: предмет, ціна і строк надання комплексу туристичних послуг. Одночасно це і є тою необхідною і достатньою інформацією, яка дозволяє сторонам узгодити усі найважливіші питання їх домовленостей.

Узгоджуючи предмет договору надання туристичних послуг, сторони договору повинні узгодити наступні умови щодо конкретного туристичного продукту:

– місце призначення подорожі;

– засоби, ознаки і категорії належного для використання транспорту для від'їзду і повернення з подорожі;

– дати і пункти відправлення і повернення з подорожі;

– місце, туристична категорія чи ступінь комфортності жилого приміщення, його основні риси, а також вид харчування у місці надання жилого приміщення;

– маршрут подорожі;

– спеціальні вимоги, які споживач повідомив особі, яка здійснює туристичну діяльність.

Інформація про всі інші умови має міститися у договорі у відповідності з імперативними вимогами законодавства. Як вірно зазначає В.В. Вітрянський: «Що стосується умов конкретного договору і їх співвідношення з імперативними нормами, то вони мають відповідати вказаним загально-визнаним правилам поведінки. Протиріччя умов договору імперативним нормам тягне за собою їх недійсність» [4, с.139].

Отже, слід також визнати, що неузгодженість істотних умов туристичного договору не впливає на обсяг прав туриста і їх захист, оскільки може потягти за собою негативні наслідки лише для організатора подорожі.

Обов'язок своєчасного надання споживачу інформації про туристичний продукт випливає із сутності усього інформаційного законодавства. Втім наявність окремої статті щодо інформації (ст. 19-1 Закону) – необхідна данина часу і вельми корисна для розвитку туристичних відносин в інформаційну добу.

Так, будь-яка інформація, надана туроператором (турагентом), повинна містити достовірні відомості про умови договору на туристичне обслуговування. Інформація про умови надання туристичних послуг, які туроператор (турагент) поширює до укладення договору на туристичне обслуговування, має доводитися у доступній, наочній формі, бути розбірливою, зрозумілою та містити відомості про:

1) місце надання туристичних послуг, програму туристичного обслуговування;

2) характеристику транспортних засобів, що здійснюють перевезення, зокрема їх вид і категорію;

3) характеристику готелів та інших об'єктів, призначених для надання послуг з тимчасового розміщення, у тому числі місце їх розташування, категорію, строки і порядок оплати готельного обслуговування;

4) види і способи забезпечення харчування під час туристичної подорожі; мінімальну кількість туристів у групі, а також інформування туриста про те, що туристична подорож не відбудеться через недобір групи, не пізніше ніж за три дні до початку туристичної подорожі;

5) ціну туристичних послуг (ч.ч. 1 і 2 ст.19-1 Закону).

Туроператор (турагент) зобов'язаний при цьому додержуватися умов надання комплексу туристичних послуг, про які був поінформований споживач до укладення договору на туристичне обслуговування, крім випадків, коли про зміну таких умов повідомлено споживача до укладення договору або якщо зміни внесено на підставі угоди, укладеної між сторонами договору (ч. 3 ст. 19-1 Закону).

Комплекс інформації, яка повинна бути надана туристу до укладання договору на сьогодні вражаючий за переліком відомостей. Перш за все, це інформація про основні вимоги до оформлення в'їзних/виїзних документів (паспорт, дозвіл (віза) на в'їзд/виїзд до країни тимчасового перебування), у тому числі строк їх оформлення; медичні застереження стосовно здійснення туристичної подорожі, зокрема протипоказання через певні захворювання, особливості фізичного стану (фізичні недоліки) і вік туристів, а також умови безпеки туристів у країні (місці) тимчасового перебування та цілий ряд інших відомостей, які закріплені у п.п. 1 – 10, ч.4 ст.19-1 Закону.

Права і обов'язки сторін, які складають зміст зобов'язального правовідношення, заснованого на договорі надання туристичних послуг, визначаються у відповідності зі структурою і особливостями цього правовідношення. Основні права і обов'язки туриста сформульовані у Законі і нині повністю відповідають загальновизнаним на міжнародному рівні вимогам у цій сфері.

Згідно Закону, реалізація турпродукту здійснюється на підставі договору, який укладається в письмовій чи електронній формі відповідно до закону (ч. 3, ст. 20 Закону).

В Україні законодавець в якості форми письмового договору на туристичне або екскурсійне обслуговування називає, як це прийнято у переважній більшості країн, ваучер (ст. 23 Закону). У договорі на туристичне обслуговування, укладеному шляхом видачі ваучера, мають міститися такі дані:

– найменування та місцезнаходження суб'єкта туристичної діяльності, номер ліцензії на відповідний вид діяльності, юридична адреса;

– прізвище, ім'я (по-батькові) туриста (при груповій поїздці прізвища, імена, по – батькові членів групи);

– строки надання і види туристичних послуг, їх загальні вартість;

– назва, адреса та номер телефону об'єкта розміщення, його тип та категорія, режим харчування;

– розмір фінансового забезпечення відповідальності туроператора (турагента) або межі відповідальності суб'єкта туристичної діяльності за договором агентування;

– інші дані, обумовлені характером угоди, складом групи;

– дата видачі ваучера (ч.2, ст. 23 Закону).

Істотними умовами договору надання туристичних послуг безумовно є предмет, ціна та строк надання комплексу туристичних послуг. Втім Закон визначає сьогодні дванадцять істотних умов, що слід визнати невиправданим перебільшенням.

Ряд дискусійних питань в теорії і на практиці викликає визначення сторін договорів у сфері туризму, їх права та обов'язки, а також порядок укладання відповідних договорів. Обсяг тез не дозволяє дослідити їх усі, тому ми зупинимося лише на тих які мають інформаційну складову.

Так, зокрема, останнім часом привертає увагу той факт, що туроператори – як суб'єкти туристичного ринку несуть всю повноту відповідальності перед споживачами, тоді як турагенти фактично виключаються із правового простору, а ступінь їх відповідальності обмежується лише повнотою і якістю інформації, яка надається. В результаті, турагентська діяльність інколи перетворюється на бізнес, який розвивається будь-якими шляхами – від офісів до приватних квартир – і не пов'язаний фактично з будь-якими ризиками.

Недоліки можуть з'являтися і у випадках, коли турагент доповнює продукт туроператора власними послугами, при туристичному консалтингу (надання консультативних послуг з самостійної організації подорожі), географічному коучингу (надання туристам інформації про географічні особливості передбачуваного місця відвідування для самостійного планування маршруту і організації поїздки) та ряді інших випадків.

Ряд спірних питань виникає як в теорії, так і на практиці щодо припинення (розірвання) договору туристичних послуг і при настанні відповідальності сторін за невиконання або неналежне виконання договорів у сфері туризму.

Договір як основний документ, який призводить до виникнення цивільно-правових відносин між замовником і виконавцем туристичних послуг, передбачає наявність ряду суттєвих і факультативних умов, а також зобов'язань, які набувають чинності для обох сторін з моменту його укладення. Укладений договір є обов'язковим для виконання сторонами, однак через різні причини як виконавець, так і замовник можуть розірвати договір на реалізацію туристичного продукту за тими чи іншими підставами.

Договір також може бути розірваний за узгодженням сторін у випадку істотної зміни обставин, якими сторони керувалися при його укладенні (ст. 652 ЦК України).

Виходячи із зазначеного, договір про надання туристичних послуг може бути припинений (розірваний) переважно за таких обставин:

– у зв’язку із істотною зміною обставин;

– у зв’язку із появою обставин, що загрожують життю і здоров’ю туристів;

– *у зв’язку з ненаданням чи наданням недостовірної інформації про споживчі якості туристичного продукту;*

– при наявності умов, які ущімлюють права туриста як споживача туристичних послуг.

Розірвання договору у зв’язку з ненаданням чи наданням недостовірної інформації про споживчі якості туристичного продукту пов’язана із розумінням обсягу і якості, а також вчасності інформації, яка має надаватися туристу.

Втім, на нашу думку, слід вести мову не тільки про необхідну і достовірну інформацію, але і повну, своєчасну, доступну для сприйняття інформацію, зокрема, про наступне:

– про правила в'їзду в країну (місце) тимчасового перебування і перебування там;

– про звичаї місцевого населення;

– про релігійні обряди, святині, пам'ятки природи, історії, культури та інших об'єктів для показу туристам, які перебувають під особливою охороною;

– про стан оточуючого природного середовища тощо.

Отже, до істотних умов договору про реалізацію турпродукту належить, як вже було зазначено, також інформація про ціну турпродукту (у гривнях), а також про його споживчі якості – програму перебування, маршрут і умови подорожі, включаючи інформацію про умови розміщення, про умови проживання (місцезнаходження засобу розміщення, його категорію) і харчування, послуги з перевезення туриста в країні (місці) тимчасового перебування, про наявність екскурсовода (гіда), гіда – перекладача, інструктора-провідника, а також про додаткові послуги.

Турист має право вимагати інформацію про: споживчі якості, вартість і порядок використання турпродукту; третіх осіб, які надають туристичні послуги; правила в'їзду – виїзду і документи, необхідні для цього; звичаї місцевого населення, пам'ятники, порядок доступу до туристичних ресурсів; ризики і небезпеки, які виникають під час подорожі; митні, санітарно – епідеміологічні, медичні, прикордонні та інші правила; контактні дані органів державної влади, дипломатичних представництв і консульств України; національні та релігійні особливості країни перебування; реєстровий номер туроператора, його фінансове забезпечення; умови забезпечення екстреною допомогою за рахунок засобів компенсаційного фонду об'єднань туроператорів у сфері виїзного туризму у випадку неможливості виконання, невиконанні чи неналежному виконанні туроператором зобов'язань за договором про реалізацію турпродукту, який формується виконавцем – членом об'єднання туроператорів у сфері виїзного туризму тощо.

Таким чином регулюються інформаційні відносини між споживачами і виконавцями послуг, а також їх продавцями (турагентами), встановлюються права споживача на отримання послуг та інформації про їх виконавців і продавців.

Законодавець має детально визначати обсяг інформації, яка в обов'язковому порядку має надаватися туристам як до, так і в момент укладання договору. Втім в нинішній час ще недостатньо врегульовані способи надання такої інформації, не достатньо регламентується порядок оформлення і зміст джерел такої інформації. Крім того, на практиці часто надається менш

широкий спектр інформації ніж необхідна, що призводить до порушень прав туристів, які йому складно довести.

Автори неодноразово зазначають, що не дивлячись на те, що законодавство містить норми про необхідність надання інформації, проблема інформування туристів має місце. Так, недоліки в інформаційному забезпеченні породжують, за їх дослідженнями, близько 90% усіх конфліктів між туроператорами чи турагентами і туристом. Перш за все, - роблять вони висновок, - це стосується основних характеристик інформації, яка надається – її необхідності, повноти, достовірності, строків надання, що, в кінцевому рахунку, визначає правильність вибору того чи іншого турпродукту [5, с.12].

Якщо споживачу не надана можливість негайно отримати під час укладання договору інформацію про послугу, він вправі вимагати від виконавця відшкодування збитків, спричинених необґрунтованим ухиленням від укладання договору, а якщо договір укладений, у розумний строк відмовитися від його виконання і вимагати повернення сплаченої за послугу суми та відшкодування інших збитків.

Можливо також ставити питання про компенсацію моральної шкоди. Виконавець, який не надав туристу повну і достовірну інформацію, несе відповідальність за недоліки послуги, які виникли в процесі її надання в результаті відсутності у туриста такої інформації.

Отже, ненадання достатньої чи надання недостовірної інформації, що мало наслідком набуття послуги, яка не має необхідних якостей, може бути ще однією підставою для розірвання договору з боку туриста.

Таким чином, необхідно, істотно конкретизувати перелік підстав для розірвання договору про реалізацію турпродукту у зв’язку із ненаданням чи неналежним наданням інформації про споживчі якості туристичного продукту і окремі туристичні послуги, а також правові наслідки такого розірвання для сторін.

Список літератури

1.Брагинский М.И., Витрянский В.В. Договорное право. Книга третья: Договоры о выполнении работ и оказании услуг. – М.: Статут, 2005. – 1055с.– С.211 – 212;

2.Цивільний кодекс України від 16.01.2003 р. №435 – IУ/ Відомості Верховної Ради України (ВВР). – 2003. – № 40 – 44. – Ст. 356.

3.Про туризм. Закон України 15.09.1995 р. № 324/95 – ВР// Відомості Верховної Ради України (ВВР). – 1995. – № 131. – Ст. 241.

4.Витрянский В.В. Существенные условия договора в отечественной цивилистике и правоприменительной практике / В.В. Витрянский. // Вестник ВАС РФ, 2002. – № 5-6. – С. 139.

5.Шендрикова А.И. Конфликт между турфирмой и потребителем: причины возникновения и способы разрешения / А. И. Шендрикова. // Туризм: право и экономика, 2003. – № 3. – С. 12.

Лесько Н. В. –
доцент кафедри права адміністративного та інформаційного права
Навчально-наукового інституту права та психології
Національного університету «Львівська політехніка»,
кандидат юридичних наук

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДІТЕЙ В МЕРЕЖІ ІНТЕРНЕТ

Дитина як повноцінний громадянин України має право бути захищеною від будь-якого негативного впливу, що може завдати шкоду її фізичному та психічному здоров'ю. В сучасному світі існує безліч небезпек для дітей і одну з серйозних загроз представляють засоби масової інформації, зокрема, Інтернет.

Загальновідомо, що сучасний технологічний розвиток на перше місце висунув проблему правового забезпечення інформаційної безпеки держави, неодмінною складовою якої є інформаційна безпека підростаючого покоління. При цьому весь суспільний обіг інформації регулюється багатьма видами соціальних норм, основними серед яких є: правові та моральні. Однак, якщо в минулі століття правовий обіг інформації охоплював лише найбільш важливу частину суспільного обігу

інформації, то в сучасних умовах назріла нагальна необхідність розширення кола інформаційно-комунікативних відносин, що мають підпадати під правове регулювання. Особливо ця проблема стосується проблем правового регулювання інформаційного обігу та комунікації у всесвітній мережі Інтернет, до якої в наш час долучаються діти вже навіть з дошкільного віку.

Слід наголосити, що складність забезпечення ефективності правового регулювання мережі Інтернет не стільки полягає у відсутності систематизованого або узгодженого законодавства, що регулює відповідні види відносин у Всесвітній мережі, скільки в об'єктивних особливостях та закономірностях функціонування самого Інтернету, які фактично «дозволяють» будь-кому анонімно робити в цій інформаційній мережі загального користування що завгодно. Саме фактична неможливість законного притягнення до юридичної відповідальності правопорушників у мережі Інтернет, що особливо проявляється на прикладі адміністративної та кримінальної відповідальності, зумовлює майже безмежну свободу дій, яку нині можна спостерігати у віртуальному кіберпросторі.

Враховуючи те, що будь-яка дитина внаслідок об'єктивної недостатньої сформованості своєї свідомості є вразливою, а отже, значно більше за дорослих та дієздатних осіб дитина піддається впливу з боку відповідних джерел інформації, в сучасних умовах вже фактично побудованого глобального інформаційного суспільства потрібно ретельно підходити до питання захисту дітей від інформації, яка може завдати шкоди їх здоров'ю та розвитку. У таких умовах особливо небезпечною для дитини є саме Всесвітня мережа Інтернет, яка і дотепер у будь-якій сучасній державі залишається фактично неконтрольованим «інформаційним майданчиком», на якому має місце абсолютно вільне поширення будь-якої інформації. Складність вирішення вказаних проблем за допомогою формально визначених правових норм полягає насамперед у тому, що в Інтернеті чи не найбільше має місце «зіткнення» протилежних інтересів відповідних суб'єктів, у зв'язку з чим навіть на сьогодні дана проблема поки що є лише предметом численних дискусій, а не практичних дій.

У цьому контексті цікавим є розгляд міжнародного досвіду спроб вирішити вказане питання на нормативно-правовому рівні. Зокрема, 3 грудня 2009 року Міжпарламентська Асамблея держав-учасниць СНД прийняла Модельний закон «Про захист дітей від інформації, що завдає шкоду їх здоров'ю та розвитку» [1], який встановлює правові та організаційні основи державної політики і міжнародного співробітництва держав-учасниць СНД у сфері забезпечення інформаційної безпеки дітей з урахуванням загальновизнаних принципів і норм міжнародного права, в тому числі закріплених в Конвенції ООН про права дитини та Модельному законі держав-учасниць СНД «Про основні гарантії прав дитини в державі».

Найважливішими, на нашу думку, положеннями цього Модельного закону є встановлення 11 принципів державної політики у сфері захисту дитини від інформації, що завдає шкоду їх здоров'ю та розвитку; нормативне визначення на міжнародному рівні таких понять, як: «вікова категорія інформаційної продукції», «вікова класифікація інформаційної продукції», «демонстрація жорстокості», «демонстрація насильства», «доступ дитини до інформації», «доступний для дитини час», «інформаційна безпека дітей», «інформаційна продукція, призначена для дітей», «інформація, що дискредитує соціальний статус сім'ї», «інформація, що завдає шкоду здоров'ю та розвитку дітей», «інформація, що провокує дітей на антисуспільні та протиправні дії», «інформація, що провокує дітей на дії, потенційно небезпечні для їх життя і здоров'я», «інформація, що провокує дітей на кримінально карані діяння (злочини)», «інформація, що включає в себе ненормативну лексику», «пропаганда антисуспільних та протиправних дій», «пропаганда насильства та жорстокості», «пропаганда злочинів» тощо; закріплення критеріїв визначення інформаційної продукції для відповідної вікової категорії дітей; визначення додаткових вимог до розповсюдження інформаційної продукції з використанням інформаційно-телекомунікаційних мереж загального користування, в тому числі через мережу Інтернет, а також додаткових вимог до розповсюдження комп'ютерних та інших електронних ігор; встановлення вимог до експертизи

інформаційної продукції з метою здійснення її вікової класифікації та маркування тощо.

В.В. Василевич з метою посилення захисту дітей від шкідливої інформації в мережі Інтернет пропонує внести зміни до Закону України «Про телекомунікації» та передбачити окремі норми, які б встановлювали відповідальність власників веб-сайтів в українській частині мережі за розміщення сайтів, що можуть містити інформацію, котра може негативно вплинути на дітей. Окрім того, науковець зазначає, що необхідно зобов'язати Інтернет-провайдерів, які надають хостинг, інформувати своїх користувачів про необхідність індексації сайту та про методику її здійснення. Вважається, що такий захід може бути ефективним, оскільки, як правило, сайти, які містять шкідливу для дітей інформацію, призначені для продажу або надання її дорослим покупцям. Подібна індексація сайтів не суперечитиме комерційним інтересам їх власників. Введення системи індексації дасть змогу легко виділити та, за необхідності, відфільтровувати в мережі інформаційну продукцію, не призначену для перегляду дітьми [2, с.4].

Слід зазначити, що в останні роки в Україні та світі почались проводитися масштабні дослідження впливу Інтернету на безпеку дітей, на їх взаємовідносини з батьками та навколишнім середовищем. Так, вперше кафедрою превентивної роботи та соціальної політики ЮНЕСКО в Україні було проведено дослідження щодо рівня знань українців про безпеку дітей в Інтернеті. Результати показали, що переважна більшість дітей (96 %) не знають про небезпеки, які існують в мережі, майже половина дітей знаходиться в потенційній небезпеці, оскільки регулярно розміщує особисті дані, а кожен п'ятий неповнолітній вже опинявся в небезпечних ситуаціях, маючи безпосередній контакт зі зловмисником [3].

Також один з найбільших мобільних операторів України ініціював проведення всеукраїнського соціологічного дослідження «Знання та ставлення українців до питання безпеки дітей в Інтернеті». Його результати показали, що 76 % батьків навіть не знають, які сайти відвідують їхні діти. Понад 28 % опитаних дітей готові надіслати свої фотокартки незнайомцям у

Мережі. 17 % повідомляли інформацію про себе і свою родину незнайомцям: адресу, телефон, графік роботи батьків [4, с. 10-11].

Ітернет-технології стали природною частиною нашого життя і діти, як найбільш активна, така, що швидко розвивається аудиторія, дуже часто раніше за дорослих знайомляться з новими можливостями, що надає всесвітня мережа. Однак для батьків головним завданням є створити такі умови, щоб Інтернет не завдавав шкоди фізичному та психічному здоров'ю дитини.

Часто підліток, як найбільш вразлива людина, поводиться в світовій мережі віктимно, ненавмисно провокуючи вчинення протиправних дій. Мова може йти про встановлення з дитиною незаконного контакту (грумінгу) з подальшими злочинними діями, кіберпереслідування, он-лайн насилля, шахрайство, порнографія та ін. Причому, іноді може мати місце і так звана «інверсія ролей», коли підліток з жертви перетворюється на порушника.

Також дуже небезпечним для психологічного здоров'я дитини є встановлення так званого небажаного контенту, під яким фахівці розуміють матеріали непридатного для дітей та протизаконного змісту – порнографічні, такі, що пропагують наркотики, психотропні речовини й алкоголь, тероризм і екстремізм, ксенофобію, сектантство, національну, класову, соціальну нетерпимість, нерівність, асоціальну поведінку, насилля, агресію, суїцид, азартні ігри, інтернет-шахрайство [5, с. 19].

Особливу увагу слід приділити комп'ютерним іграм із деструктивним, агресивним змістом, до яких в мережах дуже легкий доступ. Такі ігри суттєво впливають на свідомість дитини, вчать її вирішувати проблеми силовими методами, викликають тривожність, жорстокість, дратливість, емоційну неврівноваженість.

Виходячи із специфіки дитячого віку, слід сказати, що у профілактичній роботі з даною групою велике значення мають, насамперед, заходи не правового характеру, а педагогічні, психологічні, медичні [6, с. 69].

Науковець О.Ю. Юрченко наводить перелік головних загальних заходів, які мають здійснити батьки та педагоги для зниження рівня віктимності дітей як в звичайному житті, так і соціальних мережах: догляд за нормальним розвитком дитини з метою раннього виявлення психічних чи фізичних вад; правильне загальне та статеве виховання, формування культури спілкування; прищеплення дитині навичок поведінки в нестандартних, у тому числі віктимогених ситуаціях; закладення основ правових знань, які через засоби масової інформації та іншим способом повинні доводитись різними фахівцями – юристами, психологами, педагогами; роз'яснення батькам, що їхня поведінка є головним зразком та авторитетом для дитини і найкраща профілактика – це їх особистий приклад правильного поводження; Національною поліцією України створено телефони довіри, на які можна повідомити про веб-сайти, що пропагують насильство і жорстокість або розпалюють расову ненависть, дискримінацію, займаються створенням чи розповсюдженням дитячої порнографії, торгівлею людьми та тому подібні дії [7, с.336-338].

Все сказане дає змогу зробити висновок, що для того щоб захистити дітей від негативного впливу Інтернету, українське суспільство повинне протистояти загрозам, які несе сьогодні інформаційний простір, а державна політика має бути спрямована на підтримку духовного та культурного розвитку дітей. Хоча, всесвітня мережа є важливою складовою сучасного життя, проте через недостатнє правове регулювання захисту дітей від негативного впливу Інтернету, він стає зручним «плацдармом» для протиправної діяльності. Слід підкреслити, що Інтернет є площиною не лише для вчинення адміністративних, але й цивільних та кримінальних правопорушень. Єдиним шляхом виправлення ситуації є якомога скоріше внесення змін і доповнень у чинне законодавство.

Список літератури

1. Про захист дітей від інформації, що завдає шкоду їх здоров'ю та розвитку : Модельний закон. [Електронний ресурс]. – Режим доступу : http://jurconsult.net.ua/zakony-stran-sng.

2. Василевич В. В. Зарубіжний досвід кримінологічної політики захисту прав потерпілих від поширення дитячої порнографі ї у мережі

Інтернет / В. В. Василевич // Часопис Академії адвокатури України. – 2013. – № 3. – Режим доступу: http://nbuv.gov.ua.

3. Чачанидзе І. Интернет: Правила безопасности / І. Чачанидзе. [Електроний ресурс]. – Режим доступу: // http://www.my-baby.info/news.

4. Голіна В. Проблеми боротьби зі злочинністю неповнолітніх з психічними аномаліями / В. Голіна, В. Ємельянов, П. Петрюк // Право України. – 2005. – № 10. – С. 74–76.

5. Литовченко І. Діти в Інтернеті: як навчити безпеці у віртуальному світі: посібник для батьків / І. Литовченко, С. Максименко, С. Болтівець та ін.. – К. : ТОВ «Видавни-чий будинок «Аванпост-Прим»«, 2010. – 48 с.

6. Веселуха В. Значення віктимологічної профілактики в системі запобігання злочинам / В. Веселуха // Право України. – 1999. – № 10. – С. 67–73.

7. Юрченко О.Ю. Проблеми безпеки дітей в соціальних мережах та Інтернеті (віктимологічний аспект) / О.Ю. Юрченко // Порівняльно-аналітичне право : електрон. фахове наук. видання. – 2013. – № 3–1. – С. 336–338.

Ортинська Н.В. –
доцент кафедри адміністративного та інформаційного права
Навчально-наукового інституту права та психології
Національного університету «Львівська політехніка»,
кандидат юридичних наук

ІНТЕРНЕТ ТА НЕПОВНОЛІТНІ: СУЧАСНІ ПРАВОВІ ПРОБЛЕМИ

Зростання ролі соціально-комунікативних практик Інтернету має значний вплив на поведінку цієї категорії осіб. До таких практик належать блоги, соціальні мережі, мережеві групи та інтернет-товариства тощо.

Інтернет-спільноти – це такі соціальні спільноти, кожний учасник яких ідентифікує себе з цією групою і, разом з тим, має всі атрибути звичайної спільноти, проте ця група об'єднується технологіями Інтернету і взаємодіє через Інтернет у межах різних інтересів спільноти, що реалізуються у контексті ресурсів глобальної мережі. Блог як тип інтернет-спільноти має аналогічні характеристики з соціальними спільнотами, проте відрізняється специфікою у вигляді регулярно доповнюваних позначень на різноманітні теми мультимедіа.

Такого роду соціально-комунікативні практики дозволяють отримати необхідну інформацію та знання про досвід інших людей. У залежності від суті обговорюваної тематики можуть виступати як корисними, так і негативними для неповнолітнього.

Фахівці визначають багато варіантів для проявів агресії та протиправної поведінки в мережі. Р. Ковальскі, С. Лімбер і П. Агатстон виділили вісім типів поведінки, характерних для кібер-буллінгу:

1) Перепалки, або флеймінг – обмін короткими гнівними і запальними репліками між двома чи більше учасниками, використовуючи комунікаційні технології. Частіше за все розгортається в «публічних» місцях Інтернету, на чатах, форумах, дискусійних групах, інколи перетворюється в затяжну війну.

2) Нападки, постійні виснажливі атаки – найчастіше це залучення повторюваних образливих повідомлень, спрямованих на жертву (наприклад, сотні СМС-повідомлень на мобільний телефон, постійні дзвінки) з перевантаженням персональних каналів комунікації.

3) Обмовлення, зведення наклепів – розповсюдження принизливої неправдивої інформації з використанням комп'ютерних технологій. Це можуть бути і текстові повідомлення, і фото, і пісні, які змальовують жертву в шкідливій інколи сексуальній манері.

4) Самозванство, втілення в певну особу – переслідувач позиціонує себе як жертву, використовуючи її пароль доступу до її аккаунту в соціальних мережах, блогу, пошти, системи миттєвих повідомлень тощо, а потім здійснює негативну комунікацію. Організація «хвилі зворотних зв'язків» відбувається, коли з адреси жертви без її відома відправляються ганебні провокаційні листи її друзям і близьким за адресною книгою, а потім розгублена жертва неочікувано отримує гнівні відповіді.

5) Ошуканство, видурювання конфіденційної інформації та її розповсюдження – отримання персональної інформації в міжособовій комунікації й передача її (текстів, фото, відео) в

публічну зону Інтернету або поштою тим, кому вона не призначалася.

6) Відчуження (остракізм), ізоляція. У віртуальному середовищі виключення також наражає на серйозні емоційні негаразди, аж до повного емоційного руйнування дитини. Онлайн відчуження можливе в будь-яких типах середовищ, де використовується захист паролями, формується список небажаної пошти або список друзів. Кіберостракізм проявляється також через відсутність швидкої відповіді на миттєві повідомлення чи електронні листи.

7) Кіберпереслідування – це дії з прихованого вистежування переслідуваних і тих, хто тиняється без діла поруч, зазвичай зроблені нишком, анонімно, з метою організації злочинних дій. Відстежуючи через Інтернет необережних користувачів, злочинець отримує інформацію про час, місце і всі необхідні умови здійснення майбутнього нападу.

8) Хепіслеппінг – відеоролики нападів з метою ґвалтування чи його імітації. Відеоролики, розміщені в Інтернеті, можуть продивлятися тисячі людей, зазвичай без жодної згоди жертви [1].

Опитування підлітків навело нас на думку про ще одну проблему – реклама в мережі Інтернет. Банери з рекламою аморального змісту висять на сайтах будь-якого спрямування, тобто, навіть не шукаючи корисну інформацію, підліток наочно отримує інформацію неадекватного змісту. Зазвичай це стосується певних агресивних відеоігор чи ігор еротичного спрямування.

Так само легко знайти інформацію девіантного характеру. На наш запит «скінхеди» пошукова система Яндекс надала 54 тисячі відповідей, 705 тис. відповідей на запит «Як зробити бомбу в домашніх умовах» та 2 млн. відео про бійки неповнолітніх. Отож у мережі можливе пропагування антисоціальної поведінки, саме через різного роду сайти організації, що мають антидержавні чи антисоціальні цілі, поповнюють свої ряди новими членами (терористичні групи, скінхеди тощо). Вони можуть бути основним чинником з метою формування мотивації для протиправної поведінки неповнолітнього.

Глобалізоване суспільство ставить перед людиною багато викликів, на які психіка не завжди може адекватно реагувати. Тому констатуємо значний приріст агресії у всіх сферах людського існування на рівні людей, громад, народів, держав.

З погляду психології Т.В. Алексєєва і Н.І. Ковальчишина визначають агресію як мотивовану деструктивну поведінку індивіда, що суперечить заведеним правилам і нормам існування людей у соціумі, що завдає моральної, фізичної, матеріальної або психологічної шкоди іншим людям [2, с.5].

Правова природа агресії виявляється в тому, що вона є фактором, який стимулює протиправність діяння, чинником, що сприяє деформації правосвідомості та, як наслідок, неправомірній поведінці особи.

Агресія в масовій культурі активно культивується, зі швидкістю лавини збільшується кількість негативного контенту в медіа. Медіапростір пропагує агресію як засіб досягнення успіху в життя, за твердженням Е. Фромма, стає «генератором» насильства, яке виходить з екрану в життя [3].

Здавалось би, агресія є психологічною проблемою, тому вирішуватися повинна на психологічному рівні, а не правовому. На жаль, агресія підлітків вже давно переросла у вагому міждержавну проблему, на яку державно-правові інституції не можуть не реагувати. У дослідженнях [4] показано, що жертви кіберзалякування серед підлітків у 1,9 рази частіше вдаються до суїциду, отож трансформаційні процеси глобалізаційного суспільства спричинили нове соціальне явище – кіберсуїцид, тобто самогубство прямо або побічно пов’язане з online-агресією. Кваліфікація такого діяння міститься в ст. 120 Кримінального кодексу України, де вказано, що Доведення особи до самогубства або до замаху на самогубство є наслідком жорстокого з нею поводження, шантажу, примусу до протиправних дій або систематичного приниження її людської гідності. Систематичне приниження людської гідності полягає, зокрема, у багаторазових образах, глумі над потерпілим, цькуванні, поширенні наклепницьких вигадок, іншому принизливому ставленні до потерпілого. Законодавець не вказує, в який спосіб можуть бути здійснені такі дії, тому кіберагресія повноправно може вважатися таким діянням.

Зауважимо, що частина 3 ст. 120 Кримінального кодексу України визначає, якщо вищевказане діяння було вчинене щодо неповнолітнього, то карається позбавленням волі на строк від семи до десяти років.

Для підлітків характерна групова агресія, що спричиняє в майбутньому групові правопорушення. Формуючись у свого роду колектив, вони за підтримки групи переступають грань, що веде до злочинних дій. Фахівці виділяють три етапи формування такої агресивної групи.

На першому етапі негативного розвитку групи відносини підлітків у ній є неглибокими, випадковими, групи аморфні, визнаного ватажка немає. Членами такої групи є «важкі» підлітки, яким властиві негативне ставлення до навчання, недисциплінованість, епізодична девіантна поведінка (паління, азартні ігри, вживання спиртних напоїв, наркотиків, дрібні крадіжки, бродяжництво).

На другому етапі, якщо група зберігається, вона стабілізується, численність її зменшується, у ній з'являється ватажок. Негативне ставлення до навчання перетворюється на вороже ставлення до педагогів, кращих учнів, загалом до школи. Члени таких груп уже регулярно скоюють не тільки аморальні вчинки, але й серйозні правопорушення: крадіжки, хуліганські дії.

На третьому етапі деформації група починає жити за власними вузькогруповими нормами, що виправдовують асоціальну поведінку. Лідером групи здебільшого стає особа, що відбула покарання. Спостерігається остаточний розрив із школою, девіантна поведінка перетворюється на злочинну (розкрадання, грабежі, злісне хуліганство, викрадення автотранспортних засобів тощо).

Медіапростір на сьогодні займає значне місце у суспільному житті неповнолітніх. Сучасний медіапростір містить значну кількість сцен насильства, не здійснює градацію між дорослим та дитячим телевізійним продуктом та подає девіантну поведінку як соціальну норму, не вказуючи на негативні прояви агресивних дій. Такий продукт є одним із основних соціальних факторів стимулювання агресивної поведінки неповнолітніх, яка зростає швидкими темпами в

сучасному суспільстві та стає проблемою для всього світового співтовариства. Ми переконані, що подібний стан вимагає комплексного психологічного, педагогічного та правового розв'язання. На нашу думку, з боку держави необхідна реалізація наступних заходів:

– активізація діяльності компетентних органів державної влади, щодо усунення з медіапростору особливо небезпечних телевізійних продуктів;

– пропаганда правових знань підлітків, створення медіапродукту, що націлене на патріотичне, соціально-правове, моральне виховання неповнолітніх, повагу прав та свободи вибору іншого, толерантності та гуманізму;

– комплексна робота педагогічних працівників, батьків, учнів, громади, релігійних та громадських організацій щодо усунення проявів агресії неповнолітніх, антисоціальної поведінки підлітків, буллінгу тощо, опитування учнів про розповсюдженість антисоціальних проявів агресії, обговорення проблем агресії на всіх рівнях, посилення спостереження вчителів за неповнолітніми;

– навчання неповнолітніх соціальним правилам взаємодії, комунікації, тренінгів щодо підвищення рівня свідомості, їх правової культури способів придушення агресії, самодисципліни і саморегуляції та правових можливостей реакції на протиправний казус загалом;

– підвищення рівня профілактичної роботи щодо виявлення загрозливих факторів в оточенні неповнолітніх.

Список літератури

1.Kowalski Robin M. Cyber bulling: bulling in the digital age / Robin M. Kowalski, Susan P. Limber, Patricia W. Agatston. – Oxford: Blackwell Publishing Ltd, 2008. – 218 p.

2.Алексеєва Т. В. Психологія підліткової злочинності : навчальний посібник / Т. В. Алексєєва, Н. І. Ковальчишина. – Донецьк : Ноулідж, 2010. – 335 с.

3.Фромм Э. Величие и ограниченность теории Фрейда / Э. Фромм. − М.: ООО «Фирма «Издательство АСТ», 2000. − 448 с.

4.Найдьонова Л. А. Агресивний кібер-простір чи агресивні користувачі? – психологічні засади долання кібер-буллінгу / Л. А. Найдьонова // Психологічні перспективи. Спеціальний випуск. Проблеми кіберагресії / Інститут соціальної та політичної психології НАПН України. − 2012. Т. 2. – С. 83-92.

Савінова Н. А. –
Науково-дослідний інститут інформатики і права
Національної академії правових наук України,
доктор юридичних наук, старший науковий співробітник
Розенфельд М.Д. –
студентка третього курсу факультету психології
Київського національного університету ім. Т. Шевченка

ДЕВІАЦІЇ АГРЕСІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ: СПРОБА СОЦІАЛЬНО-ПСИХОЛОГІЧНОЇ ОЦІНКИ

Однією з важливіших платформ здійснення соціальних комунікацій в Інформаційному суспільстві сьогодні стали соціальні мережі. Переважно «Facebook» та «Tweeter», а також «LiveJournal», як міжнародні площадки, останнім часом перебувають на зльоті популярності, адже дають значно ширші можливості політичних, полярних і відносно інтелектуальних дискусій, в порівнянні з такими «однополярними» площадками як «Однокласники» (РФ) чи орієнтованими на віковий критерій – «ВКонтакте» (тінейджер+), тощо.

У той же час, саме ці площадки виступають тим самим краєм леза, яке, з одного боку, демонструє межу протистояння таборів групової комунікації та підтримки такої (якуайменше через «Like»), а з іншого – і місцем групування основних, нерідко примарних, ідей, і кабінетом психоаналітика, і фабрикою штампування конформізму, який формується реальними та фейковими лідерами.

Фактично, переважна більшість первинних повідомлень в соціальних мережах носять девіантний характер, за умови, що вони не рекламні, чи не «офіційні повідомлення». Саме такі «чіпляють» комунікатора сміливістю, нестандартністю, яскравою позицією – тобто, є саме «девіаційними» – відмінними від загальних, звичних, притаманних, а іншими словами – застарілих форм комунікації, де звично говорити «в тренді», де підтримується «генеральна лінія» основних комунікаторів.

У перекладі з латини девіація – відхилення від шляху.[8] І хоча визначення її на рівні соціологічних словників

[8] Словарь иностранных слов. – М.: Русский язык, 1989. – С. 151.

притримуються визначення такої як «відхилення від норми», сучасні підходи девіантологів значно глибше і конструктивніше оцінюють девіації як соціально необхідне явище що сприяє розвитку суспільства.

Першим з девіантологів, хто оцінив соціально необхідне і конструктивне значення девіацій був і лишається Я. І. Гілінський, який писав: «Девіації (флуктуації у неживій природі, мутації – у живій) є всезагальною формою, механізмом, способом мінливості, і, відповідно, і життєдіяльності, розвитку кожної системи».[9] Під девіатною, тобто, такою, що відхиляється від норми, він поведінкою розуміє: «1) вчинок, дії людини, які не відповідають відповідним офіційно встановленим або таким що фактично склалися в даному суспільстві нормам (стандартам, шаблонам); 2) соціальне явище, виражене у масових формах людської діяльності, яке не відповідає офіційно встановленим або таким, що фактично склалися в даному суспільстві нормам суспільства (стандартам, шаблонам)».[10]

Враховуючи той фактор, що саме нестандартні і незвичні для попередніх форм комунікацій можливості соціум отримав саме завдяки соціальним мережам – самі по собі вони є девіантною формою комунікації. Утім і можливості, які вони забезпечують, і складність моніторингу, і відверта можливість приховувати реальне ім'я авторів «постів» нерідко обумовлюють в соціальних мережах безлічі агресивних і відверто деструктивних інформаційних атак, які, за конструкцією соціально мережі підхоплюються, коментуються, тиражуються (поширюються) відбувається інтеракція (взаємодія).

Але особливість інтеракції в соціальних мережах полягає у тому, що будь-яка реакція є інтеракцією: позитивна, чи негативна, але вона «спацбовує» на відповідну інформацію якнайменше «кліком» миші – балом, оцінкою, ставленням. При цьому, переважна більшість комунікаторів не замислюється над тим, що особливість знеособлено дистанційно комунікації інша.

---

[9] Гилинский Я.И. Социология девиантного поведения как специальная социологическая теория // СоцИс. – 1991. – №4. – С. 74.

[10] Там само. – С. 74.

Як вказує О. Марков, фахівець у галузі біологічної еволюції, «Інтернет – комунікативне середовище, яке зовсім не схоже на те, що існує в природі. Тут ми модемо тільки зі здивуванням спостерігати, як наші психологічні риси, що розвивалися в інших умовах проявляють себе в цих нових умовах і незвичних обставинах. В соціальних мережах ми не бачимо співрозмовника, не бачимо його, лише читаємо, що він написав, і тому у нас не включаються механізми емпатії, здатності приймати і відчувати чужі емоції. /…/ в Інтернеті зеркальі нейрони не працюють, ми бачимо лише голий смисл. Якщо цей смисл нам не подобається, то співрозмовник моментально потрапляє в ранг чужинця, ворога, і на нього можна виливати свій гнів скільки завгодно».[11] Утім, чи небезпечні такі «віртуальні» агресії на фоні того, що, Інтернет, і соціальні мережі, як раніше, переважно, неінтерактивне телебачення, виступало засобом каналізації агресії, турбот, страхів?

Фактично, навіть, за умови всіх нарікань щодо агресії, «розпалювання воржнечі» тощо, соціальні мережі виступають не засобом породження, а місцем «заземлення агресії», де особа може висловитися, знайти однодумця, а далі, випустивши агресію в поле невідомих, або відносно знайомих персонажів, займатися своїми побутовими справами.

Цікаво, що ще у 1998 р. О. С. Осіповою була висловлена така теза: «деаіантна поведінка деструктивної спрямованості – вчинене людиною або групою людей соціальних дій, що відхиляються від домінуючих в соціумі (окремій соціальній групі, страті) соціокультурних очікувань і норм, загальноприйнятих правил виконання соціальних ролей, *що тягнуть за собою зниження темпів розвитку суспільства: руйнування енергетичного потенціалу окремих особистостей і суспільства в цілому*. Руйнівну (асоціальну) девіацію не можна ототожнювати лише зі злочинністю»[12] (*виділено курсивом нами,* Н.С., М.Р.). Вказаний автор визначає і альтернативу – «творчі

[11] Марков А. Чем человеческая агрессия отличается от агрессии животных // Портал «Афиша Daily» / https://daily.afisha.ru/

[12] Осипова О.С. Девиантное поведение: благо или зло? // Социологические исследования. 1998. № 9. С. 106-109 – С. 107.

девіації» (за Я.І.Гілінстким – «девіації творчості», Н.С., М.Р.). О. С. Осіпова під останніми розуміє соціальні новації, нововведенення – «соціально значущі в діях людини відхилення від загальновизнаних норм поведінки, які визначають найбільш прогресивний в енергетичному, а, відповідно, в адаптаційному плані, вектор еволюційного розвитку суспільства».[13]

Утім, якщо самі соціальні мережі, за цим визначенням, не можуть бути віднесені аж ніяк до деструктивних девіацій, адже їх позитивна для суспільного розвитку очевидна, слід звернути увагу на реалізацію можливостей людини у них, яка, відповідно, певним час також була девіантною, аж доки не стала масовою, традиційною, повсякденною.

Можливість моделювання віртуальної комунікативної реальності особами самостійно з використанням соціальних мереж, в яких з соціальною користю може каналізуватися агресія, є позитивним фактором, додатковим засобом зняття психологічної напруги.

Феномен внутрішньої свободи людини, притаманний Інформаційному суспільству, виражається у випадку будь-якої девіації у соціальній мережі через можливість варіативної участі, висловлювання соціально очікувано або опозиційної позиції, які можуть бути агресивними, у тому числі. Але, переважно, мережева агресія – фактор позитивний, працюючий на мінімізацію агресії в реалії.

У той же час, агресія, у якій міститься склад певного правопорушення, за умови наявності складу злочину у її прояві і у мережі, підлягає юридичній відповідальності. В соціальній мережі, переважно, це – прямі заклики до вчинення злочинів, адже вчинення злочину в соціальній мережі, з урахуванням декриміналізації у більшості цивілізованих країн світу «Наклепу» та «Образи» фактично неможливо. Крім того, спірним постає питання щодо «Вільних зон Інтернет», але, як вбачається з оцінок експертів, на користь визнання на міжнародному рівні таких зон і віднесення до низ соціальних мереж, як гарантій «свободи вираження поглядів» все ближче.

[13] Осипова О.С. Девиантное поведение: благо или зло? // Социологические исследования. 1998. № 9. С. 106-109 – С. 107.

Але говорити про суцільну користь можливості каналізації агресії в соціальних мережах було б відверто однобоко. Так, це – корисно для самого агресора, і, об'єктивно корисно для суспільства, яке позбавляється від реальної агресії, яка каналізується. Але – «при інших рівних», адже в умовах напруги у суспільстві (реальне соціальне протистояння, революції, війни) агресія в соціальних мережах може виступати каталізатором збудження реальної агресії.

Крім той, слід враховувати той фактор, що агресія в соціальних мережах є своєрідним «лакмусовим папером» настроїв. Саме моніторинг рівня агресії в соціальних мережах є самостійним завданням розвідувальних заходів гібридних війн, результати якого дають підстави для проведення інформаційних та економічних операцій на територіях супротивника.

Отже, резюмуючи висловлене, акцентуємо увагу на наступному:

1. Соціальні мережі є одним з найбезпечніших сьогодні засобом каналізації агресії людини. Завдяки ним, агресивні прояви «випускаються» людиною у віртуальний простір, внаслідок чого психічна напруга знижується, і, відповідно, на рівні сім'ї, спільноти, суспільства агресія мінімізується. В цьому полягає основний позитивний аспект агресії в соціальних мережах.

2. В умовах соціальної напруги агресія в соціальних мережах, і, зокрема, спрямована, маніпулятивна, може виступати каталізатором агресивної інтеракції в реальності.

3. В умовах гібридної війни агресія в соціальних мережах є предметом дослідження, концентрація якої демонструє характер спрямування інформаційних атак супротивника з метою досягнення цільової аудиторії у разі здійснення дискредитації влади або певних лідерів чи груп, провокацій геноциду, розпалювання расової, міжетнічної, релігійної ворожнечі.

Спасова К. І. –
аспірант кафедри цивільного права,
фахівець 3-ї категорії науково-дослідної частини
Національного університету «Одеська юридична академія»

ВІДШКОДУВАННЯ ШКОДИ, ЗАВДАНОЇ ЦИВІЛЬНИМИ ПРАВОПОРУШЕННЯМИ У СФЕРІ ІТ-ВІДНОСИН

Відносно новим і дуже важливим напрямком розвитку сучасної України та й багатьох інших країн світу, є інтеграція в європейський і світовий інформаційний простір. На сьогоднішній день існують стрімкі процеси вдосконалення глобального інформаційного простору, що собою являє розвиток «інформаційної особистості», розвиток глобального інформаційного суспільства, які варто розглянути як одну з сучасних тенденцій трансформації суспільства, який має неабиякий вплив на їх становлення.

Саме суспільні перетворення, що відбуваються у світі, переоцінка суспільних пріоритетів і створює підвищену зацікавленість для закріплення правових гарантій забезпечення відшкодування збитків, які все більше завдаються цивільними правопорушеннями у сфері ІТ-відносин [1, с. 354]. На сьогоднішній день немає єдиної системи нормативно-правових актів, які врегулювали би ті чи інші ІТ-відносини, адже коло їх регулювання достатньо об'ємне. Тому для початку необхідно визначити коло відносин які складають предмет ІТ-права, а вже потім зазначимо безпосередньо питання, що стосуються відшкодування шкоди за цивільно-правові порушення в ІТ-відносинах.

Отже, дуже багато фахівців розглядають ІТ-право у вузькому розумінні, не висвітлюючи його в цілому, в сукупності, а виокремлюють лише деякі його складові (так званні інститути), що його забезпечують це інформатика, комп'ютери, засоби зв'язку і їх системи тощо, коли до предмету правого регулювання ІТ-права, на думку Л.П. Коваленко, входять не тільки суспільні відносини, що зазначенні вище, а й вся сукупність цих відносин в інформаційній сфері, що включає

в себе увесь цикл обігу інформації: її створення, перетворення, в тому числі й засобами зв'язку і телекомунікації, використання й знову створення інформації, здійснюваної на основі сучасних засобів мікропроцесорної та обчислювальної техніки, а також на базі різноманітних засобів інформаційного обміну [2, с. 149]. Виходячи з цього поняття слід звернути увагу на те, що тут переважають більше публічно-правові елементи, а варто було би досліджувати ІТ-право, з приватно-правової точки зору, як сукупність норм, що регулюють опосередковують діяльність по забезпеченню безпеки інформаційних технологій та інформаційної активності в мережі Інтернет [3]. Також слід зазначити, що ІТ-відносини регулюються цивільним, кримінальним, адміністративним, господарським правом тощо, але зараз найбільш актуальним для нас є все ж таки регулювання зазначених правовідносин цивільним правом.

Розглянемо трохи ближче відшкодування шкоди, завданої цивільними правопорушеннями у сфері ІТ-відносин, адже на фоні стрімкого розвитку інформаційного права, постає питання, захисту прав та інтересів, закріплення правових гарантій, забезпечення недоторканості та не порушення прав фізичних та юридичних осіб.

Для початку зазначимо, що відшкодування шкоди – це такі цивільно-правові зобов'язання, в яких потерпіла сторона (кредитор) має право вимагати від боржника (заподіювача шкоди) повного відшкодування протиправно заподіяної шкоди шляхом надання відповідного майна в натурі або відшкодування збитків. Характеризуючи коло ІТ-відносин, з яких виникають зобов'язання з відшкодування шкоди, то є необхідність зазначити деякі з них, а саме:

– відшкодування шкоди за порушення авторських прав в мережі Інтернет;

– відшкодування шкоди пов'язаних з неправомірним використанням товарних знаків та доменних імен;

– відшкодування шкоди за розміщення недостовірної інформації на сайті (захист ділової репутації), звинуваченням в «спам», звинуваченням в порушеннях чинного законодавства про зв'язки;

– відшкодування шкоди завдану покупцям інтернет-магазинів;

– відшкодування шкоди у зобов'язаннях, що виникають з порушення договорів, таких як:

- ✓ договорів, необхідних для роботи ІТ-компаній;
- ✓ агентських договорів, включаючи договори з іноземними контрагентами;
- ✓ договорів підряду на створення і підтримку сайтів;
- ✓ ліцензійних договорів
- ✓ договорів на ІТ аутсорсинг;
- ✓ дистриб'юторських угод тощо.

Специфіка відшкодування шкоди завданої цивільними правопорушеннями у сфері ІТ-відносин може бути встановлена інтерпретацією її основних рис в «інформаційному ракурсі». По-перше необхідно визначитися з поняттям, що таке «інформаційне правопорушення»? Під яким слід розуміти протиправне діяння, яке виражається в порушенні цивільних інформаційних прав та невиконанні чи неналежному виконанні цивільних інформаційних обов'язків, передбачених договором та/або актом законодавства, що призводить до моральної та/або матеріальної шкоди, збитків, інших витрат [4, с. 38].

Порушення інформаційних прав та обов'язків можуть мати як майновий так і немайновий характер, тому для відшкодування шкоди дуже важливим моментом є встановлення категорій осіб, яким може бути нанесена немайнова шкода інформаційним правопорушенням. Керуючись роз'ясненням Пленуму Верховного Суду України «Про судову практику в справах про відшкодування моральної (немайнової) шкоди» [5], встановлюється наступне:

– можуть зазнавати як фізичні так і юридичні особи (моральну шкоду як втрату немайнового характеру внаслідок моральних чи фізичних страждань або інших негативних явищ, заподіяних незаконними діями чи бездіяльністю суб'єктів цивільного правопорушення у сфері ІТ-відносин);

– можуть зазнавати лише юридичні особи (немайнову шкоду як втрату немайнового характеру, що настала у зв'язку з приниженням ділової репутації, посяганням на фірмове

найменування, товарний знак, виробничу марку, розголошенням комерційної таємниці, а також вчиненням дій на зниження престижу чи підриву довіри до діяльності потерпілого) [4, с. 39].

Однією з основних рис зобов'язань з відшкодування шкоди є відновлювально-компенсаційна спрямованість, під якою розуміється повернення становища потерпілого до того, яким воно було на момент вчинення правопорушення, а якщо не можливо це здійснити, то потерпілому компенсуються усі витрати, що були завданні інформаційним правопорушенням у майновій формі.

Розглянемо дану рису на прикладі рішення Печерського суду м. Києва від 16.11.2012 р. у справі ТОВ «Видавнича Організація «Юстініан» та ПП «Українська Правда» про захист честі, гідності та ділової репутації, спростування недостовірної інформації яка була розміщення на сайті. У ході розгляду справи було встановлено, що власником домену є і власником веб-сайту і несе правову відповідальність за всі матеріали, розміщенні на ресурсі, оскільки завдяки власникові було створено технологічну можливість й умови для розміщення і поширення недостовірної інформації [6, с. 34]. Так як позивач висунув вимоги, щодо відшкодування ще і моральної шкоди, то суд керуючись пунктом 27 постанови Пленуму яка передбачає, що способами захисту гідності, честі чи ділової репутації від поширення недостовірної інформації можуть бути, крім права на відповідь та спростування недостовірної інформації, також і вимоги про відшкодування збитків та моральної шкоди, заподіяної такими порушеннями як фізичній, так і юридичній особі. Зазначені вимоги розглядаються у відповідності до загальних підстав щодо відповідальності за заподіяння шкоди. Вирішуючи питання про відшкодування моральної шкоди, суд враховував роз'яснення, що містяться в постанові Пленуму ВСУ [5].

Це одне з небагатьох рішень суду в якому задовольнили, хоч частково, вимоги щодо відшкодування моральної шкоди завданої інформаційним правопорушенням. На сьогоднішній день існує проблема захисту порушених цивільних прав інформаційними проступками, відновлення фундаментальних для сучасного суспільства інформаційних прав як майновими,

так і спеціальними немайновими засобами, яку слід виправляти, адже зі стрімким розвитком ІТ та інформаційного суспільства, інформаційної культури слід вдосконалювати і ІТ-право, ІТ-законодавство і діяльність судової системи.

Список літератури

1. Відшкодування моральної та матеріальної шкоди : навч. посібн. / М.К. Галянтич, А.Б. Гриняк, А.І. Дрішлюк, Т.С. Ківалова [та інш.] ; за ред.. М.К. Галянтича. – К. : Юрінком Інтер, 2011. – 624 с.
2. Коваленко Л.П. Інформаційне право в Україні / Л.П. Коваленко // Проблеми законності. – №119. – 2012. – С. 148-156.
3. Харитонова О.І. Проблемні питання визначення системи (структури) ІТ-права.
4. Тихомиров О.О. Цивільно-правова відповідальність за інформаційні правопорушення: загальнотеоретичні аспекти / О.О. Тихомиров // Порівняльно-аналітичне право. – №1. – 2015. – С. 37-40
5. Про судову практику в справах про відшкодування моральної (немайнової) шкоди : Постанова Пленуму Верховного Суду України № 4 від 31.03.1995 р. [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/v0004700-95
6. Тарас Бачинський Основи ІТ-права / Тарас Бачинський. – Львів : Апріорі, 2016. – 136 с.
7. Кафтя А.А. Інформаційне право як галузь права: плюралізм наукових підходів / А.А. Кафтя // Право і суспільство. – №5-2. – 2015. – С. 148-153.

Столярчук А.Л. –
аспірант кафедри цивільного права та процесу
Львівського національного університету ім. І. Франка

ОСОБЛИВОСТІ ВНЕСЕННЯ МАЙНОВИХ ПРАВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В СТАТУТНИЙ КАПІТАЛ ГОСПОДАРСЬКИХ ТОВАРИСТВ

Розвиток суспільства сьогодні, як ніколи залежить від інновацій. Інформаційні технології в 21 столітті розвиваються з неймовірною швидкістю, тим самим змінюючи умови життя людей, що в свою чергу спричиняє їх значимість в житті кожного. Відтак в сучасній економіці на перші ролі сьогодні

виходить інтелектуальний капітал який формують нематеріальні активи.

Зростання конкурентоспроможності підприємств передбачає ефективне використання нематеріальних активів, частка яких у структурі активів суб'єктів підприємницької діяльності постійно зростає. Наявність нематеріальних активів у складі ресурсів підприємства збільшує ринкову вартість підприємств та підвищує їх інвестиційну привабливість. Найпопулярнішими нематеріальними активами які можуть бути внеском у статутний капітал юридичної особи є майнові права інтелектуальної власності.

Статутний капітал товариства формується за рахунок вкладів учасників. Відповідно до ст. 13 закону "Про господарські товариства" [3], вкладами до статутного (складеного) капіталу господарського товариства можуть бути гроші, цінні папери, інші речі або майнові чи інші відчужувані права, що мають грошову оцінку, якщо інше не встановлено законом. Таке ж формулювання передбачається ч. 2 ст. 115 Цивільного кодексу України [1].

У ст. 86 Господарського кодексу України [2] зазначено, що вкладами учасників та засновників господарського товариства можуть бути будинки, споруди, обладнання та інші матеріальні цінності, цінні папери, права користування землею, водою та іншими природними ресурсами, будинками, спорудами, а також інші майнові права (включаючи майнові права на об'єкти інтелектуальної власності), кошти, в тому числі в іноземній валюті.

Отже, аналізуючи наведені вище законодавчі норми, майнові права (включаючи майнові права на об'єкти інтелектуальної власності) можуть бути вкладом до статутного капіталу товариства, за умови що, вони мають грошову оцінку та можуть бути відчуженими.

Саме через невідчужуваність особистих немайнових прав інтелектуальної власності (ч. 4 ст. 423 ЦК України) вони не можуть бути предметом вкладу до статутного капіталу юридичної особи.

Майнові права інтелектуальної власності виникають щодо об'єктів інтелектуальної власності, до яких згідно із ст. 420 ЦК

України належать: літературні та художні твори; комп'ютерні програми; компіляції даних (бази даних); виконання; фонограми, відеограми, передачі (програми) організацій мовлення; наукові відкриття; винаходи, корисні моделі, промислові зразки; компонування (топографії) інтегральних мікросхем; раціоналізаторські пропозиції; сорти рослин, породи тварин; комерційні (фірмові) назви, торговельні марки (знаки для товарів і послуг), географічні зазначення; комерційні таємниці.

Відповідно до ст. 424 ЦК України майновими правами інтелектуальної власності є:

1) право на використання об'єкта права інтелектуальної власності;

2) виключне право дозволяти використання об'єкта права інтелектуальної власності;

3) виключне право перешкоджати неправомірному використанню об'єкта права інтелектуальної власності, зокрема і забороняти таке використання;

4) інші майнові права інтелектуальної власності, встановлені законом.

Отже, згідно ч. 3 ст. 424 ЦК України майнові права інтелектуальної власності можуть відповідно до закону бути вкладом до статутного капіталу юридичної особи. Проте, слід зазначити, що не всі права інтелектуальної власності можуть бути вкладом до статутного капіталу. Для прикладу законом (ч. 2 ст. 490 ЦК України) чітко встановлено, що майнові права інтелектуальної власності на комерційне найменування передаються іншій особі лише разом з цілісним майновим комплексом особи, якій ці права належать, або його відповідною частиною.

Крім цього, слід зазначити, що формування статутного капіталу юридичних осіб не завжди допускається за рахунок внесення майнових прав інтелектуальної власності. Зокрема, законами «Про банки і банківську діяльність», «Про фінансові та державне регулювання ринків фінансових послуг», «Про страхування» передбачено, що статутний капітал банків, інших фінансових установ та страховиків має бути сплачений у грошовій формі. Тобто законодавець встановив вимоги для

окремих видів компаній, статутний капітал яких не може формуватися за рахунок прав інтелектуальної власності.

Оскільки в цивільному та господарському законодавстві не визначено порядку передання засновниками їх майнових прав інтелектуальної власності для формування статутного капіталу товариства, тому серед науковців існують різні позиції.

В. М. Кравчук вважає, що для передачі прав інтелектуальної власності доведеться не лише передбачити такий вклад в установчому документі, але й згодом, після реєстрації товариства, укласти відповідний договір. За таких умов зобов'язання учасника зробити вклад матиме характер попереднього, тобто обіцянки [6]. З даним висновком можна погодитись з огляду на те, що згідно із ст. 1107 ЦК України внесення до статутного капіталу вкладу у вигляді об'єктів інтелектуальної власності може бути зроблене виключно шляхом укладення письмового договору (з винятками, які прямо передбачені законом). В іншому випадку, у разі недодержання письмової форми договору щодо розпоряджання майновими правами інтелектуальної власності такий договір є нікчемним.

Пленум Вищого господарського суду України в п. 5.1. Постанови Пленуму № 12 від 17.10.2012 року займає таку ж точку зору і звертає увагу на те, що за змістом статей 424 і 426 ЦК України, суб'єкт права інтелектуальної власності вправі у будь-який визначений законом спосіб використовувати об'єкт цього права. У разі внесення майнового права до статутного капіталу юридичної особи, окрім зазначення про це в установчому договорі, необхідне укладення окремого договору про передання виключного права, а у випадках, передбачених законом, – також і державна реєстрація такого окремого договору [8].

Постає запитання, які саме майнові права інтелектуальної власності та на підставі якого договору можна їх внести до статутного капіталу товариства. О.О. Тверезенко, думку якої ми розділяємо, робить висновок, що вкладом до статутного капіталу можуть бути майнові права у своїй сукупності, тобто право використовувати об'єкт права інтелектуальної власності, виключне право дозволяти використання об'єкта права інтелектуальної власності та виключне право перешкоджати

неправомірному використанню такого об'єкта. Оскільки в такому випадку передаються всі майнові права, то фактично відбувається відчуження майнових прав інтелектуальної власності. Таке відчуження відбувається на підставі ст. 427 та ст. 1113 ЦК України шляхом укладення договору про передання виключних майнових прав інтелектуальної власності [7, с. 56].

Під час визначення правової підстави внесення до статутного капіталу господарського товариства майнових прав інтелектуальної власності насамперед слід враховувати законодавче положення ст. 115 ЦК України про те, що господарське товариство є власником майна, переданого йому учасниками товариства у власність як вклад до статутного (складеного) капіталу. У ст. 85 ГК України зафіксоване подібне положення, що господарське товариство є власником майна, переданого йому у власність засновниками й учасниками як внески. Як випливає зі змісту ч. 1 ст. 316 ЦК України власником є особа, яка має права на майно, яке вона здійснює відповідно до закону за своєю волею та незалежно від волі інших осіб.

Отже, аналізуючи положення ст. ст. 1108 та 1109 ЦК України, можна прийти до висновку, що в разі укладання ліцензійного договору чи видачі ліцензії відбувається не відчуження майнових прав інтелектуальної власності, а їх надання іншій особі на певній період в обмеженій сфері. Таким чином, як зазначає О.О. Тверезенко, ліцензіат не стає власником прав на відповідний об'єкт інтелектуальної власності; ліцензіату не відчужуються (не переходять) майнові права інтелектуальної власності на такий об'єкт. У випадку внесення майнових прав інтелектуальної власності до статутного капіталу господарського товариства останнє стає власником прав на відповідний об'єкт. Для цього необхідно укласти договір про передання (відчуження) майнових прав інтелектуальної власності на такий об'єкт [7, с. 56].

Ще одним важливим питанням, яке потребує детального розгляду є оцінка вкладів до статутного капіталу у вигляді прав інтелектуальної власності. Згідно із ч. 2 ст. 115 ЦК України, грошова оцінка вкладу учасника господарського товариства здійснюється за згодою учасників товариства, а у випадках, встановлених законом, вона підлягає незалежній експертній

перевірці. Як випливає із змісту даного положення, згода щодо визначення вартості вкладу надається саме учасниками товариства, а не загальними зборами учасників, тобто згоду щодо оцінки має дати кожен учасник особисто, на відміну від простої більшості від загальних зборів.

Дане положення особливо важливе для застосування під час збільшення статутного капіталу, оскільки саме за таких умов може відбутись підміна понять із загальними зборами, в той час як при створенні товариства очевидним є той факт, що згода щодо оцінки вкладів вимагається від всіх засновників особисто.

Отже, по суті, засновники (учасники) товариства самостійно на власний розсуд визначають вартість вкладу, зокрема майнових прав інтелектуальної власності. Адже закон не встановлює порядку чи критеріїв, якими мали б керуватись учасники під час оцінки вкладів. В даній випадку може виникнути ситуація, коли учасники навмисно оцінять вклад у вигляді майнових прав інтелектуальної власності (чи будь-який інший вклад) за ціною, що явно завищена і не відповідає економічній цінності даного внеску. Це може бути зроблено задля штучного роздування статутного капіталу з метою підвищення ділової репутації та створення іміджу потужного товариства. І якраз немайнові права інтелектуальної власності підходять для такої недобросовісної поведінки найкраще.

Проте існують випадки, коли оцінка вкладів підлягає обов'язковій перевірці незалежним експертом, така перевірка здійснюється після оцінки вкладу самими учасниками з метою підтвердження справедливості такої оцінки. Відповідно до ст. 7 Закону України «Про оцінку майна, майнових прав та професійну оціночну діяльність в Україні» [4], визначення вартості внесків учасників та засновників господарського товариства, якщо до зазначеного товариства вноситься майно господарських товариств з державною часткою (часткою комунального майна), а також у разі виходу (виключення) учасника або засновника із складу такого товариства.

Крім цього незалежна експертна оцінка вимагається при здійсненні іноземної інвестиції у вигляді майнових прав інтелектуальної власності як внеску у статутний капітал товариства. За таких умов, згідно ст. 2 закону України «Про

режим іноземного інвестування» [5], їхня вартість у конвертованій валюті має бути підтверджена згідно з законами (процедурами) країни інвестора або міжнародними торговельними звичаями, а також підтверджена експертною оцінкою в Україні, включаючи легалізовані на території України авторські права, права на винаходи, корисні моделі, промислові зразки, знаки для товарів і послуг, ноу-хау тощо.

В.М. Кравчук вважає, що оцінка вкладів належить до виключної компетенції учасників, тому, на його думку, їх рішення не може бути оскаржене у судовому порядку. Не ґрунтуються на законі також і вимоги учасника про переоцінку вкладу у зв'язку із їх несправедливою, на його думку, початковою оцінкою. Також, згода з оцінкою вкладів вимагає певної фіксації. Під час створення товариства учасники вправі домовитися про оцінку негрошових вкладів і закріпити її в протоколі установчих зборів або у засновницькому договорі (статуті). Це повинно бути одноголосне рішення [6].

Слушну позицію висловив у листі № 6279 від 14.09.2004 року «Про статутний фонд товариства з обмеженою Відповідальністю» [9] Держкомпідприємництво України, зазначається, коли засновники господарських товариств самі оцінюють майно або майнові права та визначають критерії оцінки своїх вкладів (договірна ціна) в статутний фонд господарського товариства, то це повинно оформлятися відповідним актом оцінки та прийняття-передачі у статутний фонд.

Таким чином, підбиваючи підсумки, можна відзначити, що особливості формування статутного фонду господарського товариства за рахунок майнових прав інтелектуальної власності є складним та цікавим не лише з позицій теорії, але й практики, оскільки породжує цілу низку наслідків як правового, так і фінансового характеру.

Список літератури

1. Цивільний кодекс України від 16 січня 2003 року N 435-IV. – Відомості Верховної Ради України. – 2003. – № 40. – Ст. 356.

2. Господарський кодекс України від 16 січня 2003 року № 436-IV. – Відомості Верховної Ради України. – 2003. – № 18. – Ст. 144.

3. Закон України «Про господарські товариства» 19 вересня 1991 р. // Відомості Верховної Ради України. – 1991. – № 49. – Ст. 682.
4. Закону України «Про оцінку майна, майнових прав та професійну оціночну діяльність в Україні» № 2658-III від 12.07.2001 [Електронний ресурс] / Верховна Рада України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2658-14
5. Закон України «Про режим іноземного інвестування» від 19.03.1996 р. // ВВР України. – 1996. – № 19. – Ст. 80.
6. Кравчук В.М. Майнові права інтелектуальної власності як вклад до статутного капіталу / М.М. Кравчук [Електронний ресурс]. – Режим доступу: www.ligazakon.ua/content/intelekt.pptx.
7. Тверезенко О.О. Майнові права інтелектуальної власності як внесок до статутного капіталу господарського товариства / О.О. Тверезенко // Теорія і практика інтелектуальної власності. – № 6. – 2009. – С. 50–59.
8. Постанова Пленуму Вищого господарського суду України від 17.10.2012 № 12 «Про деякі питання практики вирішення спорів, пов'язаних із захистом прав інтелектуальної власності» // Вісник господарського судочинства. – 2012. – № 6. – Ст. 57.
9. Лист Державного комітету України з питань регуляторної політики та підприємництва № 4-451-2030/6118 від 15.11.2002 «Щодо оцінки вкладу засновника (учасника) господарського товариства до статутного фонду, внесеного ним у вигляді права на використання «ноу-хау» [Електронний ресурс]. – Режим доступу : http://ua-info.biz/legal/basene/uacmpwdr.htm.

Тарасенко Л. Л. –
доцент кафедри інтелектуальної власності, інформаційного та корпоративного права юридичного факультету Львівського національного університету ім. Івана Франка, кандидат юридичних наук, доцент

КОМП'ЮТЕРНА ПРОГРАМА ЯК ОБ'ЄКТ ІНТЕЛЕКТУАЛЬНОГО ПРАВА

Судові спори у сфері інтелектуальної власності мають свою специфіку, обумовлену предметом позову, суб'єктним складом, предметом та засобами доказування, спеціальними способами захисту, які може застосувати суд тощо. Зважаючи на вказані особливості в систему судоустрою України введено Вищий суд з питань інтелектуальної власності, який розглядатиме справи цієї категорії.

Одним з об’єктів авторського права є комп’ютерна програма. У ст. 1 Закону України «Про авторське право і суміжні права» наводиться визначення комп’ютерної програми, відповідно до якого комп'ютерна програма – це набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах). Визначення є досить складним, оскільки містить багато технічних характеристик, які є не повною мірою зрозумілими для пересічної особи, в тому числі для суду, який розглядає спір. Варто додати, що комп’ютерна програма має свою візуалізацію, зокрема, це інтерфейс веб-сайту, мобільних додатків тощо. Комп'ютерні програми прирівнюються до літературних творів і мають таку ж правову охорону. Така охорона поширюється на комп'ютерні програми незалежно від способу чи форми їх вираження. Також про це йдеться і у міжнародно-правових актах. Так, у ст. 4 Договору ВОІВ про авторське право вказано, що комп’ютерні програми охороняються як літературні твори у розумінні ст. 2 Бернської конвенції незалежно від способу або форми їх вираження.

У науковій літературі слушно наголошують на те, що законодавче визначення недаремно піддано критиці фахівцями у цій сфері, оскільки у ньому зазначено більше ознак, ніж у її технічному визначенні, що вживається на практиці. Комп’ютерна програма з технічної точки зору є описом процесу оброблення інформації; такий опис має зчитуватися комп’ютером та приводити його у дію для вирішення конкретної задачі [1, с. 180]. Зокрема, йдеться про обробку інформації, виконання певної функції, досягнення певного результату тощо. Дати правове визначення комп’ютерної програми без фахових знань у цій сфері неможливо, оскільки складно відобразити правовою термінологією певні технічні процеси. Враховуючи можливе тлумачення законодавчих визначень, зокрема і комп’ютерної програми, може бути встановлено, що певний програмний продукт не містить однієї

чи двох ознак, що містяться у законодавчому визначенні, а відтак його не можна вважати комп'ютерною програмою.

Справді, комп'ютерна програма запускає певний технічний процес, який обов'язково повинен завершуватися результатом. У цьому контексті комп'ютерна програма близька до об'єктів патентного права. А саме вона, як і винахід або корисна модель, може вирішувати певне технічне завдання в будь-якій сфері технології. Поняття «технологія» може розумітися та тлумачитися по-різному, однак слід зважати на законодавче визначення цього поняття, з якого вбачається, що технологією є результат науково-технічної діяльності, сукупність систематизованих наукових знань, технічних, організаційних та інших рішень про перелік, строк, порядок та послідовність виконання операцій, процесу виробництва та/або реалізації і зберігання продукції, надання послуг (ст. 1 Закону України «Про державне регулювання діяльності у сфері трансферу технологій»). Враховуючи те, що об'єктом винаходу (корисної моделі) може бути або продукт, або процес (спосіб), що вирішує певне технічне завдання, комп'ютерна програма також може бути об'єктом винаходу (корисної моделі). Про це свідчить і судова практика, а саме у справі за позовом винахідників до Міжнародного науково-навчального центру інформаційних технологій і систем НАН та МОН України, про стягнення винагороди суд встановив наступне. Позивачі (винахідники) створили службовий винахід «Спосіб комп'ютерної ідентифікації особи за зображенням її обличчя», і уклали з роботодавцем договір щодо розміру та умови виплат винахіднику винагороди відповідно до економічної цінності винаходу і іншої вигоди, яка може бути одержана роботодавцем (Договір 1). В подальшому між відповідачем (роботодавцем) та компанією «Х») був укладений Договір про передання права на подання заявок і одержання патентів на винахід у країнах Паризького Союзу. В результаті виконання цього договору роботодавець, передавши право на подання заявки на винахід третій особі, отримав грошову винагороду, однак не сплатив винахідникам належну їм частину грошових коштів, що і було предметом судового спору [2]. З цього судового рішення вбачається, що комп'ютерна програма являла собою службовий

винахід, суть якого полягала у способі комп'ютерної ідентифікації особи за зображенням її обличчя. Відтак комп’ютерна програма може виступати складовою частиною винаходу (корисної моделі), яка виконує певну функцію в межах винайденого технічного рішення.

Комп’ютерна програма також є складовою частиною Інтернет-сайту як складного об’єкту інтелектуального права (поряд з інформаційною складовою, доменним ім’ям). Програмні засоби забезпечують його функціонування та можливість інформаційного наповнення веб-сайту.

Зазвичай комп’ютерна програма є об’єктом авторського права. А відтак вона повинна відповідати критеріям, які є визначальними для віднесення певного об’єкту до об’єктів авторського права. Вищий господарський суд України у п. 25 постанови Пленуму від 17 жовтня 2012 року «Про деякі питання практики вирішення спорів, пов’язаних із захистом прав інтелектуальної власності» вказує, що при вирішенні питань про те, чи є конкретний результат об’єктом авторського права, суду слід ураховувати: об’єктом правової охорони є лише такий результат, який створений творчою працею; доки не доведено інше, результат інтелектуальної діяльності вважається створеним творчою працею; правовій охороні як об’єкт авторського права підлягає твір, виражений в об’єктивній формі, а не його зміст [3]. Вказаний підхід базується на положеннях чинного законодавства України, а саме – на нормах Закону України «Про авторське право і суміжні права». Тому комп’ютерна програма як об’єкт авторського права повинна бути результатом саме творчої діяльності, який виражений в об’єктивній формі. Відсутність однієї з цих ознак зумовлює ненадання правової охорони такому об’єкту. Зокрема, в судові справі, предметом якої був захист майнових авторських прав, судом було встановлено, що комп’ютерна програма, яка була предметом спору, у порівнянні з іншою вже існуючою комп'ютерною програмою, містить відмінності, які не мають ознак оригінальності, не мають ознак творчого характеру. Тому розробниками цього програмного комплексу було використано існуючу комп'ютерну програму шляхом внесення у неї змін. Цей змінений програмний комплекс не відповідає умовам

оригінальності та не має ознак творчого характеру. Вказані обставини були встановлені відповідно до висновку комплексної судової експертизи комп'ютерної техніки та програмних продуктів та об'єктів інтелектуальної власності [4]. Тому суд цілком слушно констатував, що авторське право на комп'ютерну програму не виникло, а відтак і не підлягає захисту.

Відзначаємо, що у разі судового спору, в якому підлягають з'ясуванню обставини щодо похідного характеру комп'ютерної програми, незаконного використання подібної комп'ютерної програми, права на яку належать позивачеві тощо, належним та допустимим засобом доказування буде висновок експерта, оскільки суд не володіє спеціальними технічними знаннями у цій сфері, а відтак не може надати самостійно відповідну оцінку таким обставинам справи. Хоча в окремих випадках з урахуванням конкретних обставин справи та у разі, коли знань судді достатньо для з'ясування обставин справи, пов'язаної із захистом прав інтелектуальної власності, можливе вирішення суддею (суддями) питань, які виникають у розгляді справи, з позиції споживача без призначення судової експертизи. На це наголошує Вищий господарський суд України у Постанові Пленуму «Про деякі питання практики призначення судових експертиз у справах зі спорів, пов'язаних із захистом права інтелектуальної власності» № 5 від 23.03.2012 р. [5].

У зв'язку з наведеним слід наголосити, що процесуальний обов'язок доказування для автора у разі порушення його прав полягає в тому, що автор перш за все як позивач повинен довести належність йому авторського права (у тому числі, що спірний об'єкт належить до об'єктів авторського права) та права на його захист. При вирішенні цієї категорії справ не слід забувати про законодавчу презумпцію авторства, яку суди повинні застосовувати, поки відповідач не доведе протилежного належними та допустимими доказами. Як слушно наголошує Верховний Суд України п. 12 Постанови Пленуму від 04.06.2010 р. № 5 «Про застосування судами норм законодавства у справах про захист авторського права і суміжних прав», суду слід виходити із наявності матеріально-правової презумпції авторства [6]. Тому автор твору є первинним суб'єктом, якому

належить авторське право, і саме відповідач повинен доводити протилежне. Позивач також повинен виконувати свій процесуальний обов'язок по доказуванню факту наявності в нього авторського права, представляючи суду примірник твору (зокрема, і комп'ютерної програми) з зазначеним ім'ям автора або відповідне свідоцтво про авторство (за його наявності), яке і засвідчує наявність у позивача авторських прав. Однак наявність зазначеного імені автора на примірнику твору або наявність свідоцтва вже, своєю чергою, звільняє позивача від необхідності подання інших доказів для підтвердження вказаного факту авторства та дає суду змогу застосувати презумпцію авторства.

Водночас далеко не завжди автори, а особливо автори комп'ютерних програм, звертаються до Державної служби інтелектуальної власності України з заявами про отримання Свідоцтва про реєстрацію авторського права на твір, в тому числі на комп'ютерну програму, в порядку, визначеному Постановою Кабінету Міністрів України від 27 грудня 2001 р. № 1756 «Про державну реєстрацію авторського права і договорів, які стосуються права автора на твір». У більшості випадків автори не мають відповідного підтверджуючого авторство документа, що видається вказаним вище органом державної влади. І це цілком відповідає закону, оскільки авторське право на твір (в тому числі і на комп'ютерну програму) виникає внаслідок факту його створення. Для виникнення і здійснення авторського права не вимагається будь-яка реєстрація твору чи будь-яке інше спеціальне його оформлення, чи виконання будь-яких інших формальностей (ч. 2 ст. 11 Закону України «Про авторське право і суміжні права»).

Водночас в авторів нерідко виникають труднощі у доведенні авторства на комп'ютерні програми. Зокрема, ПрАТ «Лізинг інформаційних технологій» та ОСОБА_1 звернулися до суду із заявою про забезпечення позову до подання позовної заяви, мотивуючи це тим, що їм належать майнові авторські права на комп'ютерну програму «Конфігурація lC:LeaseIT» та базу даних «1С:LeaseIT», а відповідач своїми діями порушує їх авторські права. Суд відмовив у задоволенні такої заяви, вказавши, що позивачі не довели авторства на вказані об'єкти. При цьому суд в ухвалі послався на презумпцію авторства, але в

подальшому вказав, що автор у будь-який час протягом строку охорони авторського права може зареєструвати своє авторське право у відповідних державних реєстрах. Відтак суд (при чому як суд першої, так і апеляційної інстанції) дійшов висновку, що документом, який засвідчує авторство на оприлюднений чи неоприлюднений твір, а також факт і дату оприлюднення твору, є свідоцтво. А тому в даному випадку відсутні належні та допустимі докази, які б свідчили про те, що позивач є автором комп'ютерної програми «Конфігурація 1С:LeaseIT» та бази даних «1С:LeaseIT» [7]. Комп'ютерна програма охороняється як літературний твір. Водночас не врегульованим є питання фіксації авторства на цей об'єкт авторського права. Тому суд у вказаній вище справі відмовив автору у вжитті заходів забезпечення позову, мотивуючи це відсутністю доказів авторства і неможливістю застосувати презумпцію авторства. Враховуючи розвиток інформаційних технологій, розвиток IT–права, є потреба у відповідному правовому регулюванні вказаних відносин на рівні закону або бодай у тлумаченні норм права вищими судовими інстанціями. У цій ситуації можна зрозуміти позицію суду, оскільки рішення про забезпечення позову може потягнути несприятливі наслідки для відповідача, тому таке рішення повинно бути обґрунтованим. Водночас відмова (що і мало місце) в таких заходах може зашкодити інтересам позивача. Тому суд вважав, що виключно документом (Свідоцтвом про авторство) позивач повинен доводити факт його авторства, а не покликанням на недоведену позивачем презумпцію авторства. Але презумпція, власне, і не потребує доведення. Презумпція є чинною, поки її не спростують, а цей обов'язок покладається вже на відповідача по справі. Однак, враховуючи те, що згідно презумпції авторства автором твору (в даному випадку – комп'ютерної програми) вважається особа, зазначена як автор на оригіналі або примірнику твору, виникає питання: яким чином зазначити ім'я автора на примірнику комп'ютерної програми, щоб це могла побачити будь-яка особа, в тому числі суд, розглядаючи спір. Комп'ютерна програма має свою специфіку як об'єкт авторського права, оскільки це не літературний твір, а набір інструкцій у вигляді слів, цифр, кодів, схем, символів тощо, що зчитуються комп'ютером.

Комп’ютерну програму неможливо прочитати як певний письмовий твір. Варто погодитися з позицією Селіванова М.В., який зазначає, що ім’я автора комп’ютерної програми може бути відображене у вихідному коді, в аудіовізуальних зображеннях, породжуваних комп'ютерною програмою, у супровідній документації і на упаковці носіїв екземпляра програми [8, с. 6]. Відтак при відкритті файлу з вихідним кодом можна побачити ім’я автора, за умови його розміщення. Водночас суди не завжди вдаються до таких дій при розгляді спору. Більше того, автори не у всіх випадках вказують своє ім’я самим таким способом. Крім того, як слушно вказує Яворська О.С., комп’ютерна програма нерідко створюється колективом авторів, і цей колектив може бути досить чисельним, зважаючи на складність комп’ютерного продукту [1, с. 181], а відтак виникає питання щодо технічної можливості зазначення імен всіх авторів у примірнику комп’ютерної програми. Так, в іншій судовій справі позивачі просили суд визнати їх співавторами твору «Комп’ютерна програма «ПК «ЛІРА 9.6», припинити дії, що порушують їх авторське право, шляхом заборони відповідачам вчиняти дії щодо розпорядження майновими авторськими правами без згоди позивачів як співавторів [9]. Суд відмовив у задоволенні позову, вказавши, що позивачі повинні були довести факт наявності в них авторського права на спірний об’єкт та, навіть виходячи із наявності матеріально-правової презумпції авторства, мали надати документи та докази, які підтверджують, що саме вони є суб’єктами відповідного права. Аналізуючи вказане рішення суду, можна стверджувати, що справді позивачі не надали суду жодного доказу створення ними комп’ютерної програми. Суд не міг застосувати презумпцію авторства, оскільки позивачі на примірнику комп’ютерної програми не вказані як автори, договір між співавторами про створення об’єкту авторського права також відсутній. Більше того, суд вірно відзначив, що позивачами не надано доказів того, у чому саме полягає творча участь кожного із позивачів у створенні комп’ютерної програми.

Висновки. Законодавче визначення комп’ютерної програми є досить складним, містить багато технічних

характеристик, які не зовсім зрозумілі як для пересічної особи, так і для суду, який розглядає спір. Однак дати нормативне визначення комп'ютерної програми без фахових знань у цій сфері неможливо, бо складно відобразити правовою термінологією певні технічні процеси.

Комп'ютерна програма має свою візуалізацію, зокрема, це інтерфейс веб-сайту, мобільних додатків тощо. Комп'ютерна програма також є складовою частиною Інтернет-сайту як складного об'єкту інтелектуального права (поряд з інформаційною складовою, доменним ім'ям). Програмні засоби забезпечують його функціонування та можливість інформаційного наповнення веб-сайту.

За правовою охороною комп'ютерні програми прирівнюються до літературних творів. Комп'ютерна програма як об'єкт авторського права повинна бути результатом саме творчої діяльності, який виражений в об'єктивній формі. Відсутність однієї з цих ознак зумовлює ненадання правової охорони такому об'єкту. Комп'ютерна програма може бути складовою частиною винаходу (корисної моделі), яка виконує певну функцію в межах винайденого технічного рішення.

Невирішеним на законодавчому рівні є питання щодо технічної можливості автора зазначати своє ім'я на примірнику комп'ютерної програми таким чином, щоб це могла побачити будь-яка особа, в тому числі суд при розгляді та вирішенні спору з приводу авторських прав на комп'ютерну програму. З урахуванням стрімкого розвитку цифрового середовища, розвитком ІТ–права, є потреба у вдосконаленні правового регулювання цих відносин на рівні закону (доречним було б також і наявність роз'яснень чинних норм закону вищими судовими інстанціями).

Список літератури

1. Інтелектуальне право України / За заг. ред. О.С. Яворської. – Тернопіль: Підручники і посібники. – 2016. – 608 с.

2. Рішення Апеляційного суду м. Києва від 16.09.2015. Справа №752/9813/13 // [Електронний ресурс]. – Єдиний державний реєстр судових рішень. – режим доступу: http://reyestr.court.gov.ua/Review/50793926

3. Про деякі питання практики вирішення спорів, пов'язаних із захистом прав інтелектуальної власності: Постанова Пленуму Вищого

господарського суду № 12 від 17.10.2012 р. // [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/v0012600-12

4. Рішення господарського суду м. Києва від 12.05.2015 р. Справа №9/174 // [Електронний ресурс]. – Єдиний державний реєстр судових рішень. – режим доступу: http://www.reyestr.court.gov.ua/Review/44342133

5. Про деякі питання практики призначення судових експертиз у справах зі спорів, пов'язаних із захистом права інтелектуальної власності: Постанова Пленуму Вищого господарського суду № 5 від 23.03.2012 р. // [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/v0005600-12

6. Про застосування судами норм законодавства у справах про захист авторського права і суміжних прав: Постанова Пленуму Верховного Суду України № 5 від 04.06.2010 р. // [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/v0005700-10

7. Ухвала Апеляційного суду м. Києва від 18.02.2015 р. Справа № 756/960/15-ц // [Електронний ресурс]. – Єдиний державний реєстр судових рішень. Режим доступу: http://www.reyestr.court.gov.ua/Review/42783733

8. Селіванов М.В. Захист права на комп'ютерну програму (авторсько-правовий аспект): автореф. дис. канд. юрид. наук : 12.00.03 / М.В. Селіванов; Нац. ун-тет внутр. справ. – Харків, 2002. – 16 с.

9. Рішення Соломянський районний суд м. Києва від 31.10.2011 р. Справа № 2-6118/11 // [Електронний ресурс]. – Єдиний державний реєстр судових рішень. Режим доступу: http://reyestr.court.gov.ua/Review/21645618

Тищенко М.М. –
професор кафедри адміністративного та інформаційного права
Навчально-наукового інституту права та психології
Національного університету «Львівська політехніка»,
доктор юридичних наук, професор
член-кореспондент Національної академії правових наук України

ДО ПИТАННЯ ПРО ЗАБЕЗПЕЧЕННЯ ПРАВА СПОЖИВАЧІВ НА ІНФОРМАЦІЮ

Сфера споживання являє собою одну з найбільш складних і значущих соціальних сфер, яка багато в чому визначала, визначає і визначатиме розвиток людства. Протягом століть саме ця сфера не тільки служила локомотивом економічного зростання, але і багато в чому визначила тенденції розвитку як внутрішньодержавних, так і міждержавних відносин.

Не менш важливою є і те, що сфера споживання займає ключове місце у забезпеченні життєдіяльності протягом всього життя людини. Від рівня і якості споживання залежить не тільки здоров'я, а іноді і саме життя людини, але так само й ступінь комфортності умов життя, тобто фактично те, що називається прийнятними для цивілізованого суспільства умовами існування.

В умовах сьогодення особливого значення набуває осмислення ряду факторів, які, на нашу думку, повинні відігравати ключову роль у процесах подальшого підвищення ефективності правового регулювання у сфері забезпечення прав споживачів. Уявляється, що визначення цих факторів має концептуальне значення в контексті сучасних євроінтеграційних процесів, прагнення привести рівень життя громадян України у відповідність із загальноприйнятими світовими стандартами. При цьому, пріоритетним слід визнати системний підхід до проблем забезпечення безпеки у сфері споживання, який являє собою один з найбільш важливих концептуальних аспектів забезпечення прав споживача, особливо в ситуації, коли безпека споживання повинна набути значення відповідного імперативу. Сутність останнього полягає в чіткому визначенні та неухильній реалізації на практиці належних параметрів безпеки продукції та послуг, забезпечуваним як зусиллями держави, так і активною діяльністю інститутів громадянського суспільства. Може здатися, що реалізація цього імперативу певною мірою звужує право вибору споживача. Думається, що це не так. Навпаки, йдеться про виведення права вибору споживача на інший, якісно новий рівень, тобто дозволяє вибрати найкраще з безпечного.

Очевидним є те, що одним з найбільш важливих компонентів, що визначають відносини у сфері споживання, слід визнати інформацію, яка представляє собою універсальний ресурс, багато в чому визначає динаміку відповідних процесів і, перш за все, з точки зору формування суб'єктивної позиції споживача і, як результат, його поведінки. На даний час людство перебуває в стадії переходу від індустріального суспільства до суспільства інформаційного. У цьому суспільстві ще більшу роль будуть грати системи розповсюдження, зберігання і обробки інформації. З часом єдине інформаційне

середовище подібно світовій системі зв'язку забезпечить кожному індивіду доступ до всієї необхідної для нього інформації, накопиченої людством. При цьому, інформація, з одного боку, формує матеріальне середовище життя людини, виступаючи у ролі інноваційних технологій, комп'ютерних програм тощо, а з іншого – служить основним засобом міжособистісних взаємин, постійно виникаючи, видозмінюючись і трансформуючись у процесі переходу від однієї людини до іншої. Тим самим інформація одночасно визначає і соціокультурне життя людини, та її матеріальне буття [1, с. 22-23].

Не вдаючись у докладний аналіз категорії інформації, зазначимо ті ключові аспекти, які прямо співвідносяться з проблемами забезпечення прав споживачів. Насамперед, підкреслимо ту важливу обставину, що інформація не тільки лежить в основі формування тих чи інших потреб людини, але і багато в чому визначає їх реалізацію. Іншими словами, шлях від усвідомлення необхідності до отримання бажаного результату супроводжується і забезпечується певною інформацією. При цьому, як правило, той чи інший вибір ґрунтується на певних аргументах, тобто передбачає інформованість споживачів, яка, в свою чергу, передбачає отримання деяких даних. Поряд з цим, прийняття рішення споживачами залежить як від внутрішньої (тобто знань вже наявних), так і від зовнішньої інформації (тобто те, що пізнається з навколишнього світу). Потребою людини в інформації можуть бути мотивовані покупки і споживання багатьох товарів і послуг. Також, важливість потреби людей в інформації визначається її роллю в процесі переконання [2, с. 375-376]. Останнє підкреслює значимість налагодженості відносин, які виникають у сфері товарів і послуг. Не викликає сумніву і те, що саме наявність і обсяг відповідної інформації обумовлюють поведінку споживачів, їх активність при задоволенні тих чи інших потреб. Поряд з цим, інформація забезпечує реалізацію функції, важливість якої важко переоцінити. Йдеться про налагодження зворотного зв'язку, тобто інформування всіх інших учасників відносин у сфері споживання про суб'єктивну позицію споживача з тих чи

інших питань, серед яких провідне місце займають питання формування ринку продукції або послуг, їх безпеки і якості.

З позицій правового регулювання представляється важливим сконцентрувати увагу на наступних аспектах інформаційних відносин у сфері споживання. По-перше, це забезпечення надання інформації споживачам в обсязі, необхідному для прийняття конкретних рішень, по-друге, забезпечення достовірності та об'єктивності споживчої інформації, в тому числі і з позицій ідентифікації товару або послуги, співвіднесення їх з конкретною отриманою інформацією. По-третє, це виключення або максимальна мінімізація інформації про товари або послуги, яка несе або містить потенційну загрозу для фізичного чи психічного здоров'я споживача. Прикладом такого положення є певне поширення в останній час рекламування речовин та технічних пристроїв, які начебто дозволяють суттєво покращити стан здоров'я людини, не маючи насправді їх науково доведеної ефективності і, що не менш важливо, не враховує можливих побічних негативних ефектів. І нарешті, вважаємо, що осмислення питань про інформаційну забезпеченість споживачів слід пов'язувати з проблемами юридичної відповідальності за порушення права на інформацію в сфері споживання.

В цілому, на наш погляд, необхідна також певна корекція підходів до поширення інформації про реальні кроки, спрямовані на забезпечення прав споживачів з боку державних інституцій та громадських організацій. Певною мірою повинні бути переглянуті і підходи до розгляду і вирішення звернень громадян, пов'язаних зі сферою споживання не тільки з позицій презюмування правочинності їх домагань, але й з позиції цінності їх громадської позиції в питаннях удосконалення сфери споживання.

Говорячи про значення інформації в сфері споживання, не можна не звернути увагу на важливість інформованості громадян-споживачів про їх права і обов'язки, наявних правових механізмах їх реалізації та захисту. По суті, мова йде про підвищення правової культури споживачів і ступеню їх правової активності. Остання, на наш погляд, має особливе значення, оскільки виступає в ролі каталізатора для вирішення багатьох

проблем, що виникають у цій сфері. Саме активність споживачів у захисті своїх прав і свобод здатна забезпечити стратегічну перевагу в боротьбі за безпеку і якість товарів і послуг.

Список літератури

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

2.Блэкуэлл Р. Поведение потребителей/ Блэкуэлл Р., Минард П., Эджел Дж.: Пер.с англ. – СПб: Питер, 2007. – 944 с.

Фасій Б.В. –
аспірант кафедри цивільного права, член Ради молодих вчених Національного університету «Одеська юридична академія»

СУБСИДІАРНЕ ЗАСТОСУВАННЯ НОРМ ЦИВІЛЬНОГО ЗАКОНОДАВСТВА ДО ІТ-ВІДНОСИН

Прискорення та розвиток науково-технічного прогресу, інформаційних технологій, комп'ютерної техніки та комп'ютерних мереж в Україні засноване на впровадженні у виробництво гнучких автоматизованих систем, мікропроцесорних засобів і пристроїв програмного управління, роботів і обробних центрів, поставило перед сучасною наукою важливе завдання – виховати та підготувати підростаюче покоління науковців та юристів, здатних активно включитися в якісно новий етап розвитку сучасного суспільства, пов'язаний з інформатизацією. У цій сфері законодавство не здатне стрімко впроваджувати норми і не встигає реагувати на різкі зміни у розвитку суспільних відносин. Це є нормальним явищем не тільки для України, але й для інших європейських країн, навіть найстабільніших. Звичайно, зі спливом часу дані суспільні відносини, знайдуть своє відображення у праві.

Інформаційні технології або ІТ (використовується також загальніший / вищий за ієрархією термін інформаційно-комунікаційні технології (Information and Communication Technologies, ICT) – сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання,

опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів [1].

Діяльність ІТ-компаній вагомо впливає на правовідносини в Україні. Чимало ІТ-компанії або засновані нерезидентами або мають контракти з іноземними компаніями. Тому, на управління ІТ-компаніями впроваджуються інноваційні методики і сучасні світові моделі управління персоналом та контроль за продуктивністю компанії. Проте й на суспільні відносини має вплив середовище ІТ-спеціалістів, їхня термінологія та світогляд, стиль життя, що зазвичай відрізняється від середньо-статистичного, а особливо відносини з іноземними замовниками та засновниками, що застосовують в українських реаліях свої правові стандарти і навіть своє право – ІТ-право [2, с. 6].

У науці можна розглядати ІТ-право як: міждисциплінарну галузь права; навчальну дисципліну тощо. Проте, не торкаючись питання про визначення місця ІТ-відносин в системі права, необхідно зазначити, що це, перш за все, це звичайні відносини, які регулюються господарським, трудовим, адміністративним, кримінальним та цивільним правом. Саме про застосування останньої галузі права до ІТ-відносин і піде мова в даному дослідженні, яке в юридичній доктрині йменується «субсидіарне застосування норм законодавства».

Під субсидіарним застосуванням норм цивільного законодавства потрібно розуміти правовий механізм, який дозволяє розвантажувати законодавство від нераціонального дублювання тотожних та аналогічних норм і понять у суміжних галузях, інститутах права.

У ст. 9 ЦК України визначається допустимість субсидіарного застосування положень ЦК України до природоресурсних, трудових, сімейних відносин, за умови якщо вони не врегульовані іншими актами законодавства.

Механізм субсидіарного застосування норм цивільного законодавства виступає як засобом подолання прогалин, так способом економії нормативного матеріалу. Зазначені засоби подолання прогалин можна віднести до додаткових процедур, оскільки повного подолання прогалин не відбувається.

У цивільному праві України необхідно розмежувати субсидіарне застосування норм цивільного законодавства від аналогії закону (міжгалузевої аналогії).

По-перше, субсидіарне застосування норм цивільного законодавства в ряді випадків може носити не тимчасовий характер як різновид аналогії закону (міжгалузева аналогія), а стабільний, безпосередньо встановлений законодавцем з метою досягнення єдності в правовому регулюванні суспільних відносин, як це відбувається при регулюванні ІТ-відносин.

По-друге, субсидіарне застосування норм законодавства здійснюється безпосередньо по волі законодавця, який у відповідній правовій нормі вводить спеціальні відсилання до інших норм, які регулюють подібні відносини.

По-третє, підставою для здійснення регулятивної дії аналогії закону у цивільному праві України є ст. 8 ЦК України, а підставою субсидіарного застосування норм цивільного законодавства – ст. 9 ЦК України.

По-четверте, суб'єктами застосування як аналогії закону, так міжгалузевої аналогії є лише судові органи, субсидіарне застосування норм законодавства може здійснюватись усіма учасниками цивільних правовідносин, у тому числі ІТ-компаніями, ІТ-спеціалістами, ІТ-юристами тощо.

Видається більш правильним трактувати субсидіарне застосування норм законодавства ширше, ніж тільки в якості міжгалузевої аналогії, оскільки воно може використовуватися як при наявності прогалин у законодавстві, так при їх відсутності (як засіб економії нормативного матеріалу).

Існують такі юридичні поняття, які однаково трактуються і застосовуються в різних галузях та інститутах права (позовна давність у випадку захисту честі, гідності і ділової репутації, загальні положення про договір надання послуг, відшкодування шкоди). Тому, однією з найбільш істотних особливостей субсидіарного застосування цивільного законодавства до суміжних відносин, оскільки воно не змінює галузеву приналежність суміжних правовідносин. Зокрема, якщо в ІТ-відносинах використовуються термін «фізична особа-підприємець», «юридична особа», то відносини, що виникли в результаті її дії залишаються ІТ відповідно, хоча і припускають

субсидіарне використання цивілістичного нормативного матеріалу.

Умовами субсидіарного застосування норм цивільного законодавства до ІТ-відносин є: 1) неврегульованість суспільних відносин ІТ-сфері; 2) наявність норми, яка регулює саме ці відносини у цивільному законодавстві; 3) однорідність предмету регулювання між цивільними та ІТ-відносинами; 4) відсутність прямої заборони на субсидіарне застосування норм законодавства (ч. 2 ст. 1 ЦК України); 5) прийняття рішення на підставі та в межах правових норм законодавства, відповідних їх цілям, принципам й загальному смислу.

Наведемо деякі приклади субсидіарного застосування норм цивільного законодавства до ІТ-відносин докладніше.

Більшість підприємств (незалежно від того, зареєстровані в Україні чи в інших країнах) укладають ІТ-договори про надання послуг (наприклад, захист вашої інформації від пошкодження і небажаного розповсюдження) або про виконання робіт (наприклад, розроблення програмного забезпечення із фізичними особами-підиріємцями (далі – ФОП) та юридичними особами (ІТ-компаніями), тим самим використовується механізм субсидіарного застосування норм цивільного законодавства.

ФОП здійснює підприємницьку діяльність відповідно до гл. 5 ЦК України «Фізична особа-підприємець». Зокрема, ч. 1 ст. 50 ЦК України передбачено право фізичної особи з повною цивільною дієздатністю на здійснення підприємницької діяльності, яку не заборонено законом.

У свою чергу, ІТ-компанії здійснюють свою підприємницьку діяльність згідно з гл. 7 ЦК України «Загальні положення про юридичні особи» та гл. 8 ЦК України «Підприємницькі товариства». Так, відповідно до ст. 80 ЦК України юридичною особою є організація, створена і зареєстрована у встановленому законом порядку, наділяється цивільною правоздатністю і дієздатністю, може бути позивачем та відповідачем у суді. Юридична особа може проводити свою діяльність у однієї з форм господарських товариств: повного товариства, командитного товариства, товариства з обмеженою

або додатковою відповідальністю, акціонерного товариства (ч. 2 ст. 113 ЦК України).

Якщо відносини замовника та ІТ-спеціаліста щодо розробки програмного забезпечення існують у межах цивільно-правового договору, то постає питання про визначення правової природи цих відносин. В ІТ-сфері субсидіарно застосовуються два види цивільно-правових договорів, які регулюються цивільним законодавством: цивільно-правовий договір про виконання робіт і цивільно-правовий договір про надання послуг.

Цивільно-правовий договір про виконання робіт – договір підряду – це договір, за яким одна сторона (підрядник) зобов'язується на свій ризик виконати певну роботу за завданням другої сторони (замовника), а замовник зобов'язується прийняти та оплатити виконану роботу. Договір підряду може укладатися на виготовлення, обробку, переробку, ремонт речі або на виконання іншої роботи з передатнім її результату замовникові (ст. 837 ЦК України). Прикладам договорів про виконання робіт в ІТ-сфері є створення програмного забезпечення, ремонт обладнання тощо.

Інший вид договору – про надання послуг – це договір, за яким одна сторона (виконавець) зобов'язується за завданням другої сторони (замовника) надати послугу, яка споживається в процесі вчинення певної дії або здійснення певної діяльності, а замовник зобов'язується оплатити виконавцеві зазначену послугу, якщо інше не встановлено договором (ст. 901 ЦК України). Положення гл. 63 ЦК України «Послуги. Загальні положення» можуть застосовуватися до всіх договорів про надання послуг (і навіть до договорів про надання ІТ-послуг), якщо це не суперечить суті зобов'язання (ч. 2 ст. 901 ЦК України). Досить поширеними ІТ-послугами в Україні є: технічне обслуговування робочих станцій; обслуговування програмного забезпечення робочих станцій; обслуговування мережевої інфраструктури; технічне обслуговування серверного обладнання; обслуговування серверного програмного забезпечення; обслуговування пристроїв друку та периферії; обслуговування телефонії; захист інформації тощо.

Як відомо корисний ефект від діяльності з надання послуги не виступає у вигляді певного осяжного матеріального результату, як це має місце при виконанні роботи (наприклад, створення програмного забезпечення), а полягає в самому процесі надання послуги (наприклад, технічне обслуговування серверного обладнання). Особливістю послуги є збіг у часі та просторі процесів виробництва, реалізації та витрачання їх споживчої вартості. Тобто споживання послуги має місце в процесі її надання, на відміну від роботи, споживання результатів якої зазвичай не співпадає з часом їх надання [3, с. 613]. Ще однією різницею між договорами про виконання робіт та про надання послуг є оплата. Тобто за договором про виконання робіт оплачується його конкретний результат, який визначається визначається у договорі й оформляється актом приймання передачі виконаних робіт, а при наданні послуг оплачується процес, який є триваючим (оплата здійснюється протягом певного періоду в часі).

На практиці необхідно відрізняти договір про надання послуг і трудовий договір. Цивільно-правовий договір про надання ІТ-послуг укладається у письмової формі (згідно ст. 208 ЦК України) та не містить положень щодо режиму роботи, внутрішнього трудового розпорядку, часу відпочинку, оплати праці, трудової дисципліни. Оскільки в ст.ст. 232, 235 Кодексу законів про працю України йдеться про врегулювання трудових спорів за позовами працівників «про оформлення трудових відносин у разі виконання ними роботи без укладення трудового договору», то у випадку укладання договору в усній формі, суд вважатиме, що фізичну особу фактично було допущено до роботи, а тому, з нею укладено трудовий договір.

Враховуючи сучасний рівень розвитку суспільства неможливо уявити собі людину, яка жодним чином не приймає участі в ІТ-відносинах. Саме для того, щоб забезпечити повноцінну участь індивідуальних фізичних осіб в суспільних правовідносинах, законодавець закріплює (ст.ст. 297, 299, 301 ЦК України) наступні немайнові права, положення яких субсидіарно застосовуються до ІТ-відносин, а саме: право на повагу до гідності і честі; право на недоторканність ділової репутації; право на особисте життя та його таємницю.

Захист честі, гідності і ділової репутації в ІТ-сфері – право громадянина та юридичної особи вимагати через суд спростування на веб-сайті недостовірної інформації (відомостей, що не відповідають дійсності або викладені неправдиво), яка принижує їхню честь, гідність чи ділову репутацію або завдає шкоди їхнім інтересам. Недостовірною вважається інформація, яка не відповідає дійсності або викладена неправдиво, тобто містить відомості про події та явища, яких не існувало взагалі або які існували, але відомості про них не відповідають дійсності (неповні або перекручені). Право на захист честі, гідності і ділової репутації у ІТ-сфері закріплено Конституцією України (ч. 4 ст. 32), ЦК України (ст. 277). Питання процедури захисту честі, гідності і ділової репутації також роз'яснив Верховний Суд України [4] з метою забезпечення правильного й однакового застосування судами законодавства, що регулює захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи. У постанові Пленуму Верховного Суду України зазначено, що відповідачем у справах, де є поширення неправдивої інформації в мережі Інтернет, є автор та власник веб-сайту. Позивач сам повинен встановлювати автора та власника веб-ресурсу для складання та подачі позовної заяви. У випадку неможливості знайти автора або його місця проживання (місцезнаходження) відповідачем у справі є та особа, в якої у власності знаходиться веб-сайт. Тобто, якщо неможливо встановити автора – тоді ідентифікується веб-сайт.

Захисті честі, гідності і ділової репутації є явищем досить поширеним. Для прикладу наведемо рішення Рівненського міського суду Рівненської області від 1 листопада 2016 року в справі за позовом фізичної особи до Головного управління Державної фіскальної служби у Рівненській області, приватного підприємства «Рівне вечірнє» та інших осіб про захист честі, гідності та ділової репутації шляхом спростування недостовірної інформації та стягнення моральної шкоди. Субсидірно застосувавши ст. 277 ЦК України в ІТ-відносинах, суд визнав інформацію розміщену на веб-сайті в статті «Квартиру батьків начальника Рівненської митниці обшукали – знайшли десятки тисяч доларів»: «…начальника митниці, якого власна безпека звинувачує у розтраті державного майна, а

відтепер і у корупції», «Як зазначає заступник начальника відділу власної безпеки при ГУ ДФС у Рівненській області ГУВБ ДФС України, вилучили з квартир митників також речі, які мають значення для вказаного кримінального провадження та можуть бути доказами.» недостовірною та такою, що порочить честь, гідність та ділову репутацію позивача [5]. У таких справах, що випливають з ІТ-відносин, відповідно до п. 2 ч. 2 ст. 258 ЦК України, позовна давність є спеціальною та становить 1 рік (у цьому разі позовна давність обчислюється від дня поміщення цих відомостей на веб-сайті або від дня, коли особа довідалася чи могла довідатися про ці відомості).

Одночасно із вимогами про захист честі, гідності та ділової репутації у позивачі можуть вимагати також відшкодування моральної шкоди згідно ст. 1167 ЦК України. У цьому випадку обов'язок довести, що була заподіяна моральна шкода, покладається на позивача. На нього також покладається обов'язок визначити розмір моральної шкоди, але остаточно розмір грошового відшкодування моральної шкоди визначається судом залежно від характеру правопорушення, глибини фізичних та душевних страждань, погіршення здібностей потерпілого або позбавлення його можливості їх реалізації, ступеня вини особи, яка завдала моральної шкоди, якщо вина є підставою для відшкодування, а також з урахуванням інших обставин, які мають істотне значення. При визначенні розміру відшкодування враховуються вимоги розумності та справедливості. У разі відмови у задоволенні позову у рішенні повинні бути вказані причини та обгрунтування такої відмови. І як показує судова практика в ІТ-сфері за 2016 рік, суди масово відмовляють у позовах про стягнення моральної шкоди за недоведеністю та безпідставністю позовних вимог. Хоча, особа має також право звернутися до Європейського суду з прав людини, якщо всі засоби захисту прав та інтересів в Україні вичерпалися.

Також необхідно звернути увагу на те, що цивільним законодавством врегульовано зобов'язання відшкодування шкоди, положення яких субсидіарно застосовуються в ІТ-відносинах. Права на відшкодування шкоди у таких випадках виникає, якщо відбулося копіювання інформації з чужого веб-

сайту або привласнення ІТ-відкриття, ІТ-винаходу тощо. Зокрема, майнова шкода, завдана неправомірними рішеннями, діями чи бездіяльністю особистим немайновим правам фізичної або юридичної особи, а також шкода, завдана майну фізичної або юридичної особи, відшкодовується в повному обсязі особою, яка її завдала (ст. 1166 ЦК України).

Як уявляється, § 3 гл. 82 ЦК України «Відшкодування шкоди, завданої внаслідок недоліків товарів, робіт (послуг)» також підлягає субсидіарному застосуванню до ІТ-відносин, якщо за договором про виконання робіт або про надання послуг виготовлювач товару, що є нерухомим майном, ІТ-спеціаліст (ІТ-компанія) завдав шкоду фізичній або юридичній особі внаслідок конструктивних, технологічних, рецептурних та інших недоліків товару, робіт (послуг), а також недостовірної або недостатньої інформації про них.

Встановлення режиму комерційної таємниці та її збереження є першочерговим завданням учасників ІТ-відносин. Зокрема, ст. 505 ЦК України визначає комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційною, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Ознаками інформації, яку можливо віднести до комерційної таємниці є: відсутність загальновідомості; відсутність загальнодоступності; комерційна цінність [6]. Якщо інформація не відповідає даним критеріям, вона не може бути визнана комерційною таємницею.

Найчастіше нерозголошенню підлягають: власні ІТ-винаходи та раціоналізаторські пропозиції, які не захищенні авторським або патентним правом; всі програмні об'єктні коди, які не розповсюджуються публічно, вихідні коди, альфа- та

бета-версії програмної продукції компанії; методологія програмування, техніка дизайну, способи оптимізації роботи програмного забезпечення; технічна документація, специфікація; використані в програмі алгоритми, формули; плани на нові послуги та програмні продукти, дані про замовників продукції та послуг; ідеї, які дають фірмі конкурентні переваги; інформація про нове програмне забезпечення, яке знаходиться на стадії розробки; бізнес-процеси; інші дані.

Підводячи підсумки, хотілося б зазначити, що субсидіарне застосування норм цивільного законодавства до ІТ-відносин – це реалії сьогодення, оскільки цивільні та ІТ-відносини є суміжними. І допоки не будуть врегульовано ІТ-відносини спеціальними законодавчими актами, даний механізм застосування є неминучим. Зокрема, з приводу ІТ-договорів з надання послуг програмного забезпечення або його розробки; оформлення та захисту авторських прав і торгової марки в мережі Інтернет; захисту прав інтелектуальної власності; захисту інформації; позовної давності; зобов'язань відшкодування шкоди, комерційної таємниці тощо.

Список літератури

1.Інформаційні технології [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Інформаційні_технології

2.Бачинський Т. Основи ІТ-права / Т. Бачинський. – Львів : Апріорі, 2016. – 136 с.

3.Харитонов Є.О., Харитонова О.І., Старцев О.В. Цивільне право України: Підручник. – Вид. 3, перероб. і доп. – К. : Істина, 2013. – 808 с.

4.Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи : Постанова Пленуму Верховного Суду України від 27.02.2009 р. № 1 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/v_001700-09

5.Рішення Рівненського міського суду Рівненської області від 01.11.2016 р. № 569/2732/16-ц [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/62373793

6.Комерційна таємниця в ІТ-індустрії [Електронний ресурс]. – Режим доступу: http://go-advocate.com/komertsijna-tajemnytsya-v-it-industriji-2

Харитонов Є.О. –
завідувач кафедри цивільного права
Національного університету «Одеська юридична академія»
доктор юридичних наук, професор,
член-кореспондент Національної академії правових наук України

СУТНІСТЬ ІТ-ПРАВА (ІТ- ПРАВО ЯК КОНЦЕПТ)

Проблематика, пов'язана з ІТ-правом, останнім часом викликає усе більший інтерес науковців, що зумовлено поширенням ІТ-відносин та зростанням питомої ваги юридичної активності у цій галузі на практиці. Разом із тим, дефініція ІТ-права, його характеристика та встановлення сутності поки що належать до числа питань, які потребують серйозного дослідження.

У найбільш загальному вигляді під ІТ-правом розуміють сукупність норм та правил, що опосередковують діяльність по забезпеченню безпеки інформаційних технологій та інформаційної активності в мережі Інтернет. До сфери його правового регулювання відносять широке коло різноманітних відносин, які регулюються нормами цивільного, господарського, адміністративного законодавства. При цьому ІТ-право характеризують як мультидисциплінарну галузь права, котра поєднує в собі згадані вище та інші галузі. У такому, чи приблизно такому сенсі, позначення «ІТ-право» використовується науковцями та практикуючими юристами при визначенні сфери відповідної діяльності, в освітніх програмах, у рекламі тощо.

Проте, характеристика ІТ-права як мультидисциплінарної галузі права викликає заперечення.

По-перше, вираз «мультидисциплінарна галузь права» не несе змістовного навантаження, а лише вказує на відсутність адекватного уявлення про суспільне явище, будучи парафразом «комплексна галузь права».

По-друге, невдалим є сам вираз «мультидисциплінарна галузь права», оскільки з нього випливає, що «галузь права» складається з «дисциплін». З усіх варіантів дефініцій багатозначного поняття «дисципліна» стосовно нашого випадку

прийнятним є лише визначення останньої стосовно системи знань, як конкретної галузі академічних, наукових, навчальних та інших знань (синонім – фах) [1]. Але тоді виходить, що галузь права, як суспільний феномен, характеризується через категорію «знання про право».

Нарешті, сумнівною здається спроба використання стосовно сучасної категорії «ІТ-право» достатньо давньої і скомпрометованої категорії «комплексна галузь права». Як слушно зазначають критики запровадження зазначеної категорії, оцінюючи ситуацію з позиції поділу права на галузі, для такої диференціації мають існувати критерії, до яких традиційно відносять предмет та метод правового регулювання, а також принципи, на яких побудована галузь права, та функції, котрі вона виконує [2, с. 17-27].

Жоден зі згаданих критеріїв не може бути застосованим щодо ІТ-права. Зокрема, відсутній єдиний предмет правового регулювання, оскільки, фактично, йдеться не про «ІТ-відносини», а про відносини, що пов'язані зі сферою інформаційних технологій або суміжними сферами. Згадані відносини є різнорідними і за своєю сутністю можуть бути цивільними, адміністративними, фінансовими, корпоративними тощо. Так само не існує єдиного методу правового регулювання відносин, пов'язаних зі сферою інформаційних технологій або суміжними сферами, оскільки у залежності від типу відносин і конкретних завдань може застосовуватися як диспозитивний, так і імперативний метод (цивільно-правовий, адміністративно-правовий тощо методи). Не можуть бути критерієм виокремлення ІТ-права і принципи правового регулювання, які залежать від методу та відображаються у ньому. Що стосується функцій, тобто основних напрямків випливу на свідомість і поведінку суб'єктів відповідних відносин з метою вирішення конкретних завдань, то їхній перелік і конкретний зміст залежать від визнання існування певної сукупності однорідних норм.

Таким чином, слід визнати, що стосовно ІТ-права має йтися про «законодавство, що стосується ІТ», «законодавство, застосовне до відносин, що виникають у галузі функціонування ІТ», котре є сукупністю норм різної галузевої приналежності.

Отже, з позицій, так званого, «нормативістського» підходу, «ІТ-право», як галузь права, не існує.

Однак «ІТ-право» може оцінюватися і характеризуватися з погляду не лише «нормативістського», а й «цивілізаційного» підходу, згідно якому феномен права є елементом цивілізації (культури), котрому відводиться у структурі останньої важливе (і сказати б, неоднозначне) місце.

Як слушно наголошував С.С. Алексєєв, забезпечення існування та функціонування суспільства, як складної динамічної системи, є лише одним з напрямків регулювання, що здійснюється правом. Разом із тим, право у якості явища цивілізації, покликане бути носієм вищих принципів, базових цінностей цивілізації. Воно має реалізувати історичне призначення суспільства, пов'язане зі ствердженням у ньому сили розуму, високих гуманітарних засад. Отже, суть феномена права, як явища, котре відображає вимоги цивілізації, не обмежується лише тим, що право нормативно об'єктивує та реалізує ці вимоги, але також воно є чинником індивідуального самовираження особи, творчості, їх акумуляції, самозростання [3, с. 200, 219, 221, 224].

Таким чином, право є не лише елементом соціально-політичного устрою, але й має бути складовою духовного світу людини та її світогляду, виступає результатом прояву ментальності та елементом суспільної свідомості.

При розгляді його під таким кутом зору, право може бути охарактеризоване як властивий цивілізації феномен, що виступає як елемент соціально-політичного устрою та елемент суспільної свідомості, є складовою духовного світу людини та її світогляду, відображаючи уявлення окремих індивідів та суспільства в цілому про статус людини, правду і кривду, справедливість, добро і зло, порушення та поновлення прав, злочин та покарання, гуманізм і жорстокість тощо.

На такому підґрунті, у свою чергу, логічним є розуміння права як концепту (від лат. «conceptus» – думка, уявлення, поняття).

Концепт у філософії визначають як ідею, згусток смислів, з яких сотворяється буття усього – людини, світу, культури – людини у світі культури. При цьому на відміну від понять у

точному значенні терміну, концепти не лише мисляться, вони «переживаються», бо стосуються емоційної сфери людини, виступаючи як предмет емоцій, симпатій та антипатій, а іноді й зіткнень. Відтак, йдеться про уявлення, поняття, знання, асоціації, переживання, що супроводжують слово [4, с. 40].

Отже, концепт може бути визначений як виражені вербально ідея, уявлення, відчуття, що відображають сприйняття людиною світу і світом людини.

Оскільки концепт поєднує об'єктивні (світ, людина) та суб'єктивні (ідея, уявлення, відчуття) складові, виникає проблема надання пріоритетності першій чи другій з них. З одного боку, концептуальний аналіз - це аналіз концептів, під якими розуміються культурно-ментально-мовні утворення, що структурують смисловий простір культури. З іншого,- він виступає як спосіб дослідження, який здійснюється за допомогою використання концептів. На відміну від попереднього, такий підхід доцільно іменувати «концептним». (Тут варто згадати, що у правознавстві часом не розрізняють такі категорії як «концепт» і «концепція», використовуючи, як рівнозначні, то одне, то інше позначення [5, с. 69-73], що з позицій, викладених вище, навряд чи, можна визнати коректним).

Отже, розглядаємо далі концепт і як предмет дослідження, і як засіб проведення дослідження, припускаючи у другому випадку можливість та виправданість суб'єктивних оцінок концепту права (ІТ- права) та правових концептів (концептів у галузі права).

Враховуючи ту обставину, що право розглядається як елемент культури, логічно при його характеристиці розуміти «концепт» як сукупність («жмут») уявлень, понять, знань, асоціацій, емоцій, котрі виникають у зв'язку з використанням терміну «право», супроводжують і характеризують його.

«Правовий концепт» визначається як одна з форм мислення, результат узагальнення відомостей у галузі права та власного життєвого досвіду або сукупність поглядів на правове явище крізь призми суб'єктивного розуміння на підставі власного життєвого досвіду та правових знань. При цьому правовий концепт, як результат розумової діяльності,

відрізняється від правової категорії та правового поняття тим, що в ньому присутній суб'єктивний чинник. Тобто, правовий концепт не завжди є науково обґрунтованим, тому що складається з відомостей, які має суб'єкт про те чи інше правове явище [6, с. 386].

Таке положення кореспондує характеристиці сутності концепту, яку давав Жан Луї Бержель, зазначаючи, що визначення останнього спирається на аналіз самого концепту, тоді як визначення категорії відштовхується від іншої категорії. Для того, щоб описати концепт, останній слід розглянути, як такий. Натомість, для опису певної категорії необхідно виокремити зв'язки, що об'єднують одне з одним елементи, які утворюють цю категорію, і специфічні риси, котрі відрізняють ці елементи від інших елементів. Звідси випливає, що визначення концепту має підґрунтям аналіз самого концепту; визначення категорії ґрунтується на іншій категорії. Іншими словами, визначення концепту полягає в тому, щоб передати сенс слова, яким цей концепт позначається у відповідності з елементами, які цей концепт утворюють [7, с. 342].

Варто підкреслити, що коли йдеться про загальні концепти, які складають підґрунтя знань та уявлень про оточуючий людину світ, обмежуватись концептами у сфері позитивного права було б хибним, оскільки «позитивне право» само є лише одним із концептів у галузі права (так само як концепти «природне право», «приватне право», «публічне право», «право справедливості», «нормативне право», «цивільне право» тощо). Ці та інші концепти перебувають у складній системі координаційних, субординаційних, реординаційних тощо зв'язків. Відмова від врахування цієї обставини означала б зведення права взагалі лише до права позитивного, без врахування усіх інших його проявів. Тому при характеристиці концепту права та його елементів має йтися про сформоване вербально уявлення, раціональне та емоційне сприйняття людиною права як частини світу, у якому існує ця людина, відчуваючи себе частиною цього світу.

Підсумовуючи викладене вище, можна сформулювати бачення концепту таким чином.

По-перше, концепт є феноменом, що забезпечує пізнання людиною світу і себе та свого місця у світі. Він має низку спільних рис з терміно-поняттями «категорія» та «поняття», але не є тотожним їм.

По-друге, терміно-поняття «концепт» є полісемантичним і може застосовуватися у багатьох галузях знань (у філософії, логіці, культурології, лінгвістиці, праві тощо.

По-третє, якщо у галузі філософії, лінгвістики тощо «концепт», як такий, слугує самостійним предметом дослідження, то у галузі права він може застосовуватися також у якості методологічного прийому.

По-четверте, при дослідженнях у сфері права необхідно розрізняти базові концепти (право, справедливість, приватне право, публічне право, суб'єкт права, власність, договір тощо) і «правові концепти» (закон, законодавство, галузь права, правовий інститут, правова норма, судовий захист, позов, представництво тощо). До останніх належить й ІТ- право.

Запропоноване розуміння сутності концепту і права, як концепту, дає можливість визначити ІТ- право як сукупність («жмут») уявлень, понять, знань, асоціацій, емоцій, що виникають у зв'язку з використанням цього терміну, супроводжують і характеризують його. У свою чергу, підґрунтям концепту «ІТ-право» є концепт «ІТ-відносини», що поєднує як реальні, так і віртуальні (значною мірою) стосунки, тісно поєднанні і переплетенні між собою.

Розуміння ІТ-права, як концепту, дає можливість визначити критерії відбору норм законодавства, що можуть бути застосовані (обслуговують) зазначену сферу, без застереження щодо їхньої «мультидисциплінарності» тощо.

На цьому ж підґрунті, «ІТ-право» може розглядатися як навчальна дисципліна, предметом вивчення якої є фахове уявлення про правові концепти у цій сфері, концепція та практика правового регулювання відносин, що виникають у зв'язку з виникненням та використанням інформації та інформаційних технологій.

Список літератури

1. Дисципліна – Вікіпедія. – [Електронний ресурс]. – Режим доступу: https://uk.m.wikipedia.org;
2. Цивільне законодавство України (основні категорії, принципи та концепти) : монографія / авт. кол.; за заг.ред. Є.О. Харитонова. – Одеса : Фенікс, 2012. – С.17-27;
3. Алексеев С.С. Право: азбука – теория – философия: Опыт комплексного исследования / С.С. Алексеев. – М. : Статут, 1999. – С.200 , 219, 221, 224;
4. Степанов Ю.С. Константы. Словарь русской культуры. Опыт исследования / Ю.С. Степанов. – М. : Школа «Языки русской культуры», 1997. – С. 40.
5. Татарникова К.Г. Концепт комплексної кодифікації законодавства про інформацію / К.Г. Татарникова // Юридичний вісник. – № 3 (28). – 2013. – С. 69-73.
6. Ткаченко І.М. Розмежування термінів: «правове поняття», «правова категорія» та «правовий концепт» (на прикладі норм цивільного кодексу України) // Ученые записки Таврического национального университета им. В.И. Вернадского Серия «Юридические науки». – Том 22 (61). – № 1. – 2009. – С. 386.
7. Бержель Ж.-Л. Общая теория права / Под общ. ред. В.И.Даниленко : [пер. с фр.]. – М. : Издательский дом NOTA BENE, 2000. – С. 342.

Харитонова О.І.
завідувач кафедри права інтелектуальної власності та корпоративного права
Національного університету «Одеська юридична академія»,
доктор юридичних наук, професор,
член-кореспондент Національної академії правових наук України

ПРОБЛЕМНІ ПИТАННЯ ВИЗНАЧЕННЯ СИСТЕМИ (СТРУКТУРИ) ІТ-ПРАВА

Виходячи із загального розуміння ІТ-права як сукупності норм і правил, що опосередковують діяльність по забезпеченню безпеки інформаційних технологій та інформаційної активності в мережі Інтернет, спробуємо встановити структуру останнього.

Варто зазначити, що зараз до сфери його правового регулювання відносять широке коло відносин. Зокрема, до ІТ-права включають норми цивільного, господарського, адміністративного, карного, митного, податкового права.

Особливо багато різноманітних ІТ-відносин виникає у сфері цивільно-правового регулювання.

Зокрема, це:

1) ІТ-договори надання послуг програмного забезпечення або його розробки;

2) ІТ-договори роботи із ФОП або програмістами;

3) юридичний супровід фрі-лансерів;

4) юридичний аудит ІТ-компаній;

5) правовий захист web-сторінок і контенту;

6) оформлення та захист авторських прав і торгової марки в мережі Інтернет;

7) оформлення договору купівлі-продажу сайту, домену, бренду тощо;

8) правове забезпечення діяльності інтернет-магазинів;

9) створення і реєстрація юридичних осіб у цій галузі;

10) ліцензійні угоди;

11) захист прав інтелектуальної власності;

12) захист інформації тощо.

Таке розмаїття відносин, котрі вважаються «айтішними», створює на практиці істотні незручності при пошуку актів законодавства, що застосовуються для регулювання того чи іншого виду таких відносин; пошуку та систематизації матеріалів практики; субсидіарному застосуванні норм законодавства, застосуванні аналогії закону тощо.

Отже, маємо визначити орієнтири для встановлення кола норм, які можуть бути віднесені до сфери «ІТ-права».

Почати, вважаю, слід з винесення за межі ІТ-права норм адміністративного, карного, митного, податкового тощо права, оскільки зазначені галузі, як управлінські та охоронні, стосуються (можуть стосуватися) різних видів суспільних відносин, забезпечуючи їхнє впорядкування та охорону. Рівною мірою це можуть бути, скажімо, підприємницькі, аграрні, транспортні, екологічні тощо відносини. Навряд чи, є достатні підстави для включення норм згаданих «забезпечуючих» галузей до складу кожної галузі чи підгалузі права, котру вони «обслуговують». В іншому разі, довелось би книги «Право власності та інші речові права», «Право інтелектуальної власності», «Зобов'язальне право», «Спадкове право» вилучати

з Цивільного кодексу, а відповідні розділи цивільного права виводити за межі цієї галузі, оскільки відносини, які регулюються нормами, що містяться в цих книгах, «обслуговуються також нормами адміністративного, карного, митного, податкового тощо права».

Отже, до сфери дії, власне, ІТ-права доцільно відносити лише регулятивні відносини, і відповідно, норми законодавства, що їх регулюють.

Наступним кроком систематизації та структурування ІТ-права має бути розрізнення цього поняття у широкому та вузькому сенсі.

Під ІТ-правом у широкому сенсі розуміємо сукупність усіх норм і правил, що регулюють діяльність по використання інформаційних технологій та інформаційної правомірної активності в мережі Інтернет.

Структура ІТ-права у широкому сенсі виглядає як відносно інтегрована система багаторівневого порядку, що містить приватноправові та публічно-правові елементи. Необхідність врахування приватноправового та публічно-правового забарвлення ІТ-відносин має враховуватися, аби визначити пріоритетність інтересів (приватні чи публічні) і на цьому підґрунті особливості методів правого регулювання, що застосовуються. Разом із тим, публічно-правові за своєю сутністю ІТ-відносини, можуть складатися і у галузі цивільного права. Наприклад, такими є відносини цивільної відповідальності за шкоду, завдану цивільними правопорушеннями у сфері ІТ-відносин. Вони виникають не з правомірних дій; їхні суб'єкти, зміст, підстави і порядок виникнення та припинення визначаються безпосередньо нормами законодавства. Згадані вище відносини за своєю сутністю є або організаційними, або охоронними і ніколи не бувають регулятивними. Врахування цієї обставини має прагматичне значення, оскільки на практиці потребує врахування тієї обставини, що такі відносини регулюються лише нормами актів законодавства і не можуть бути змінені або припинені за домовленістю.

ІТ-відносини, пов'язані зі створенням та припиненням юридичних осіб, відносини інтелектуальної власності, договірні

відносини за участі суб'єктів ІТ-відносин, відносини спадкування тощо, належать до приватноправової сфери правового регулювання. Такі відносини переважно мірою є регулятивними, але у деяких випадках можуть також супроводжуватися цивільними організаційними відносинами (у галузі створення та діяльності юридичних осіб). Оскільки йдеться про сферу приватного права, де діє принцип «Дозволено все, що не заборонено законом», існування якого забезпечує надання договору значення норми цивільного законодавства, можна стверджувати, що саме за допомогою складається основний масив норм ІТ-права.

Таким чином, ІТ-право у вузькому сенсі це регулятивні норми (переважно цивільно-правові), що забезпечують функціонування ІТ-відносин.

Перед тим, як зробити спробу визначити структуру ІТ-права у вузькому сенсі, слід зробити застереження стосовно того, що тут здається необхідним виокремлення групи норм, присвячених загальним положенням законодавства, котрі стосуються ІТ-права. Не варто відтворювати хиби інституційної системи, де відсутність загальної частини створювала чимало незручностей, котрі були усунені лише після створення пандектної системи побудови права.

Із врахуванням зазначеного, структура ІТ-права у вузькому сенсі, як на мою думку, має виглядати наступним чином:

1) загальні положення (норми) цивільного законодавства, що стосуються ІТ-відносин (можуть бути застосовані для регулювання ІТ-відносин). До них належать засади цивільного законодавства; положення про аналогію закону та аналогію права; підстави виникнення цивільних прав та обов'язків у сфері ІТ-відносин; самозахист та захист суб'єктивних прав; положення про об'єкти цивільних прав, зокрема, про інформацію, як такий об'єкт; положення про правочини; представництво; строки та терміни; захист особистих немайнових прав фізичної особи тощо;

2) положення цивільного законодавства (норми), що стосуються суб'єктного складу ІТ-відносини. Сюди мають бути віднесені положення про створення та припинення юридичних

осіб; визначення видів юридичних осіб і форм товариств, які можуть створюватися для забезпечення діяльності у ІТ-сфері; положення про внесення продуктів ІТ у якості частки у статутному фонді; норми, що опосередковують внутрішньо корпоративні відносини; захист прав корпорацій;

3) положення (норми) цивільного законодавства, що стосуються прав інтелектуальної власності. Зокрема, положення, що стосуються визначення інформації та об'єктів прав інтелектуальної власності; правового обслуговування програмного забезпечення; захисту інформації та прав інтелектуальної власності; оформлення та захисту авторських прав і торгової марки в мережі Інтернет; правовий захист web-сторінок і контенту; положення про ліцензійні угоди тощо;

4) положення (норми) цивільного законодавства, що стосуються договорів у сфері ІТ-відносин. Зокрема, загальні положення про договори, їх укладення, зміну, виконання, припинення та способи забезпечення належного виконання; договори про надання послуг програмного забезпечення або його розробки; договори роботи із ФОП або програмістами; договори про юридичний супровід фрі-лансерів; договори про юридичний аудит ІТ-компаній; договори купівлі-продажу сайту, домену, бренду тощо; договори про правове забезпечення діяльності інтернет-магазинів; концесійні договори; ліцензійні угоди; договори про сумісну діяльність у сфері ІТ-відносин тощо;

5) положення (норми) цивільного законодавства, що стосуються недоговірних відносин у сфері ІТ. Зокрема, положення про оголошення винагороди, конкурсу щодо продуктів ІТ; діяльність у сфері ІТ-відносин в інтересах іншої особи без її доручення; відшкодування шкоди, завданої у сфері ІТ-відносин; повернення безпідставного отриманого (збереженого) майна у сфері ІТ-відносин тощо;

6) положення (норми) цивільного законодавства, що стосуються спадкування у сфері ІТ-відносин. Зокрема, положення, що стосуються складання заповіту на продукти ІТ-відносин та його виконання; спадкування інтелектуальної власності на продукти ІТ, авторських прав на них тощо; поділ

успадкованих прав на продукти ІТ між кількома спадкоємцями; переходу прав на продукти ІТ за спадковим договором тощо;

7) положення (норми) сімейного законодавства, що стосуються виникнення права спільної сумісної власності права подружжя на продукти ІТ та права спільної часткової власності членів сім'ї на такі продукти; поділ спільної сумісної власності подружжя на продукти ІТ; встановлення права власності на продукти ІТ за шлюбним договором; захист прав неповнолітніх членів сім'ї у ІТ-відносинах тощо.

Варто зазначити, що запропонована вище структура може стосуватися не лише ІТ-права у вузькому сенсі, але й інших подібних нормативних масивів (скажімо, підприємницького права, корпоративного права та ін.). Тому доцільно звернути увагу на можливість виокремлення «ІТ-права у спеціальному сенсі». При цьому до відповідного нормативного масиву мають бути віднесені вже лише ті норми, що стосуються суто сфери ІТ-відносин: інформаційних відносин; відносин створення та використання програмного забезпечення; інтернет-відносин та деяких інших.

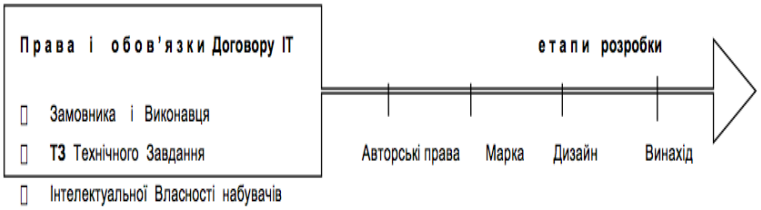
Структура (система) ІТ-права, що пропонується тут, не є, очевидно, бездоганною. Але створення такої системи, власне, і не було метою цієї розвідки, оскільки наразі важливіше привернути увагу до необхідності створення відповідної системи, ніж пропонувати готовий кінцевий результат.

Черкашин В. –
директор юридичної та патентної фірми
«Черкашин і Партнери»,
експерт МЮ

ВИНИКНЕННЯ ТА ОХОРОНА IP-RIGHT В IT- ДОГОВОРАХ

Всередині кожної інформаційної технології поштучно виникають і закріплюються об'єкти права інтелектуальної власності передбачені ст.420 Цивільного кодексу України. Технічні завдання і виконання Договорів ІТ-ТЕМИ /**ІТД**/

обов’язково пов’язані з «правовою начинкою» теми творчими продуктами **/ТП/** у вигляді кількох об’єктів інтелектуальної власності /**ОПІВ/.**



На етапах технічного завдання **/ТЗ**/, розробки, дослідження, виконання та запуску нового продукту **ІТ-договором** плануються контраверсійні заходи юридичного закріплення прав сторін Договору по **пріоритету, обсягу і змісту низки прав ІВ**, що складають «творчі нутрощі» виконаної теми.

Майбутня інтелектуальна власність, її правовий режим, виникнення та юридичне закріплення об’єктів права ІВ пов’язані зі складними процедурами **патентування, розмежуванням ОПІВ** між співавторами, сторонами ІТ-договору, співвиконавцями, тощо.

Згадані задачі віддзеркалюються при розробці ТЗ теми, саме на цьому етапі вирішуються **колізії між замовником та програмістами**, особливо щодо логіки тотожності у спільному творчому завданні.

Без знань суті одне одного, замовник та виконавець витрачають до 70% часу на ТЗ, постановку завдання, погодження умов, варіантів і методів виконання, **прав на отримання новітнього програмного продукту**, особливо при його пуску і налагодженні.

Тематика ОПІВ всередині інформаційних технологій подібна до інших «**стикових тем**», наприклад, ОПІВ у Договорах зовнішньоекономічних відносин, мало висвітлюється в фаховій літературі як комплексна і стикова, тому має значний практичний інтерес.

1. Об’єкти права інтелектуальної власності (ОП ІВ)

В умовах тотальної електронізації юридичне закріплення цивільно-майнових відносин в інформаційних технологіях значно ускладнюються проблемами правого режиму інтелектуальної власності, що закладаються у тексти ІТ – Договорів **/ІТД/** та народжуються під час науково-дослідних робіт у вигляді **творчих** результатів /далі **ТР**/.

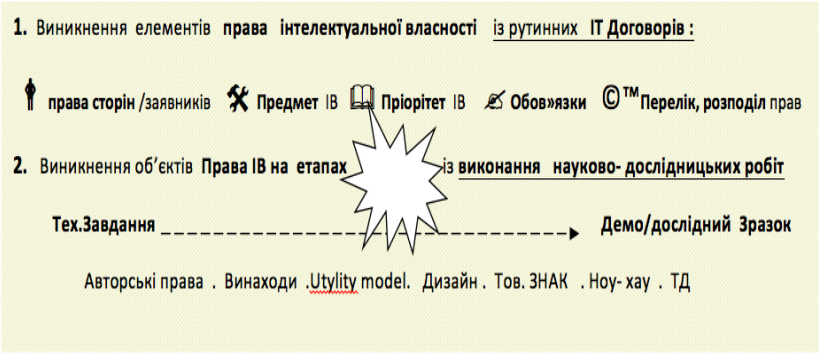
Перелік творчих результатів /**ТР**/ визначений законодавцем [18] ст. 420 Цивільного кодексу України як перелік об’єктів права інтелектуальної власності /далі **ОПІВ**/ за списком з 12-ти назв, що по суті виступають у майновому обігу як нематеріальні активи **/НМА/**. Зі зазначених ОПІВ у практиці ІТ-договорів використовуються не більше семи.

Виникнення нематеріальних активів у дослідницьких роботах,що супроводжуються **ІТ** мають два **джерела походження**:

– традиційні рутинні системи /події, що комп'ютеризуються / продаж білетів

– технічні завдання до науково-дослідницьких робіт /пошук джерела енергії

СХЕМА 1

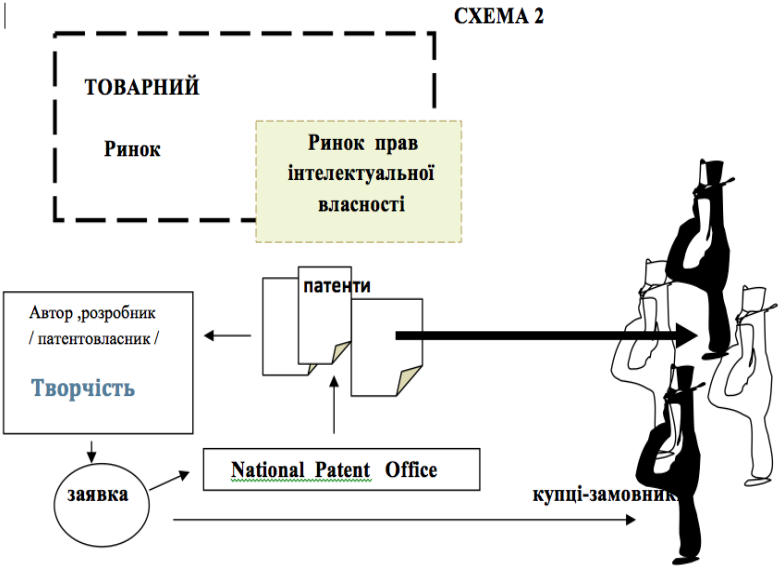


В обох варіантах важливішим завданням є оформлення прав у об’єктивну форму, що годиться для відповідного правоутворюючого документу країни: PCT, EU патенти, сертифікати, тощо. При порівнянні джерел 1-го і 2-го варіантів **Схеми 1** видно, що зміст елементів 1- варіанту **в ІТ-договорах**

та при **виконанні** 2-го варіанту /**науковомістких НД Тем/** - значно різняться обсягом, якістю та змістом творчості.

Цікаво, що при складанні проектів ІТ-договору згадані ОПІВ закріплюються у договорі переважно **як планові об'єкти,** які очікуються за суб'єктивними вимогами замовника .

У плануванні ІТД складається правова колізія, коли **виконавець ІТД** не спростовує уяву замовника, щодо **рівня творчості (креативності) результатів** замовленого і/або виконаного дослідження. Проблеми доцільності та охороноспроможності розробки розглядаються тут окремо, при розгляді доцільності патентування розробки /стор. 6-9/.



За досвідом, більшість розробок виконавця ІТ -договорів запозичуються або компілюються контрафактними частками типу – **«костюм Арлекіно»**, переносом рішень з існуючого досвіду, літератури, публікацій, дизайну, Інтернету, тощо, без патентно-правової аналітики перевірок суттєвих ознак запозичених рішень.

Важливо зауважити колізії сторін Договору щодо філософії **«планування» творчості** [11,12] на рівні світової новизни, коли замовник намагається запланувати творчість ІТД,

невиправдано вимагає результатів та їх привласнення на умовах упереджених думок про «.. найвищу, світову якість» замовної теми.

Такі суперечки сторін ІТД спростовуються посиланнями на норми (умови) технічного завдання **/ТЗ**/ теми, змістом замовних етапів, виконання їх результатів /винаходи, дизайн, знаки, авторські права, комерційні таємниці, тощо/ [24].

Планування творчості при виконанні теми завжди викликало спори фахівців щодо можливості прогнозування і планування достовірних творчих результатів в стислих строках виконання. /… **Nota bene ! Let make invention tomorrow !.... /.** Це протиріччя було блискуче спростовано американськими вченими, що з 1920 р. працювали над методами та технологіями творчості синектика, морфологічний аналіз, тощо) [26].

Доктор Мілан Мікулаштик /**Чехія**/ в роботі «Творчість і іновації у процесі робіт» /С**REATIVITY AND INNOVATION IN PROCESS OF WORK/** згадує історичне становлення синектики, поділяє думку про необхідність планування творчості [11].

Посилаючись на власну статистику пошуку запланованих творчих рішень, методом Функційно-Вартостевого Аналізу /ФВА/, інших синектичних методів, автор вважає планування творчості доцільним.

У кожному разі твори та інші різновиди ОПІВ, юридично закріплювати планово визначені об’єкти інтелектуальної власності, налаштовані більшість сучасних ІТ груп [4,6].

Поділ прав інтелектуальної власності

Починаючи розробку тимчасові творчі колективи, роботодавці, співавтори, набувачі прав, у яких виникає спільне майно, приречені **юридично закріпити поділ прав** на творчі результати, оскільки ці результати потім виступатимуть в майновому обігу як об’єкт власності, м**айно у вигляді прав:** «Результати інтелектуальної творчої діяльності» (ст. 199 ЦКУ) , «Інформація» (ст. 200 ЦКУ), «Особисті немайнові блага / ім’я, ділова репутація (ст. 201 ЦКУ) [18].

За ознаками оцінки творчого внеску правової концепції, ще з Кодексу Наполеона був закріплений статус **«пріоритету купця перед творцем»**, а наш законодавець встановив правило

службового твору в ст. 16 Закону України «Авторське право на службові твори» [22], де права поділено:

(ч.1) – Авторське особисте **немайнове** право **/АОНП/** – **автору /творцю /**

(ч.2) – **Виключне** */див. монопольне/* майнове право **/МП/** – **купцю**

Слід пам'ятати, що до згаданого закріплено примітку**… якщо /ч. 2 ст.16 [22].**

Таким чином норми Цивільного кодексу України ділять авторські права на дві групи: майнові – немайнові. Співвідношення особистих немайнових прав інтелектуальне права ІВ з майновими правами ІВ дістало юридичне закріплення ст. 423-424 ЦКУ [18].

Майнові частки права на твір можуть ділитися співавторами на частки за власним бажанням, та вказівкою про творчий внесок. Така вимога записується у ІТ-договори не як імперативна норма, але як рекомендація до психології рівноваги співавторства творчого колективу[22].

Поділ майна у вигляді ОПІВ, як авторського внеску, частки ознак патентів, часток художніх проектів дизайну, програмного продукту, завжди супроводжується передбаченими спорами **щодо кількості та якості творчої участі особи у створенні продукту:** хто, коли, при яких обставинах проголосив, подав ідею, яка ця ідея т.д.

Колізії вирішуються колективно, прозоро, дослідженнями рівня творчої участі усіх учасників творчого процесу, бажано до реалізації проекту на ринку. За результатами перемовин співавторам рекомендується підписання Протоколу з погодженням частки творчої участі кожної особи.

2. **СТОРОНИ**

При укладанні ІТД слід усвідомити осіб, які виступають **суб'єктами прав ІВ.**

Сторони Договору, юридичні і/або фізичні особи, складають іноді багатоланкову структуру на кожному боці [8].

Сторона 1 (**творці**). Ідеєтворці, автори/співавтори, роботодавці, розробники, діячі мистецтва та культури, в залежності від завдань, планів виконання, рівня кваліфікації, службових вимог набувають права інтелектуальної власності та

відповідні обов'язки закріплені національним та міжнародним законодавством [18, с. 186].

Сторона 2 (**купці).** Сторони в ІТ-договорі фіксують зміст прав інтелектуальної власності кожний на своїй стороні. Зважаючи на випадки службової творчості **[18, ст. 16]** замовник вважає майнові права ІВ своєю власністю і забезпечує заходи повного привласнення ОПІВ у вигляді Сертифікатів, патентів, технічної документації, тощо [19].

Забезпечення прав інтелектуальної власності, інтересів сторін ІТД в часі та просторі сфери ІТ вимагається як :

- своєчасне , випереджаюче;
- повне, без прогалин;
- вимоги /claims/ «сильної» правової охорони.

Розробники, програмісти, фахівці, розуміючи прогалини у праві і неефективне правосуддя в Україні воліють шляхи технічних засобів забезпечення власних авторських прав /коди, Е- ідентифікація, тощо/, вважаючи їх /технічні засоби захисту авторських прав/ надійними і незворотними, що закріплюють власні права на ІВ, шляхом включення в ІТ-договір вимог щодо нерозголошення програмного коду, інших зобов'язань проти контрафакції.

3. Доцільність витрат на патентування та заходи , що закладаються у ІТ-договори перевіряється за трьома принципами визначеними у Глосарії Патентного Відомства США /*Glossary of Pt.Office of USA*/:

… «**Patents granted by the US Patent Office are only prima facie valid**». (Stringhem p.61)…*Видані патенти дійсні тільки на перший погляд …*

«**The Government grant of an exclusive right for a limited time».** *Виключні права видаються Державою на обмежений час.*

«**Public Domain Belonging to the people**». *Опубліковане належить народові.*

При визначенні доцільності патентування розрізняють протиречиві практичні та «законні» вимоги. **У Таблиці 1** здійснено порівняння практичних потреб /вигод / з нормативними критеріями патентоздатності кожного з об'єктів права інтелектуальної власності ОПІВ .

Таблиця 1

P R A C T I C ABILITY / Practicable **Практична потреба отримання патентів**	**P A T E N T ABILITY/ Patentable** **Патентоздатність / норми – критерії охороноздатності /**
Вирішується під ліквідний рівень творчих непатентоздатних результатів	**Вирішується за нормою Закону країни патентування**
Ким : Вченою Радою,НТР, НР / Автором	**Вибраними країнами за географією патентування**
Етап : Стадія ідеї або освоєння продукту	**Державною Експертизою окремої країни**
Цензура : Список відомостей, режим носіїв .	**Нормами Міжнародних Угод**
Витратність: Ціноутворення та Official & Attornney Fee, пільги вибраних країн	

Висновки про доцільність заявок на патентування базуються на простих питаннях:

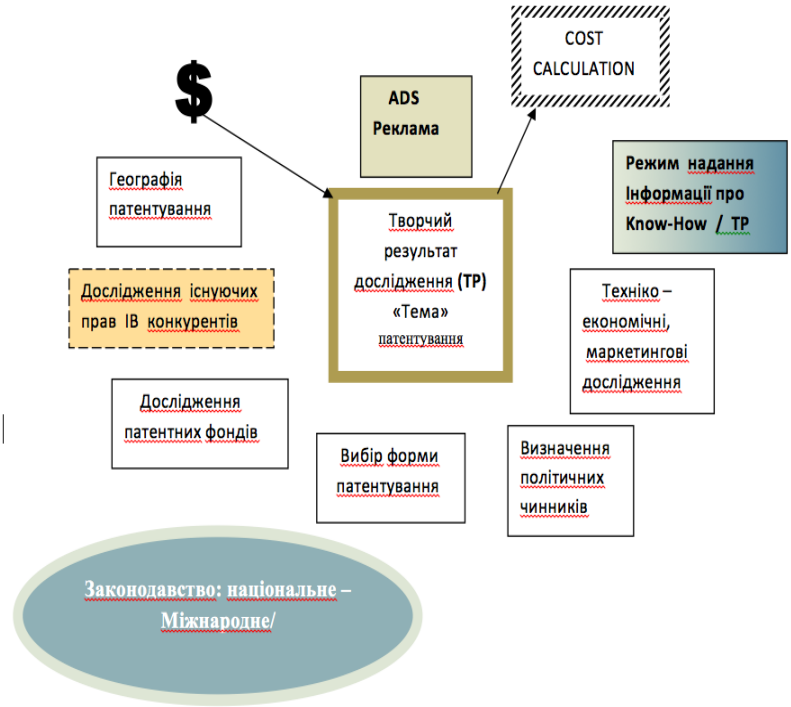
- Цілі патентування / охорона експорту - торгівля правами /
- Вартість патентування
- Конюнктура цільового ринку сегменту продукції
- Заважаючі патенти / « патентна чистота» продукту
- Географія патентування /особливості національного законодавства
- Строк дії патентів / поточна чинність
- Юридична сила заявленої формули /claims / «сильні патенти»
- Проблеми просування продукту /маркетинг VS режиму SR /
- Політичні чинники

Цілі патентування вагомих результатів загалом визначаються двома завданнями :

- **продаж ліцензій** на об’єкти права ІВ отримані в ІТД
- **правовий захист ПРОДУКЦІЇ українського експорту**

Для реалізації цілей планується та фінансується складний Комплекс досліджень і заходів

Схема 3



Послідовність запланованих заходів патентування жорстко регламентується на етапах виконання:

1. Завдання/ Пропозиції по темі
2. Призначення Теми дослідження / ТЗ про НДР /
3. Фінансування $
4. Виконання теми
5. Звіт про тему / рівень
6. Захист теми
7. План публікацій
8. Перші публікації , зразки ,виставки, пуско-наладки

9. Експорт/розмитнення
10. Супровід патентних спорів
11. Зовнішня торгівля

Наслідки прийняття рішення визначаються згаданими комплексними техніко-економічними та правовими дослідженнями, що плануються за власною логістикою («спочатку до юристів») по «портфелю» ОПІВ */ draft/.*

В А Р І А Н Т 1 Наслідки **додатнього рішення** про патентування креативу.

Затверджений портфель список ***(IP draft***) винаходів, промислових зразків, товарних знаків, секретів, дозволених до патентування, вимагає проведення у стислі строки у т. ч. міжнародних заходів:

1. **План** комплексної інформаційної та правової охорони по списку ОПІВ
2. Закриття каналів витоку інформації по суті / **цензура** /
3. **Патентні дослідження** рівня і пріорітету (Патентно-правовий висновок ,юридичні питання)
4. **Список заважаючих патентів** і їх власників (чистота)
5. **Конвенційні** переваги
6. **Конюктурний лист** маркетологічних досліджень ринку
7. **Заявки та описи** до кожного ОПІВ Драфту
8. **Ноу-хау** / закрите провадження
9. **Вибір способу та географії** патентування
10. **Мовні засоби** перекладання/ claims / в сучасних умовах
11. Планування залученя інвестицій та супутних установ
12. Розрахунок і конюнктура валютних витрат
13. Пропозиції до Замовника, тощо

В А Р І А Н Т 2 Наслідки **від'ємного рішення** про патентування ТР та відкритої публікації по суті новинки /вільний доступ до знань, ноу-хау/.

Історично доведено, що динаміка інвестицій співпадає з динамікою патентування базових винаходів в інтересах власної легальної патентної монополії /legal monopoly/.

Наведення відкритих посилань у Патентах, наприклад США, /*citation of references*/ дає можливість вивчення світового іноваційного рівня галузі знань, осіб патентовласників,

заявницький пріорітет власника, строки монополії, винахідницьку кон'юнктуру, тощо.

Більшість інвестицій у виробництво науковомістких виробів починають з забезпечення патентно-правової аналітики, звертаючись до **виключно релевантної інформації**, що стає базовою для алгоритмів патентно- правової політики у визначеному сегменті ринку збуту.

На жаль, пересічні замовники ІТД не знають, або не хочуть знати про існування нормативно-технічних вимог з обов'язкових ДСТУ України в частині патентних досліджень ОПІВ **/intellectual property/.**

Існують нормативно-технічні вимоги ДСТУ показників та вимог дотичних до робіт пов'язаних з інтелектуальною власністю [26-30] .

Такі ДСТУ у практиці ІТ- Договорів майже не застосовуються ні замовниками , ні виконавцями через складість їх виконання до рівня кожного стандарту .

Важливіши з них - ДСТУ 3574-97 **«Патентний формуляр»** та **ДСТУ 3575-97 «Патентні дослідження»** – є визначальними для тактики та стратегії управління правами інтелектуальної власності в структурі ІТ-Договорів.

Список літератури

1.Бачинський Т. Основи ІТ-права. Львів, Вид-во «Апріорі», 2016.

2.Зразок договору про надання ІТ послуг. – [Електронний ресурс]. – Режим доступу: http://dogovir.net/a179472-dogovr-poslug.html

3.Розробка програмного забезпечення: договір про виконання робіт чи надання послуг? Деякі особливі договори та поради щодо їх укладення у ІТ сфері. – [Електронний ресурс]. – Режим доступу: http://aphd.ua/publication-22/

4.Договор для ІТ-компаний. Чек-лист руководителя, который хочет выйти на западный рынок. – [Електронний ресурс]. – Режим доступу: http://ain.ua/2015/02/18/563850

5.Думаєте права на службовий ІТ продукт ваші? – [Електронний ресурс]. – Режим доступу: http://yur-gazeta.com/dumka-eksperta/dumaete-prava-na-sluzhboviy-it-produkt-vashi.html

6.Договір на розробку програмного забезпечення або сайту. – [Електронний ресурс]. – Режим доступу: http://vreshetov.com/ua/obrazcy-dokymentov/dogovora-predostavlenia-uslug/172-dogovor-na-razrabotku-saita

7.Важливі моменти договору про створення програмного забезпечення. – [Електронний ресурс]. – Режим доступу: http://go-advocate.com/vazhlyvi-momenty-dohovoru-pro-stvorennya-prohramnoho-zabezpechennya/

8.Новий тлумачний словник української мови. В 3-х т. – К.: Аконіт, 2004 – Т.3 – С. 501.

9.Дроб'язко В.С., Дроб'язко Р.В. Право інтелектуальної власності. – К.: Юрінком Інтер, 2004. – С. 470.

10. Brennan A., Dooley L., Networked Creativity: a StructuredManagement Frameworkfor Stimulating innovation, In Technovation (article in press), 2004.

11. Basadur M.S., Leading others to Think Innovatively together: Creative Leadership, In The Leadershio Quarterly, 15 (1), 2004, s. 103-121.

12. Прохоров-Лукін Г. Проблема встановлення факту відповідності ОІВ умовам надання правової охорони / Г. Прохоров-Лукін // Інтелектуальна власність. – № 11. – 2006.

13. Постульга В. Некоторые аспекты правового статуса информации с ограниченным доступом / В. Постульга // Юридическая практика. – 1998-2006.

14. Котляр Д. Комерційна таємниця в законодавстві іноземних країн та міжнародному праві // Інтернет-сайт «ВЯПат» (www.patent.km.ua)

15. Право інтелектуальної власності [Текст] : Наук.-практ. коментар до Цивільного кодексу України / М. В. Паладій [та ін.] ; заг. ред. М. В. Паладій [та ін.] ; Державний департамент інтелектуальної власності, АПН України, Інститут приватного права і підприємництва. – К. : Парламентське вид-во, 2006. – 432 с.

16. Черкашин В. Оформлення прав власності на «KNOW-HOW»: реєстрація та оцінка //VIP. – № 42 (215). – С. 4.

17. Цивільний кодекс України від 16.01.2003 року № 435-IV.

18. Господарський кодекс України від 16 січня 2003 року № 436-IV.

19. Закон України «Про державне регулювання діяльності у сфері трансферу технологій« від 14 вересня 2006 року № 143-V.

20. Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII.

21. Закон України «Про авторське право і суміжні права» від 11 липня 2001 року № 2627-III.

22. Закон України «Про власність» від 7 лютого 1991 року № 697-XII.

23. Закон України «Про державну таємницю» від 21 січня 1994 року № 3855-XII.

24. Закон України «Про захист економічної конкуренції» від 11 січня 2001 року № 462-II.

25. ДСТУ 3008-95 Документація. звіти у сфері науки і техніки. – [Електронний ресурс]. – Режим доступу :
www.sumdu.edu.ua/images/stories/...inf/.../dstu_3008-95.pd..

26. ДСТУ ГОСТ 2.052:2006 Єдина система конструкторської документації.

27. Електронна модель виробу. Загальні положення (ГОСТ 2.052-2006, IDT).

28. ДСТУ 3574-97 «Патентний формуляр. Основі положення.

29. ДСТУ 3575-97 «Патентні дослідження. Основні положення та ...

30. ДСТУ 3294-95 Маркетинг. Терміни та визначення основних понять.

Шишка Р.Б. –
в.о. завідувач кафедри цивільного і трудового права
Київського університету права НАН України,
доктор юридичних наук, професор

МЕХАНІЗМ ПРАВОВОГО РЕГУЛЮВАННЯ ПРАВОВІДНОСИН У СФЕРІ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Апріорі правове регулювання відносин у сфері інтелектуальної власності підпорядковано стимулюванню створення її результатів, насамперед найбільш витребуваних і значимих для життя та здоров' я людини, забезпечення довкілля, безпеки у суспільстві, їх використанню, забезпечення гідної винагороди творцям, і правомірним володільцям майнових прав, світового та національного правопорядку у цій сфері на основі запобігання правопорушенням, швидкого і ефективного їх виявлення, відновлення прав потерпілих та покарання винних. Це забезпечується через нормотворчу, правозастосовчу і правоохоронну діяльність у сфері інтелектуальної власності, де правове регулювання цих правовідносин здійснюється через вплив норм права та провозастосовної системи на їх елементи в межах визначених моделей їх упорядкування. Збій в певній частині призводить до відхилення в диспозиції норми права певного спрямування і потреби включати охоронні та захисні засоби: приватноправового, адміністративного чи кримінального походження.

Норми права інтелектуальної власності як і норми інших галузей та підгалузей права адресовані учасникам цих правовідносин, спонукають їх здійснювати свої цивільні права та виконувати обов'язки у бажаному для правопорядку та безконфліктному напрямку, а в разі виникнення конфлікту прав та охоронюваних законом інтересів – застосувати захист у порядку та у спосіб, що визначені законом. Врегулювання таких правовідносин досягається як існуванням самих норм права, так і правової системи, яка дозволяє втілити їх в життя і тим перевести їх із належного (визначена в нормах права мета

правового регулювання) у суще (відповідність реальних відносин приписам норм права). Ними є форми права, засоби та способи його застосування. Механізм трансформації положень норм права в практику отримав назву механізму правового регулювання. Загалом йдеться про переведення норми права чи нормативізму (позитивізму) у реальні правовідносини.

В правовій науці щодо механізму правового регулювання склались такі підходи як: 1) взята в єдності сукупність правових засобів якими забезпечується правовий вплив на суспільні відносини [1, с. 30] та складається з юридичних норм, правовідносин та актів реалізації суб'єктивних прав та здійснення юридичних обов'язків, а пізніше нормативних актів, правосвідомості та правової культури [1, с. 34-35]. В останніх роботах він відносить до механізму правового регулювання: юридичні норми; правові відносини, акти реалізації прав та обов'язків; 2) сукупність елементів, зв'язків і динамічних закономірностей, необхідних та достатніх для врегулювання одного елементарного акту поведінки [3, с. 71]; 3) послідовний ланцюг зміни окремих правових явищ: норма права, що регулює цивільні правовідносини; – юридичний факт – права та обов'язки учасників цивільних правовідносин – реалізація прав та виконання обов'язків – а, за необхідності, захист порушеного права чи охоронюваного законом інтересу [2, с. 43]. Не слід ототожнювати механізм правового регулювання та наслідками такого регулювання, зокрема законністю та правопорядком.

Категорії «механізм правового регулювання» чи «механізм регулювання правовідносин» активно використовується як опорні при моделюванні вирішення нагальних проблем та завдань правового регулювання. Це стосується врегулювання правовідносин у сфері інтелектуальної власності за напрямками: визначення охороноспроможних об'єктів та їх форм, засобів і способів; регулювання відносин на основі визначення у позитивному праві ідеальних моделей; охорона суб'єктивних прав правоволодільців, забезпечення їх захисту в разі порушення чи загрози порушення.

Парадокс наразі у тому, що немає його загальновизнаного розуміння і суб'єктивна опорна категорія, є сумнівним підґрунтям для їх проведення і отримання гідних результатів.

Можна погодитися, що механізм правового регулювання – узята в єдності система правових засобів, способів і форм, через які нормативність права переводиться в упорядкованість суспільних відносин, чим задовольняються інтереси суб'єктів права, встановлюється і забезпечується правопорядок («належне» у праві стає «сущим»). Це в повній мірі стосується й правовідносин у сфері інтелектуальної власності за напрямами: приватноправовий та публічноправовий.

Основними ознаками механізму правового регулювання є:

1. він є складовою механізму соціального регулювання взагалі і супроводжується політичним, економічним, етичним та іншим його видами;

2. охоплює явища правової дійсності: засоби (норми права, суб'єктивні права і юридичні обов'язки, рішення судів тощо, об'єктивовані в правових актах); способи (дозволення, зобов'язування, заборони);

3. передбачає форми (використання, виконання, додержання, застосування);

4. у своїй єдності є системою загальних та інституційних правових засобів, способів, форм, що перебувають у взаємозв'язку і взаємодії, де кожна з них виконує специфічні функції і впливає на зміст інших частин і зумовлює результат функціонування механізму в цілому;

5. є динамічною частиною правової системи суспільства згідно напрямів правового впливу та його стадій;

6. забезпечує правопорядок у суспільстві взагалі та у регулювання окремих відносин зокрема.

Підсистемами такого механізму є: механізм реалізації, який включає заходи, спроможні створити умови для реалізації прав і свобод людини; механізм охорони, який включає заходи з профілактики правопорушень для утвердження правомірної поведінки особи; механізм захисту прав включає заходи та способи, що призводять до відновлення порушених прав неправомірними діями і відповідальності особи, яка вчинила ці правопорушення. Кожна із них має своє завдання, засоби, способи та навіть форми.

В принципі розуміння правового механізму вже встановилось і не заперечується. Воно зводиться до того, що він

є важливим науково-гносеологічним поєднанням окремих елементів за допомогою яких забезпечується регулятивна та охоронна функція врегулювання цивільних правовідносин. При тому слід зважати на рівень такого регулювання: міжнародний (обов'язковий чи орієнтовний), національний, локальний і мононормативний.

По суті, право інтелектуальної власності у теперішньому виді виникло як частина міжнародного приватного права, де є значна частина нормативних актів (конвенцій) прямої дії, що проведені у національному законодавстві і тим забезпечує єдиний правовий простір. Окремі розбіжності є у публічній сфері, що зумовлено стратегією та тактикою забезпечення правопорядку у сфері інтелектуальної власності в окремих країнах та станом їх правової системи. У динаміці при здійсненні майнових прав інтелектуальної власності переважає мононормативне (договірне) регулювання.

Механізм правового регулювання відносин у сфері інтелектуальної власності – упорядкована система правових інститутів, які закріпляють можливість учасникам цих правовідносин оцінити свою діяльність при здійснення своїх прав та охоронюваних законом інтересів, а інших – утримуватися від свавільного втручання. Особливостями правового механізму регулювання цих правовідносин є:

1) встановлення тих його елементів, які забезпечують досягнення його мети;

2) визначення напрямків та засобів впливу на поведінку їх учасників ;

3) усунення колізій між окремими його елементами і недопущення їх дублювання;

4) приведення їх елементів до загальновизнаних вимог правового регулювання приватних відносин у світі та , зокрема для України, в країнах ЄС;

5) встановлення особливостей прояву цих елементів стосовно нових об'єктів цього права та сфер правового впливу.

Такі елементи є : обов'язковими (елементи самих правовідносин) або/та варіативними (стимули, обмеження тощо)

Загальновизнано, що метою правового регулювання є упорядкування суспільних відносин, зокрема їх закріплення,

визнання і охорона як певного стандарту у законодавстві, що визначає юридично значимі поведінку учасників цих правовідносин та оцінку її зі сторони держави, суспільства .

Встановлення розуміння механізму правового регулювання полягає у тому, щоб йому надати владно-державний характер, надати поведінці юридично значимий характер, заставити учасників правовідносин слідувати встановленим чи санкціонованим державою правилам поведінки і підпорядкувати їх правовому порядку. У приватній сфері, на відміну від публічної, ці стандарти суттєво міняються. З огляду на ст. 3 Конституції України наразі йдеться про задоволення прав та інтересів людини, витіснення та блокування деструктивних форм прояву їх поведінки чи свавілля. Гуманітарний аспект розвитку світового співтовариства – данина усвідомленню важливості людини та потреби розкрити її творчий інтелектуальний потенціал, після періоду ігнорування такого напрямку у правовому регулюванні по вернути у лоно загально визнаних цінностей. Тільки вільна людина здатна творити і вирішувати ті важливі економічні, соціальні проблеми, які загрожують існуванню цивілізації. В такому разі вона є елементом інтелектуального потенціалу суспільства, або споживачем результатів творчої інтелектуальної та подібної їм діяльності.

Задля цього обираються напрямки правового впливу на поведінку учасників суспільства взагалі і окремих правовідносин зокрема. Це досягається правовими засобами. До них належить виховання поваги до права та охоронюваних ним благ, інформація, технічні, а із введенням новітніх інформаційних технологій, і програмні засоби. Останні більше засновані на імперативах і передбачають безумовне приєднання до визначених програмними засобами способів, предметів та умов їх використання чи набуття на них прав. Зокрема у мережі Інтернет ці відносини є інтегрованими і забезпечувалися програмними і правовими засобами.

Механізм правового регулювання приватних відносин забезпечує переведення змісту правоздатності осіб, компетенції публічних утворень у конкретні суб'єктивні права та юридичні обов'язки, у даному разі у сфері інтелектуальної діяльності та

інтелектуальної власності. Якщо є суб'єктивні «ретранслятори» механізму виконання приписів, чи рекомендацій норм права, то приписи об'єктивного права перетворюються у їх протилежність, а право – у зло.

Трансформація правоздатності у суб'єктивні права та юридичні обов'язки є першим етапом у регулюванні у регулюванні цих правовідносин. Вона забезпечується завдяки встановленим законом підставам виникнення правовідносин – насамперед, як це встановлено у п. 2 ч. 2 ст. 11 ЦК України – створення результатів творчої, інтелектуальної діяльності.

Для розуміння системи підстав виникнення таких правовідносин може бути використано аналогію парасольки: у згорнутому виді – вона не функціональна, а за наявності дощу чи спеки розкривається і виконує своє призначення. Так само і чинне законодавство починає виконувати свою регулятивну роль у разі виникнення правовідносин на підставі певних юридичних фактів. Йдеться про переведенні міжнародних, національних чи локальних норм із «сплячого стану» в динаміку.

Визначальним елементом правового регулювання визнана норма права — нормативна основа механізму правового регулювання, яка охоплює інші його елементи. Вона встановлює можливий варіант поведінки (активної чи пасивної), визначає суб'єктивні права та можливості реалізувати охоронюваний законом інтерес, так і необхідний варіант поведінки – юридичні обов'язки. Завдання норми права в механізмі правового регулювання полягає в тому, щоб: а) визначити загальне коло учасників правовідносин (взагалі, у конкретних правовідносинах зокрема); б) встановити зміст суспільних відносин (зміст поведінки суб'єкта), а також об'єкти правовідносин; в) визначити гіпотезу чи обставини, за яких слід керуватися даним правилом поведінки; г) розкрити саме правило поведінки (диспозиція) вказівкою на права і обов'язки (зміст) учасників відносин, що регулюються, характер їх зв'язку між собою, а також державно-примусові заході, що можуть бути застосовані при невиконанні юридичних обов'язків.

Суб'єктивні права та юридичні обов'язки учасників правовідносин є також результатом правового регулювання.

Вони – пробний камінь механізму правового регулювання особливо у сфері інтелектуальної власності де є першосуб'єкт, як основний і «курка, що несе золоті яйця», та похідні суб'єкти. Якщо суб'єктивні права безперешкодно здійснюються, а юридичні обов'язки виконуються без примусу, то забезпечується його ефективність. Якщо ж навпаки, то слід встановити ті елементи правового механізму, які його не забезпечують, і їх виправити чи замінити.

Прагматизм правовідносин забезпечує послідовний ланцюг такого регулювання: на рівні формування волевиявлення до вступу у правовідносини де зважуються потреби, засоби чи способи їх забезпечення і можливі наслідки; на рівні конкретних елементів правовідносин. У позитивному праві це проявляється у структурі цивільного права: загальна частина де визначаються:

1) засади цивільного законодавства (ст. 3 ЦК), які уточнюють основні напрямки прояву «генетичного коду» приватноправового регулювання і встановлено напрямки впливу норм цивільного права. Вони є визначальними при оцінці дієвості інших компонентів правового регулювання суспільних відносин, а у разі лукунізму[14] на основі аналогії закону і права;

2) підстави їх виникнення та їх внутрішній зміст (ст. 11 ЦК), як різновид юридичних фактів. Більшість із них притаманні лише приватному праву. Для права інтелектуальної власності ними є створення результатів творчої, інтелектуальної та іншої діяльності, їх кваліфікація чи реєстрація, оприлюднення, передача майнових прав, спадкування того. Проте такі правовідносини можуть виникати із інших підстав, що не передбачені актами цивільного законодавства, але не заборонені ними ;

3) загальне правове становище учасників правовідносин, та випадки і наслідки відхилення від нього (Розділ II ЦК). Йдеться про право- та дієздатність, обсяг цивільних прав та обов'язків. Здебільше суб'єктивні права та юридичні обов'язки учасників правовідносин: передбачені актами цивільного законодавства. Якщо вони ними не передбачені, то діє загально

[14] Наявності прогалин.

дозвільний принцип. Законодавець формулює зміст правовідносин в актах законодавства. Проте учасники конкретних правовідносин у сфері інтелектуальної власності можуть відійти від ідеальної моделі їх змісту : зробити їх ширшими чи вужчими, якщо це не суперечить приписам закону; зробити їх змішаними і піддати під регулювання двох та більше інститутів цивільного права; надати їм комплексності та врегулювати нормами різної галузевої приналежності.

Правове становище учасників правовідносин у сфері інтелектуальної власності врегульовано наданням їм правових властивостей (правоздатності та дієздатності) і поступового зменшення їх обсягу від загального через спеціальне і до окремого чи виключного. Зокрема, це проявляється у співвідношенні категорій «юридична особа», «товариства» і «приватне акціонерне товариство». Для кожного із них у позитивному праві виписана загальна модель, яка передбачає надалі коло суб'єктивних прав та юридичних обов'язків і систему тих елементів механізму правового регулювання, які утримують його в «орбіті» такого правового регулювання.

Окремо заслуговує уваги поведінка учасників цивільних правовідносин щодо здійснення своїх прав та виконання юридичних обов'язків. Вона може вчинятися відповідно до диспозиції норми права, або відхилятися від неї. Якщо це становище погіршується виникає потреба застосовувати інший елемент – обмеження у здійсненні цивільних прав. Наближеним до обмежень[15], але не тотожними, є обтяження учасників цивільних правовідносин чи об'єктів цивільних прав як покладення на носія права певних обов'язків, які забезпечують

[15] Зокрема КМ постановою № 610 від 1 серпня 2013 р. процедуру перереєстрації транспортних засобів пов'язала із його борговими зобов'язаннями: перереєструвати автомобіль на нового власника неможливо, якщо: стосовно нього є постанова суду чи державного виконавця про накладення арешту; записані на неповнолітніх, без письмової нотаріально посвідченої згоди батьків чи піклувальників; якщо автомобіль отримано через органи соціального захисту населення чи Фонд соціального страхування від нещасних випадків на виробництві або професійного захворювання з їх дозволу; куплені у розстрочку - в разі наявності документів про кінцевий розрахунок.

права та інтерес и інших учасників суспільства чи є частиною правового режиму об'єкта права або правового становища суб'єкта права.

Також застосовуються стимули для мотивування бажаної поведінки їх учасників;

4) правовий режим об'єкта цивільних прав, що проявляється у специфіці набуття, здійснення та припиненні прав щодо нього. Тут визначається допустимість існування цих правовідносин щодо окремих об'єктів, їх оборотоздатність, специфіка та різновиди, способи здійснення прав;

5) параметри існування правовідносин у часі (строки, терміни) у просторі (місце виникнення, здійснення та припинення прав і обов'язків); виключення із загального положення про самостійне набуття та здійснення прав. Це зумовлене тим, що людина існує у просторі та у часі і ігнорувати їх неможливо.

На рівні окремих інститутів цивільного права додаються додаткові елементи механізму правового регулювання цивільних правовідносин, чи конкретизується їх зміст. Наприклад, договори як правовідношення регулюються завдяки такому елементу як спосіб його укладення – підстави виникнення, зміст договору.

Тож механізм правового регулювання правовідносин у сфері інтелектуальної власності – передбачені нормами права конструкції визначальних для права правових інститутів (предмет і метод, засади законодавства, підстави їх виникнення, правове становище учасників, правовий режим об'єктів, місце та час здійснення прав і виконання обов'язків), які визначають допустимість, вид та зміст цих правовідносин.

Список літератури

1.Алексеев С.С. Механизм правового регулирования в социалистическом государстве. – М.: Юрид. лит. 1966. – 187 с.

2.Погрібний С.О. Механізм та принципи регулювання договірних відносин у цивільному праві України : монографія. / С.О. Погрібний. – К.: Правова єдність. 2009. – 304 с.

3.Протасов В.Н. Что и как регулирует право. Учеб. пособие. М.: Юристь. 1995. – 95 с.

Яворська О.С.
завідувач кафедри інтелектуальної власності,
інформаційного та корпоративного права
Львівського національного університету ім. І. Франка
доктор юридичних наук, професор

ДОГОВОРИ У СФЕРІ ІНТЕЛЕКТУАЛЬНОГО ПРАВА: ПРОБЛЕМИ ЗАСТОСУВАННЯ ЧИННОГО ЗАКОНОДАВСТВА

Правовою формою, що опосередковує різні способи розпорядження майновими правами інтелектуальної власності та урегульовує відносини сторін, є цивільно-правовий договір. Такі договори структуровані в окрему групу – глава 75 ЦК України [1]. Якщо систематизація усіх цивільних договорів у ЦК України проведена за спрямованістю правового результату як от: договори про передання майна у власність чи користування, виконання робіт, надання послуг, то зазначена група договорів виокремлена за їх об'єктом (майновими правами інтелектуальної власності). Очевидно, що у такий спосіб підкреслюється специфіка як самих об'єктів, так і договорів, що опосередковують їх цивільний обіг.

У ст. 1107 ЦК України наведено невичерпний перелік таких договорів. Учасники цивільних відносин, опираючись на принцип свободи договору (ст. 6 ЦК України), можуть укласти і інший договір, що не передбачений актами цивільного законодавства, але відповідає загальним його засадам. Серед договорів такі, що спрямовані на створення об'єкта права інтелектуальної власності, так і такі, що спрямовані на використання уже існуючого об'єкта чи розпорядження майновими правами на створені об'єкти. Інколи це створює зовнішню подібність з договорами підрядного типу, з договорами купівлі-продажу майнових прав чи з договорами майнового найму. Тому важливою є правова кваліфікація договірного виду.

Як зазначено у п. 26 постанови Пленуму ВГС України від 17 жовтня 2012 року «Про деякі питання практики вирішення

спорів, пов'язаних із захистом прав інтелектуальної власності» [2] використання творів та/або суміжних прав, якщо інше не встановлено законом, допускається лише на підставі передбаченого ст. 1107 ЦК України договору щодо розпорядження майновими правами інтелектуальної власності. Така категоричність щодо правової підстави розпорядження авторськими майновими правами інтелектуальної власності є невиправданою, оскільки принцип свободи договору надає сторонам широкі можливості у виборі договірного регулювання. Але судову позицію слід сприймати у тому плані, що договори, перелічені у ст. 1107 ЦК України (а не будь-які інші, схожі за спрямованістю, змістом тощо), і є належною правовою підставою для встановлення, зміни та припинення інтелектуальних правовідносин. У постанові сформульовані узагальнені рекомендації щодо укладення таких договорів.

Відповідно до норм ст.ст. 31, 32 Закону «Про авторське право і суміжні права» [3] автор (чи інша особа, яка має авторське право) може передати свої майнові права будь-якій іншій особі повністю чи частково і таке передання оформляється авторським договором про передання виключного права на використання твору або на основі авторського договору про передання невиключного права на використання твору. Серед видів договорів щодо розпорядження майновими правами інтелектуальної власності, що наведені у ст. 1107 ЦК України, авторський договір не зазначено. Проте такий стан не викликає сумнівів щодо його легітимності, адже перелік договорів у ЦК України є невичерпним, а норми Закону «Про авторське право і суміжні права» підлягають застосуванню як спеціальні щодо норм ЦК України.

Серед видів договорів щодо розпорядження майновими правами інтелектуальної власності зазначена ліцензія на використання об'єкта права інтелектуальної власності. Ліцензія, як дозвіл на використання об'єкта, не є договором. Відповідно до ч. 2 ст. 1108 ЦК України ліцензія може бути оформлена як окремий документ або бути складовою частиною ліцензійного договору. Видача ліцензії користувачу майнових прав є одностороннім правочином, на підставі якого у нього і виникають відповідні права.

Ліцензійний договір, як це випливає зі змісту ст. 1109 ЦК України, набуває характеру універсальної правової підстави користування об'єктами права інтелектуальної власності. Зазвичай, про видачу ліцензії чи про укладення ліцензійного договору йшлося стосовно об'єктів права промислової власності (патентного права). У зазначеній статті не окреслена сфера застосування ліцензійного договору, тому на його підставі можуть передаватися і авторські права.

До групи договорів щодо розпорядження майновими правами інтелектуальної власності включений і договір про створення за замовленням і використання об'єкта права інтелектуальної власності. Саме укладення такого договору спрямоване на створення відповідного об'єкта, що вирізняє його за правовою спрямованістю результату від решти договорів. Зазначений договір має зовнішню подібність з договорами підрядного типу, оскільки на його підставі створюється новий об'єкт. Але відмінною його ознакою від договорів підрядного типу є власне спрямованість на створення та використання саме об'єкта інтелектуальної власності, а не будь-якого іншого. До правового регулювання відносин сторін підлягають застосуванню норми глави 75 ЦК та книги 4-ої ЦК України, норми спеціального законодавства. Також варто зауважити, що на підставі такого договору не може бути створеним об'єкт патентного права, оскільки такий результат стає об'єктом правової охорони з моменту отримання патенту, а не з моменту його створення на підставі договору.

Не варто упускати з поля зору договори організаційного характеру, що опосередковують створення, використання та розпорядження як об'єктів інтелектуальної власності, так і прав на них та виконують по суті допоміжні функції. Це, зокрема, договір між працівником та роботодавцем про створення службового твору, розподіл майнових прав інтелектуальної власності, умови виплати винагороди та урегулювання інших відносин у разі створенням об'єкта інтелектуальної власності у зв'язку з виконанням трудового договору. Такі відносини можуть урегульовуватися і трудовим договором (контрактом), а можуть бути предметом самостійного цивільно-правового договору між працівником та роботодавцем. Зазначений договір

у силу специфіки суб'єктного складу, його змісту, не «вписується» у жодну групу цивільних договорів.

Аналогічно щодо договору між співавторами творів, умовами якого визначаються взаємовідносини між співавторами різних творів, порядок, умови, способи використання творів, створених у співавторстві. Відносини між співавторами законодавчо не урегульовані. Усі відносини між ними можуть бути урегульовані саме договором. Такий підхід якраз і сприяє більш повному урахуванню інтересів усіх зацікавлених сторін. Тому договір між співавторами є єдиним регулятором їх відносин. Як і попередній договір його не можна віднести до якоїсь конкретної групи цивільних договорів.

Договір про створення аудіовізуального твору, який укладається між режисером-постановником, автором сценарію і (або) текстів, діалогів, автором спеціально створеного для аудіовізуального твору музичного твору з текстом або без нього, художником-постановником, оператором-постановником. Усі зазначені особи є авторами аудіовізуального твору відповідно до ст. 17 Закону «Про авторське право і суміжні права».

Договір між упорядником збірника, антології, енциклопедії та інших складених творів і авторами творів, які планується включити до таких збірників. Можливість укладення такого договору передбачена у ст. 19 Закону «Про авторське право і суміжні права», у якій зазначено, що такий договір є авторським.

За свою правовою природою це цивільні договори, які укладаються та виконуються з урахуванням положень договірного права України. Такі договори можливо охарактеризувати як організаційні, укладення та виконання яких спрямоване на організацію створення об'єкта інтелектуальної власності, розподілу майнових прав, визначення умов використання такого об'єкта тощо.

Майнові права інтелектуальної власності можуть бути предметом договору застави (ч. 3 ст. 424 ЦК України, Закон України «Про заставу»). У такому разі до відносин сторін, окрім законодавства у сфері інтелектуальної власності, застосовується заставне законодавство.

Майнові права можуть бути внеском до статутного капіталу юридичних осіб та передаватися у статутний капітал на підставі відповідних договорів. У разі внесення майнових прав до статутного капіталу юридичної особи, окрім зазначення про це в засновницькому договорі, необхідне укладення окремого письмового договору про передання виключного права між суб'єктом права та юридичною особою, до статутного капіталу якої передається право.

Таким чином, у групі договорів щодо розпорядження майновими правами інтелектуальної власності (хоч назва звужує функціональне значення окреслених договорів), можливо виділити:

за спрямованістю правового результату:

– договори, спрямовані на створення за замовленням та використання об'єкта інтелектуального права (наприклад, договір з аналогічною назвою – ст. 1112 ЦК України);

– договори щодо використання об'єкта інтелектуального права (наприклад, ліцензійний договір – ст. 1109 ЦК України);

– договори щодо використання майнових прав інтелектуальної власності (наприклад, ліцензійний договір на використання майнових прав – ст. 1109 ЦК України; договір про передання виключних майнових прав – ст. 1113 ЦК України);

– договори управління майновими правами інтелектуальної власності (можливість їх укладення випливає зі змісту ст. 47 Закону «Про авторське право і суміжні права»);

– організаційні договору, спрямовані на створення об'єкта інтелектуальної власності, розподіл майнових прав інтелектуальної власності, використання створеного твору (наприклад, можливість укладення договору між працівником та роботодавцем випливає зі змісту ст. 429 ЦК України).

за функціональним призначенням договору у механізмі використання об'єктів інтелектуальної власності та прав на них:

– основні договори, на підставі яких відбувається передання у використання самого об'єкта інтелектуальної власності або відповідних майнових прав на такі об'єкти;

– допоміжні, що урегульовують відносини, які передують створенню відповідного об'єкта або доповнюють основні.

Для прикладу, договір про передання майнових прав на аудіовізуальний твір як основний договір та договір про створення твору між відповідними суб'єктами як допоміжний од основного;

за закріпленістю (визначеністю, урегульованістю) у законодавстві:

– поіменовані договори (наприклад, ліцензійний договір, договір про передання виключний майнових прав інтелектуальної власності тощо);

– непоіменовані договори (договір про передання та використання ноу-хау).

Особливості майнових прав інтелектуальної власності на різні об'єкти правової охорони позначаються і на специфіці укладення та виконання відповідних договорів. Якщо у сфері авторського права діє презумпція авторства та автору не потрібно дотримуватися обов'язкових процедур щодо реєстрації своїх прав, то у сфері патентного права майнові права на відповідні об'єкти охороняються відповідно до закону тільки за умови дотримання режиму патентування. Відповідно, договори щодо розпорядження авторськими майновими правами можуть укладатися автором без будь-якого підтвердження прав з його боку. Тоді як договори щодо розпорядження майновими правами на об'єкти патентного права можуть укладатися лише за наявності у сторони відповідних правоохоронних документів (патентів, свідоцтв тощо).

Майнові права інтелектуальної власності мають строки чинності. Тому при укладенні відповідних договорів строки чинності майнових прав ураховуються обов'язково. А, відтак, усі договори щодо розпорядження майновими правами інтелектуальної власності так чи інакше є строковими. Якщо сторони і не домовилися про строки чинності договору, то чинність договору не може перевищувати граничних строків чинності відповідних майнових прав.

При укладенні зазначених договорів слід ураховувати і оборотоздатність окремих об'єктів інтелектуальної власності.

Зокрема, відповідно до ч. 2 ст. 490 ЦК України майнові права інтелектуальної власності на комерційне найменування передаються іншій особі лише разом з цілісним майновим комплексом особи, якій ці права належать. Тому неможливе окреме передання прав на комерційне найменування. Права інтелектуальної власності на географічне зазначення не включають повноваження щодо розпорядження ними (ст. 503 ЦК України). Більшість майнових прав інтелектуальної власності передаються вільно, без законодавчих обмежень.

До договорів, що визначені у ст. 1107 ЦК України, застосовуються загальні положення договірного права з урахуванням особливостей правового регулювання, викладених у главі 75 ЦК України, спеціальному законодавстві. Усі зазначені договори укладаються вільно. Конкурсні передумови укладення договору не передбачені, але не виключені при певних умовах. У ст. 1111 ЦК України передбачена можливість укладення ліцензійного договору на підставі типового. Пропозиції зразків укладення договору, що пропонуються у правозастосовній діяльності як типові, насправді не є типовими. Адже відповідно до ст. 630 ЦК України типові умови договорів певного виду оприлюднюються у встановленому порядку. Тобто, типовий договір – це такий, що затверджений відповідним рішенням компетентного органу, оприлюднений та є обов'язковим для застосування. На сьогодні типовий ліцензійний договір не затверджений.

На підставі загальної вказівки норми ч. 2 ст. 1107 ЦК України договір щодо розпорядження майновими правами інтелектуальної власності укладається у письмовій формі, недодержання якої має наслідком нікчемність договору. У випадках, установлених законом, договір щодо розпорядження майновими правами інтелектуальної власності може укладатися усно. Наприклад, відповідно до ч. 1 ст. 33 Закону «Про авторське право і суміжні права» в усній формі може укладатися договір про використання (опублікування) твору в періодичних виданнях (газетах, журналах тощо).

Стрімкий розвиток сучасних комунікаційних засобів позначається і на практиці укладення та виконання договорів. Ці процедури «переміщуються» у цифрове середовище. Тому

змінюються звиклі уявлення про форму договору, стадії його укладення, виконання тощо. Прийнятий 3 вересня 2015 року Закон України «Про електронну комерцію» [4] покликаний урегулювати відповідні відносини в окресленій сфері. Безперечно, що норми зазначеного закону урегульовують низку питань, що до його прийняття не знаходили чіткого вирішення. У контексті досліджуваної тематики звернемося до аналізу норм розділу 3 Закону «Порядок вчинення електронних правочинів». Визначення електронного договору та електронного правочину, наведені у ст. 3 Закону, тотожні аналогічним визначенням у ЦК України, з додаванням слів «електронний». Отже, електронний договір – це домовленість двох або більше сторін, спрямована на встановлення, зміну або припинення цивільних прав і обов'язків та оформлена в електронній формі; електронний правочин – дія особи, спрямована на набуття, зміну або припинення цивільних прав та обов'язків, здійснена з використанням інформаційно-телекомунікаційних систем. Можливо і критикувати зазначені визначення, але за своєю змістовною суттю електронні правочини нічим не відрізняються від своїх задокументованих аналогів. Йдеться лише про особливості як форми, так і процедури укладення та виконання договору.

Відповідно до ст. 10 Закону електронні правочини вчиняються на основі відповідних пропозицій (оферт), які здійснюються шляхом надсилання комерційних електронних повідомлень. Важливим з точки зору потенційного договірного контрагента є положення Закону про те, що комерційні електронні повідомлення поширюються лише на підставі згоди особи на їх отримання. Комерційне електронне повідомлення може надсилатися особі без її згоди лише за умови, що вона може відмовитися від подальшого отримання таких повідомлень. У Законі детально прописані вимоги щодо змісту електронного комерційного повідомлення, змісту оферти та самого електронного договору.

Варто звернути увагу на момент укладення електронного договору, оскільки він є визначальним у правовідносинах сторін. Саме з моментом укладення договору пов'язані питання виникнення взаємних прав та обов'язків його сторін, їх

виконання, умови, підстави та засоби у разі невиконання чи неналежного виконання умов договору. Відповідно до ч. 3 ст. 11 Закону електронний договір укладається шляхом пропозиції його укласти (оферти) однією стороною та її прийняття (акцепту) другою стороною. Електронний договір вважається укладеним з моменту одержання особою, яка направила пропозицію укласти такий договір, відповіді про прийняття цієї пропозиції у встановленому порядку. Фактично йдеться про укладення договору за приєднанням до пропонованих умов відповідно до ст. 634 ЦК України.

Сутнісний зміст договору приєднання є у протиріччі з розумінням договору як домовленості двох і більше сторін, спрямованої на встановлення, зміну та припинення прав та обов'язків. Але укладення договорів за приєднанням до пропонованих умов стало настільки поширеним явищем, що сьогодні простіше перелічити випадки укладення договору за взаємною домовленістю, ніж охопити сфери укладення договору за приєднанням.

У практиці продажу примірників комп'ютерних програм застосовується декілька видів ліцензій та ліцензійних договорів для надання користувачам цих програм певного обсягу прав щодо їх використання. Пропозиція укласти ліцензійний договір, як правило, надходить від суб'єкта авторського права. Такі договори, за загальним правилом, є договорами приєднання. Тому спостерігаємо і відповідні цінові пропозиції та інші умови, на які неможливо вплинути, змінити їх чи запропонувати власні.

Звичайно, що укладення договору за приєднанням до пропонованих умов значно спрощує договірну практику, але породжує важливі проблеми з точки зору сторони, що приєднується до пропонованих умов. Об'єктивно така сторона є слабшою у процедурі укладення та виконання договору, оскільки вона не може впливати на зміст договору, що пропонується до укладення та не може запропонувати свої умови договору. Відповідно до ч. 2 ст. 634 ЦК України такий договір може бути змінений або розірваний на вимогу сторони, яка приєдналася, якщо вона позбавляється прав, які звичайно мала, а також якщо договір виключає чи обмежує відповідальність другої сторони за порушення зобов'язання або

містить інші умови, явно обтяжливі для сторони, яка приєдналася. Більше того сторона, яка приєдналася, має довести, що вона, виходячи зі своїх інтересів, не прийняла б цих умов за наявності у неї можливості брати участь у визначенні умов договору. Практично доведення таких обставин є неможливим, хоча б з огляду на труднощі у доказуванні причинного зв'язку між шкідливими наслідками в особи, що приєдналася до договору, та змістом договору, що пропонувався до укладення. Оціночний характер має поняття «явно обтяжливі умови». Тому у судовій практиці відсутні справи про оскарження умов договорів приєднання та відшкодування збитків.

Такі підходи правового регулювання свідчать про те, що законодавчі гарантії прав сторони, що приєднується до договору, спрацьовують після порушення її прав. Ще й тягар доказування покладається на сторону, що приєдналася. У переважній більшості випадків, стороною, що приєднується до договору, є фізична особа. Гарантії захисту її прав та інтересів встановлює Закон України «Про захист прав споживачів». Але знову ж таки ці гарантії та механізми захисту спрацьовують уже після факту порушення прав. На сьогодні відсутні превентивні механізми, системні правові підходи, які б унеможливили дискримінацію інтересів сторони, що приєднується до договору. У жоден спосіб не можливо відслідкувати, запобігти чи заборонити явно дискримінаційні положення, які включаються до змісту договорів, що пропонуються для укладення за приєднанням до пропонованих умов. Сторона, що пропонує умови договору, сама визначає їх зміст. Є виключно об'єктивні чинники, що можуть впливати як стримуючий фактор – це економічні чинники (ринкова кон'юнктура, податкова політика, фінансовий стан тощо). Але в умовах відсутності здорової ринкової конкуренції та слабо вираженої дії антимонопольного законодавства та законодавства про недобросовісну конкуренцію, споживач залишається наодинці з проблемами, що пов'язані з укладенням договору за приєднанням до пропонованих умов.

Вирішення проблем захисту прав та інтересів сторони, що приєднується до договору, вимагає комплексного законодавчого

підходу і є неможливим виключно у рамках приватноправового регулювання. Необхідними є публічно правові механізми та гарантії, які б унеможливлювали включення до договорів положень, що дискримінують права та інтереси сторін, що приєднуються до його умов.

У електронну сферу перемістилися не тільки договори купівлі-продажу, а договори про надання послуг, виконання робіт, розпорядження майновими правами інтелектуальної власності. Це реалії часу. Тому сторони, що укладають такі договори, мають діяти з урахуванням різних ступенів ризику. Презумпції добросовісності контрагента у цивільному обороті часто спростовуються, а загальні засади справедливості, добросовісності, розумності залишаються поки що як Fata Morgana.

Список літератури

1. Цивільний кодекс України. [Електронний ресурс] – Режим доступу : http://zakon.rada.gov.ua/go/435-15

2. Про деякі питання практики вирішення спорів, пов'язаних із захистом прав інтелектуальної власності: постанова Пленуму Вищого Господарського Суду України від 17.10.2012. [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/laws/show/v0012600-12

3. Про авторське право і суміжні права: Закон України від 23.12.1993. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/3792-12

4. Про електронну комерцію: Закон України від 03.09.2015. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/675-19

Juan Ramon Iturriagagoitia
Lawyer , Legal and Institutional Expert, Consultant

A FIRST SIGHT OVER COMPUTER SOFTWARE PROTECTION IN THE EU

Introduction

In the European Union, the path leading towards the legal protection of computer programs by means of a patent registration and through copyright protection evolved around conflicting positions. In this paper, the main documents issued by the EU Commission and the most relevant phases will be presented briefly.

Main policy documents of the European Union

A first attempt to approach the issue of computer software coincides with the visionary enterprise to create the Internal Market of the European Union. Computer software was thus expressly mentioned in the White Paper on Completing the Internal Market of June 1985. At that time, the situation appeared as intricate as it became clear that differences in intellectual property laws have a direct and negative impact on intra-Community trade and on the ability of enterprises to treat the common market as a single environment for their economic activities. A first step was scheduled for the Community Trademark Proposal. The picture around that Proposal emerged as being further complicated by the need to adapt existing trademark systems in the then 12 Member States to technological change, among others, in computer software. Legal convergence had to be sought so that the changes to undertake would not weaken the existing system. The publication of a consultative document in 1985 on copyrights and related rights with a view to establishing priorities was already announced. More importantly, the introduction of a Community framework for the legal protection of software would receive particular attention.

Finally, the Green Paper on Copyright and the Challenge of Technology – Copyright Issues requiring Immediate Action saw the light on 7 June 1988. This dense and long document takes up all relevant issues in this field from piracy to audio-visual products and home copying. At that time, the creation of a Single Market for copyright goods and services became one of the fundamental concerns of the EU Commission.

The Green Paper deals with computer programs and databases in separate chapters. As far as piracy is concerned, the document points towards the increase of pirated copies since computers became available to the public at large.

The Green Paper defines at the outset computer programs as a set of instruction the purpose of which is to cause an information processing device, the computer, to perform its functions. It discusses separately operating systems and application programs.

The world software industry is expected to expand, at a time the industry is already large. The Green Paper reckoned already in 1988 that in the future software will increasingly constitute the most

important component of computer systems, with the hardware consisting increasingly of similar, standardized interoperable components. This is one the reasons why the EU has to ensure that it has a competitive and dynamic software industry.

Given the late start of the Community's software industry, it is particularly important to ensure that appropriate legal protection is available to computer programs and software generally, which will contribute to an environment favourable to investment and innovation by Community firms. In debating the scope and term of protection, a correct balance should be found between the benefits protection gives to software producers and the «opportunity costs» it may impose on software users in the form of the range and price of software products available to them.

In the first time, contractual protection was deemed sufficient for software producers. This situation changed rapidly and two areas of intellectual property rights competed for being approved by legislators as the main instruments of protection: copyright and patents. Without prejudice to this, the Green Paper concludes that computer programs ought to be one of the areas in which immediate action by the legislature was required.

A long debate ensued then. Copyrights and patents found defenders for their use with respect to computer programs, although none of them were originally conceived for computer programs.

Whatever the case, two Follow-Ups to the Green Paper were still published respectively on 17 January 1991 and on 20 November 1996. The first one contained firstly the results of extensive hearings with stakeholders and secondly the Working Programme of the Commission in the field of copyrights and neighbouring rights. The second one

In 1991 the first computer programs Directive was also adopted. The major novelty was that the Directive conclusively created a harmonized for the protection of computer software as literary works which included limitations but also economic rights. The de-compilation exception was among the most controversial issues.

In 1993 a new Directive was adopted for the sake of harmonizing the term of protection of copyright at 70 years *post mortem auctoris*. The term for the protection of neighbouring rights

was set at 50 years. It must be recalled that internationally the minimum terms were 50 and 20 years respectively.

The legislative initiatives would however rapidly become outdated in view of the emergence of internet and the thereto related Information Society. In the light of the technological progress, the EU Commission undertook a review of the existing copyright provisions in 1994. In the summer of 1994 a major public hearing was organized by the EU; This lead to the publication of yet another Green Paper on 19 July 1995 bearing the title on Copyrights and Related Rights in the Information Society. The harmonization of national copyright laws was once again the central issue discussed in this new Green Paper, which addressed however also other topics, like strengthening the IPRs and ensuring the competitiveness of the EU economy.

The follow-up to the 1995 Green Paper was then adopted on 20 November 1996. It took the form of a Communication from the Commission and its complete title reads as follows: Follow-up to the Green Paper on Copyrights and Related Rights in the Information Society. This document finally sets the policy for computer software for the EU for the years to come. From a legislative perspective, the Communication of 1996 announces that the Commission will continue its further evaluation of the other, non-software related issues that were identified:

1. whether the multiplication and development of high quality, digital broadcasting channels, broadcasting their programmes without any interruption, in combination with the availability of automatic systems built into the consumer's receiver to copy this material «off the air», necessitates harmonised action in favour of certain right holders (notably phonogram producers and performers);

2. whether there is a need for a comprehensive and coherent initiative at Community level in regard to the management of rights, given the way in which the market evolves in response to the Information Society;

3. whether existing disparities in the national legislation of the EU Member States in regard to moral rights constitute significant obstacles for the exploitation of works and related subject matter in

the Information Society, which could require a harmonised protection of moral rights across the European Union.

Other actions yet to be performed included the publication of a clarifying Communication which addresses questions on matters concerning the applicable law as well as questions relating to the enforcement of rights. The issue of liability for copyright infringements with a view to a possible initiative at the European level may also be dealt with in the next future by the EU authorities.

As for the legislative roadmap of the EU Commission, the 1996 Communication spelt out that during the first half of 1997, the Commission intended to present legislative proposals on the following four priority issues which would require immediate action in order to eliminate significant barriers to trade in copyright goods and services and/or distortions of competition between Member States:

1. definition of the scope of the acts protected by the reproduction right, including the limitations to it;

2. protection of digital 'on-demand' transmissions will be protected on the basis of a further harmonised right of communication to the public, including the limitations to it;

3. schemes concerning the legal protection of the integrity of technical identification and protection will be harmonised. In particular, the precise scope of protection will be defined, as well as the liability of the infringer; and

4. the distribution right of authors as regards all categories of works, will be harmonised so that it will only be exhausted by the first sale in the Community by or with the consent of the right holder. The principle of exhaustion will only apply to the distribution of goods and not to the provision of services (including on-line services).

Obviously, the copyright issue is dealt with from a general perspective.

In 2003, there was still another attempt to regulate patent protection for computer programs with a proposal of a EU Directive on the patentability of computer-implemented inventions. The purpose of this legislative proposal was to set a legal framework for the . Although the EU patent protection Directive could have been

the ideal starting point for a debate around software, the proposal was simply rejected.

The next relevant policy document of the EU Commission on copyrights dates back to 16 July 2008. It was the Green Paper on Copyright in the Knowledge Economy. This document relates to the role of copyright in fostering dissemination of knowledge for research, science and education. The next policy that crystallized in a policy document is a Communication dated 19 October 2009 bearing the same title «On Copyright in the Knowledge Economy». This communication deals with the mass-scale digitalisation and dissemination of books.

The 2009 computer programs copyright Directive

So, after so many policy documents containing issues that affect direct or indirectly the protection of computer programs, the only legal instrument effectively applicable is the recently adopted Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs. These are protected as copyrights, by analogy to the protection given to literary works within the meaning of the Berne Convention for the Protection of Literary and Artistic Works.

Directive 2009/24/EC is a codified version of the previous Directive 91/250/EEC of 14 May 1991 that applied to the protection of computer programs.

The term computer program is defined as including programs in any form, including those which are incorporated into hardware. The term also includes preparatory design work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage.

Member States must thus protect computer programs, by copyrights, as literary works within the meaning of the Berne Convention. The computer program shall be protected if it is original in the sense that it is the author's own intellectual creation.

The author of the computer program is the natural person or group of natural persons who has created the program or, where the legislation of the Member State permits, or the legal person designated as the right holder by than legislation. Where collective works are recognized by the legislation of a Member State, the

person considered by the legislation as having created the work shall be deemed to be its author. In the case of a computer program created by a group of national persons jointly, the exclusive work shall be owned jointly. Where a computer program is created by an employee in the execution of his duties, or following the instructions given by his employer, the employer exclusively shall be entitled to exercise all economic rights in the program so created, unless otherwise provided by the contract.

Protection shall be granted to all natural or legal persons eligible under the national copyright legislation, as applied to literary works.

The exclusive rights of the right holder are described in the Directive in accordance with the provisions of the Berne Convention. Decompilation is permitted under certain circumstances and this provision is mandatory. A contractual prohibition to make a back-up copy by the person having the right to use the computer program and other specific acts performed by the person having the right to use the computer program cannot be prohibited in a contract. Special measures of protection for the protection against piracy can be adopted.

No formality or registration is required to enjoying copyright protection; copyright protection is granted from the sole fact of the creation of the computer program. The protection extends to any element of creation of the creativity of its author, but not to the ideas behind it. Hence algorithms are not eligible for copyright protection.

Copyright will thus protect only the computer program in the form written by a programmer – i.e. its source code. Not subject to protection by copyright are the functionality of a computer program, the programming language, or the format of data files used in a computer program in order to exploit certain of its functions, because they do not constitute a form of expression of that program.

Patentability of computer programs

As a matter of fact, patent applications related to computer programs succeeded and still succeed at present. Nowadays, patent protection under article 52 of the European Patent Convention can be obtained in certain circumstances. Patentability of software is excluded to the extent that a patent application relates to a computer

program «as such». A distinction can be made between «software patents» and the so-called «computer-implemented inventions» which are accepted as patentable. The latter can be defined as inventions whose implementation involves the use of a computer, a computer network or other programmable apparatus, having one of more features realised by means of a computer program. The subject matter of the invention as a whole, i.e. a machine with related software, must have a technical character to be patentable. This technical character must be present in all variants covered by the invention, or the patent claim. The conditions that must be met to obtain patent protection for a computer program include thus the requirements of technical character and inventive step described above, and additionally is new and undisclosed.

Conclusion

This first sight into EU computer software protection under EU law reveals that being all legal instruments adopted by the EU authorities Directives, it is necessary to also take into consideration national rules when contracting with parties based in a EU Member State. It is indeed necessary to understand exactly what the stakes are in order to choose among the advantages offered by national legislations, unless more flexible solutions are chosen. In principle, the UNIDROIT Principles for International Commercial Contracts may be the ideal alternative.

Секція 3.
УПРАВЛІННЯ ЕФЕКТИВНІСТЮ ДІЯЛЬНОСТІ, РЕКРУТИНГ, ПСИХОЛОГІЧНА ПІДГОТОВКА ФАХІВЦІВ У ІТ СФЕРІ

Виноградова В.Є. –
завідувач кафедри психології та суспільних наук
Академії муніципального управління
кандидат педагогічних наук, доцент
Петровська О.В. –
HR Manager в PHP Academy

ПСИХОЛОГІЧНІ АСПЕКТИ ПІДБОРУ ПЕРСОНАЛУ В ІТ СФЕРІ

Питання підбору персоналу завжди було і залишається актуальним. Сьогодні існує система психодіагностичних методів, які допомагають HR у їх роботі. Проте в кожній професійній галузі є своя специфіка, яка залежить від психологічних особливостей фахівців та інших факторів. Галузь ІТ розвивається досить швидко і на перший план виходить питання як підібрати кваліфікований персонал з мінімальними затратами.

Однак, в багатьох випадках менеджери з персоналу підбирають фахівця за порадою знайомих, інтуїції або за зовнішністю. Безумовно, кожен менеджер з персоналу опанував певні методи, які йому допомагають у діяльності підбору. Проте процес підбору кадрів має ґрунтуватися на наукових засадах, а не на інтуїції, оскільки це може негативно позначатися не лише на ефективності роботи організації, а і на соціально-психологічному кліматі колективу [1].

Потрібно зазначити, що питаннями підбору персонала займалися такі науковці, як: Базаров Т.Ю., Виноградська А., Єрьомін Б.Л., Савченко В.А., Грехем Х.Т., Беннетт Р.А та ін. У своїх працях вони висвітлювали основні методи та етапи підбору персоналу. Проте, на нашу думку, особливу увагу необхідно приділити саме психологічним особливостям підбору персоналу в ІТ сфері.

Професійний підбір – це процес забезпечення компанії працівниками з бажаними якостями, які відповідають визначеним вимогам, а також здатні вчасно та якісно виконувати звдання та досягати поставлених цілей. Професійний підбір є однією з основних функцій підбору персоналу, від якості виконання якої залежить ефективність діяльності підприємства. Більшість компаній, на жаль, не мають чітко сформульованого плану з добору персоналу. Проблема пошуку виникає, як правило, несподівано: пішов фахівець і менеджер з персоналу терміново шукає заміну.

З розвитком технологій зростає потреба в кваліфікованих IT-спеціалістах. Сьогодні вони необхідні в кожній компанії. Це пов’язано з тим, що IT-спеціалісти відповідають за роботу комп'ютерної техніки і локальної мережі, а також створюють і підтримують web-сайти фірми. Насправді ж часто виявляється, що названі співробітники виконують зовсім не ті функціональні обов'язки, якими б вони мали займатись відповідно до своєї посади.

IT-професіонали відрізняються від здобувачів на інші позиції нестандартним мисленням, манерами і, навіть, зовнішнім видом. Тому HR-менеджеру, який проводить співбесіду на посаду системного адміністратора, програміста, тестувальника, необхідно використовувати особливий підхід до кандидата.

І тут постає питання: як же правильно оцінити кандидата, визначити усі якості, які необхідні для конкретного виду діяльності?

Щодо підбору програмістів, то ми пропонуємо такі етапи відбору на посаду.

1. Пошук резюме на сайтах, в соціальних мережах.
2. Проведення попереднього інтерв’ю по телефону.
3. Проходження психологічних тестів.
4. Співбесіда з HR.
5. Технічна співбесіда або виконання технічного завдання.

Проте, більшість компаній пропускають етап психологічних тестів, вважаючи їх зайвими. Це може призводити до того, що новий працівник не впишеться в

колектив, є варіант потрапити на «конфліктну» особистість або, якщо це рівень Trainee\Junior обрати людину, якій не притаманна робота саме в цій галузі. Це пов’язано з тим, що в цій сфері досить великі зарплати і люди, які не мають схильності до цієї діяльності також намагаються працювати в ній.

Отже, важливим етапом при відборі персоналу є встановлення відповідності фахівця до професіограми та функціональних обов’язків вакантної посади. На нашу думку, необхідно виділити окремо декілька позицій такі, як: професійні, особистісні та психологічні якості фахівця.

Процес підбору персоналу починається з вибору критеріїв оцінювання особистості і роботи претендентів. Критерії включають норми поводження і характеристику професійних навичок. Вимоги до наявних знань, вмінь та навичок претендента працедавці пред'являють залежно від того, чим вони збираються завантажити свого співробітника. Тут, окрім базових знань, часто потрібна знати такі операційні системи, як: Windows NT, Novell, Unix, мати навички об'єднання в мережу комп'ютерів різних типів, скажімо PC і MAC, досвід роботи з устаткуванням різних виробників, наприклад Cisco, 3com, Intel, Hewlett Packard. Наявність сертифікатів вітається. А решта показників стандартні для цієї сфери: як правило, потрібні чоловіки з вищою або незавершеною вищою технічною освітою і досвідом роботи за фахом.

Наступний етап підбору персоналу – його експертне оцінювання, що ґрунтується на проведенні тестів, рішенні задач і виконанні вправ. Після тестування проводиться співбесіда: запрошення претендентів і проведення інтерв'ю. На підставі вищевикладеного, відбувається опис отриманих результатів і порівняння їх із критеріями оцінки кандидатів. Завершує процес підбору кандидатів ухвалення рішення; якщо виникають труднощі з остаточним ухваленням рішення, можна провести додаткове тестування.

Ми хотіли б зупинитися більш детально на психологічному відборі фахівців. Він полягає у виявленні людей, індивідуально-психологічні особливості яких відповідають вимогам до діяльності за конкретною

спеціальністю. Його, як правило, застосовують щодо спеціальностей, які передбачають конкретні вимоги до психологічних особливостей людей і які не можна задовольнити вдосконаленням техніки або у процесі спеціального навчання. Психологічні професійно важливі якості – це якості індивіда, які безпосередньо стосуються трудового процесу і впливають на його ефективність.

До методів профвідбору належать:

- Професіографічний аналіз діяльності. Результатом такого аналізу, здійсненого психологами, є професіограма. Це опис соціально-економічних, виробничо-технічних, санітарно-гігієнічних, психологічних та інших особливостей професії. Найважливіша її складова – психограма. Це характеристика вимог, висунутих професією до людини, її психічних та інтелектуальних якостей; перелік та опис загальних і спеціальних умінь та навичок, необхідних для конкретної професійної діяльності.
- Метод експертного оцінювання. Для цього група авторитетних експертів отримує завдання незалежно один від одного назвати не менше п'яти якостей, які повинен мати майже ідеальний спеціаліст. Виокремлені експертами якості структурують, встановлюють відповідні їх показники і критерії.
- Відбірний тест. Він передбачає використання психологічних тестів і є формальним методом оцінювання придатності кандидатів на заміщення посади.

Існує певна специфіка проведення співбесіди з ІТ-спеціалістами. При підборі спеціалістів цього профілю менеджеру з персоналу необхідно враховувати специфіку професії та не звертати увагу на зовнішній вигляд, комунікабельність. «Айтішники» – особливі люди, які можуть бути інтровертами, навіть з проявами аутизму. Вони, як правило, не звертають увагу на зовнішню атрибутику, проте вміють бачити суть речей.

Також, на нашу думку необхідно виключити з числа претендентів «кофліктних» особистостей. Такі працівники характеризується як важко-керовані, схильні бути ініціаторами конфліктів, з погано передбачуваною

поведінкою. Спектр проявів характеру важких працівників досить широкий. У ньому вирізняють типи важкого працівника: «агресивний», «нерішучий», «неконтактний», «бунтівник», «всезнайка», «недобросовісний», з низькою професійною компетентністю. Для цього застосовуються психологічні тести та співбесіда. Претенденту пропонуються питання, в яких уже закладена конфліктна ситуація, з якої він має вийти або ситуація із його досвіду. Наприклад, «Яка ситуація при спілкуванні була для вас найбільш емоційно напруженою?» «Пригадайте, як ви спілкувались з агресивно налаштованою людиною?»

Однак, застосування одного методу інтерв'ю не дає вичерпної інформації про особистість фахівця, і достовірної оцінки його особистісно-професійних якостей. Тому, пропонується спільно використовувати і інші методи – психологічні тести. Найпоширенішими тестами у процесі відбору персоналу є методики що дозволяють виявити особливості психічних процесів («Оперативна пам'ять», «Пам'ять на образи», «Пам'ять на числа», методика «Мюнстерберга», «Розміщення чисел», «Складні аналогії», методика «Равена», методика визначення загальних здібностей «General skills») та індивідуально-психологічні і особистісні властивості особистості кандидата (Опитувальник К. Леонгарда – виявлення напрямків характеру, Тест-опитувальник Кеттела 16 PF. Особистісний опитувальник – варіант тесту MMPI-2, Ціннісні орієнтації М. Рокича, Орієнтаційна анкета Б. Басса, Тест-опитувальник Т. Ліри – діагностика міжособистісних відносин, Тест-опитувальник К.Томаса – діагностика реагування на ситуації конфлікту, Колірний тест Люшера та ін.).

Також для оцінки аналітичних здібностей кандидата можна використовувати практичні кейси, на основі яких визначають: які саме дані відбираються кандидатом та підлягають аналізу; яким чином він їх структурує для досягнення оптимального результату; які висовки робить з проведеного анализу.

Таким чином, інтуїтивні методи підбору кадрів неприйнятні для формування команди професіоналів. Підбирати персонал потрібно на плановій основі. У процесі планування

трудових ресурсів визначають наявність, майбутні потреби в кадрах і розробляють програми їх розвитку. Для підбору кадрів доцільно використовувати психологічний тестовий інструментарій, який допоможе підібрати ефективий персонал.

Список літератури

1. Зеленков А.В., Кононенко А.В., Налапко М.М. Організація набору та відбору персоналу // Економіка та управління підприємствами машинобудівної галузі: проблеми теорії та практики. – 2008. – № 3. – С. 125-135.
2. Кузнецова Н. Принятие решений при подборе персонала // Менеджер по персоналу. – 2008. – №9. – С. 46-51.
3. Новікова А. Подбор персонала: правильные решения // Менеджер по персоналу. – 2007. – №4. – С. 38-45.
4. Шипуліна В.О., Каспрук О.В. Новітні підходи до залучення кадрових ресурсів // Вісник Хмельницького національного університету. – 2009. – № 3. – Т. 2. – С. 111-117;
5. http://www.management.com.ua/consulting/cons009.html
6. http://www.hr-director.ru/article/63078-red-voprosy-sistemnomu-administratoru-na-sobesedovanii

Лозовицький Д.С. –
докторант Львівського торговельно – економічного університету,
кандидат економічних наук, доцент
Бачинський Т.В. –
асистент кафедри цивільного права та процесу Навчально-наукового інституту права та психології Національного університету «Львівська політехніка», кандидат юридичних наук

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ САМОКЕРОВАНИХ ІТ - КОМАНД

Ітеративні методи розробки програмного забезпечення які базуються на принципах і підходах Agile методології (*agile methodologies, agile framework*) висувають до учасників проектних ІТ команд вимогу максимальної синергічності їх роботи задля швидкого і точного досягнення поставлених робочих задач.

Практика управління ІТ командами доводить, що досягнення синергічного ефекту у роботі є складним практичним завданням [1, 2].

З науково-практичної точки зору питання досягнення необхідного явища синергізму у роботі самокерованої ІТ команди лежить у площині принципів її роботи.

На нашу думку методологічний базис основних принципів функціонування самокерованих ІТ команд можна розділи на чотири складові частини:

1. Комунікаційну;
2. Особистих відносин;
3. Організаційну;
4. Юридично забезпечуючу.

Застосування набору принципів кожної із зазначених частин сприяє формуванню єдиного розуміння процесу роботи ІТ команди.

Розглянемо детальніше кожну групу принципів і модель їх взаємодії детальніше.

Автоматизовані системи управління діяльністю, проектом, командою у своїй основі завжди базуються на методах проведення ефективної комунікації. До основних принципів комунікації самокерованих проектних ІТ команд напрацьованих у результаті практичної діяльності відносять:

1. *Інформаційного фокусування* – у роботі самокерованої команди уся необхідна інформація приймає «концентрований» і виключно об'єктно орієнтований вигляд, інформаційні «шуми» практично відсутні (учасники команди самостійно створюють у процесі комунікаці необхідну для роботи «готову» інформацію не видаючи колегам «напівфабрикат»);

2. *Прямої комунікації* – уся комунікація здійснюється напряму, без жодних посередників (чим досягається високий ступінь реагування на інформаційні сигнали у роботі команди, а також зменшується спотворення інформаційних повідомлень за практичної відсутності ієрархічних рівнів управління);

3. *Автоматичного повного зворотного зв'язку* – усі учасники самокерованих проектних ІТ команд розуміючи важливість параметрів проектного управління (швидкості, якості, вартості робіт) завжди надають вичерпний обсяг необхідної інформації за отриманим інформаційним запитом;

4. *Автоматизації інформаційного поля роботи команди* – формування цілісної і постійно доповнюваної картини

інформаційного фону проекту (для прийняття більш обгрунтованих проектних рішень).

«Краєугольним каменем» ефективності будь яких ІТ проектів завжди є люди (учасники проектної команди). Ефективність взаємодії учасників проекту, особливо самокерованих проектних команд, в першу чергу, залежить від формування середовища «довіри і авторитету» як в середині, так і зовні команди. Основними принципами особистих відносин є:

1. *Внутрішньої неконкурентності* – учасники проектної самокерованої команди конкурують не один з одним, а на особистісному рівні самі із собою (усі учасники самокерованих команд сфокусовані на задоволенні свого професійного его не за рахунок переваги над учасниками своєї команди, а виключно за рахунок спільного досягнення поставленої мети);

2. *Глибокої довіри за досягнення (авторитетності)* – учасники проектних команд довіряють лідеру (і один одному) не тільки через його особисті людські якості, скільки через рівень практичних професійних звершень керівника команди та її учасників (коли справи людини самі говорять за неї);

3. *Психологічної комфортності* – даний принцип полягає у подібності моделей професійного сприйняття ролей кожного учасника проектної команди (створення ефекту симетричного, однакового розуміння ролі);

4. *Здорового професійного егоїзму* – суть цього принципу полягає у обов'язковому індивідуальному пошуку учасниками команди у зовнішньому середовищі персонального кращого за власний прикладу «професійного еталону» у робочих досягненнях і прагненні перевершити його.

Організацію праці, як інструмент формування ефективних шляхів досягнення цілей важко переоцінити. До основних принципів організації праці притаманних учасникам самокерованих ІТ команд можемо віднести:

1. *Досконалого знання методики розробки* – учасники самокерованих ІТ команд володіють усіма аспектами обраної командою методики розробки;

2. *Чіткості визначення ролі учасника* – формування прозорого розуміння функціональних обов'язків кожного учасника ІТ команди залежно від обраної методики розробки ІТ

продукту (відсутність задвоєння функцій, чи навпаки присутність «сліпих зон» у виконанні певних видів робіт);

3. *Універсальності учасників* – кожен учасник у команді виконує свою роль, але при цьому він володіє достатнім рівнем професійної компетенції для тимчасової або повноцінної заміни іншого учасника в процесі роботи ІТ команди (це бажаний стан справ, але далеко не обов'язковий);

4. *Створення технічної основи співпраці* – формування загальних організаційних процедур співпраці команди, визначення пулу технологій та інструментів які використовуватиме команда.

Юридичні аспекти співпраці людей були, є і будуть завжди невідємною частиною процесу роботи. Важливим питанням у роботі самокерованих ІТ команд є формальна і неформальна сторони юридичного забезпечення процесу їх функціонування.

Окремого наголосу потребує розуміння необхідності дотримання балансу із юридичної точки зору між колективними правилами роботи ІТ команд і індивідуальними контрактними зобов'язаннями кожного учасника команди.

До юридичних принципів функціонування самокерованих ІТ команд відносять:

1. *Формування формального відкритого юридичного колективного поля роботи команди* – ствоерення єдиного відкритого юридичного поля (набору правил) для співпраці команди, як в її середині так і з зовнішнішнім середовищем її оточення прийнятних і зрозумілих для усіх учасників процесу співпраці;

2. *Конвергенція особливостей індивідуальних (закритих) контрактів із колективним юридичним полем діяльності команди* – юридичні особливості індивідуальних контрактів не мають суперечити юридичним аспектам колективної праці команди;

3. *Мінімізації неформальних юридичних правил поведінки* – виключення можливості формування додаткових юридичних правил поведеніки в середині ІТ команди які би не були враховані і обумовлені у індивідуальних контрактах або їх колективних версіях.

Розглянуті особливості і принципи роботи самокерованих IT команд дають можливість сформувати концептуальну мета модель їх поведінки (Рис. 1), а також схему області формування явища синергії у роботі IT команд (Рис. 2).

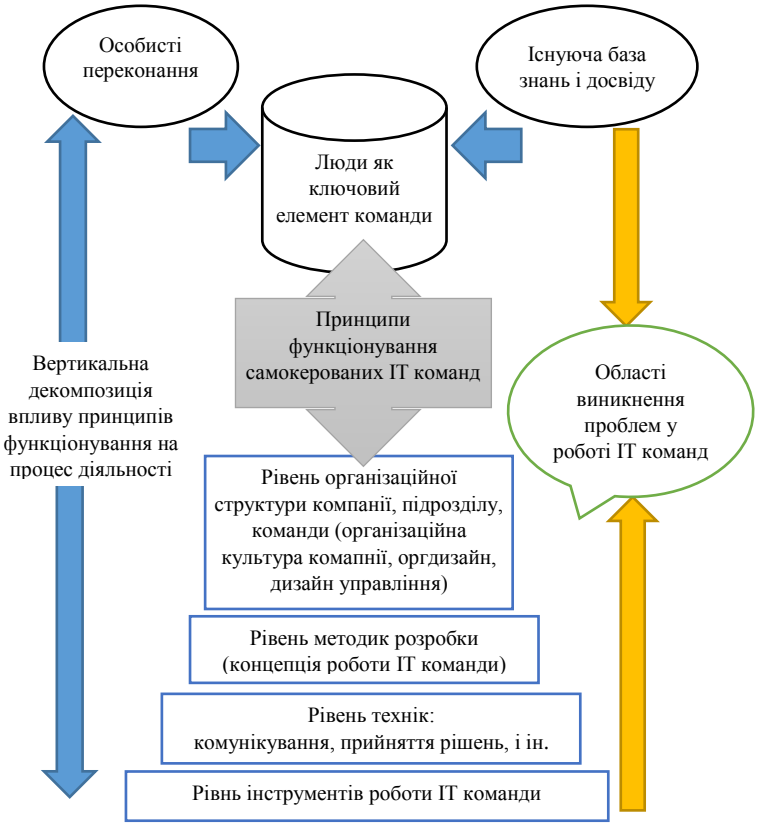


Рис. 1. Концептуальна мета модель поведінки самокерованої IT команди *(авторській підхід Лозовицького Д.)*

Рис. 2. Схема області формування явища синергії у роботі самокерованої ІТ команди *(авторський підхід Лозовицького Д.)*

Порушення базових принципів діяльності ІТ команди є причиною розбалансування її роботи на різних рівнях процесів і технологій які застосовуються під час розробки. На нашу думку такими типовими проблемами є:

– відсутність лідерства у команді або присутність одночасно формального та неформального лідерів;

– неоптимальний підбір інструментів колективної роботи над проектом;

– відхилення у розумінні цілей проекту;

– відхилення у вимогах якості продукту розробки;

– можливий зрив термінів виконання проекту;

– перевитрати у обсягах фінансування проекту;

– формування психологічних «блоків» у роботі окремих фахівців;

– втрата цінних знань і досвіду, або їх неоптимальне розповсюдження в межах проектної команди;

– непорозуміння між керівником проекту, замовником і керівництвом компанії розробника.

Вважаємо, що відповідальність за імплементацію і дотримання базових принципів роботи самокерованої ІТ команди несуть у рівній мірі як проектний менеджер, так і сама команда.

Для полегшення процесу коректного впровадження зазначених принципів роботи самокерованих ІТ команд рекомендуємо:

– під час проходження передпроектної фази продумати оптимальний шлях ранньої імплементації зазначених принципів у методику роботи ІТ команди;

– сформувати зведення правил організаційної поведінки команди із можливістю їх формального юридичного або неформального поведінкового закріплення;

– створити систему інформаційного моніторингу управлінської, організаційної і технологічної ефективності діяльності ІТ команди;

– застосовувати під час прийняття командиних рішень технолгію design thinking.

Усі пропозиції щодо вирішення зазначених проблемних аспектів роботи ІТ команд є предметом наступних індивідуальних або спільних науково-практичних досліджень.

Список літератури

1. Martin Olson. Foundations of the Scaled Agile Framework® Be Agile. Scale Up. Stay Lean. Leffingwell et al. / Olson Martin. – 2014. - Scaled Agile, Inc. Pg. 12 – 21.

2. A Guide to the Project Management Body of Knowledge (PMBOK Guide) – Fourth Edition. – Project Management Institute, 14 Campus Blvd., Newtown Square, PA 19073-3299 USA. – Pg. 232 – 244, 265 – 288.

Monika Artman
Wyższa Szkoła Społeczno Gospodarcza z siedzibą w Przeworsku

ANALIZA METODY KAM (KNOWLEDGE ASSESSMENT METHODOLOGY) – WADY I ZALETY

1. Wprowadzenie do problematyki

Od zarania dziejów człowiekowi towarzyszy nauka, która wraz z upływem czasu podlega ciągłemu procesowi rozwoju. W celu usystematyzowania ogromu zgromadzonej wiedzy, nauka zajmująca się badaniem pewnego rodzaju procesów i zjawisk, które otaczają nas w rzeczywistości, posługuje się właściwymi do tego terminami. Jednakże ich tworzenie, a następnie swoista interpretacja merytoryczna jak i semantyczna często już na tym etapie stanowi problem. Neologizmy utworzone w danym języku często prowadzą do sporów na płaszczyźnie naukowej. Poznawanie nowych elementów rzeczywistości obliguje do wprowadzania nowych pojęć, które niewątpliwie przekładają się na ludzkie poznanie oraz wzbogacenie języka. Jednocześnie zdarza się też tak, że terminy czy też pojęcia użyteczne, generowane są w środkach masowego przekazu, przy zachowaniu ich ideologicznej funkcji, a w dalszej kolejności przyjmują charakter naukowy lub poznawczy. Przykładami takich pojęć są między innymi: społeczeństwo informacyjne oraz gospodarka oparta na wiedzy.

Pierwsze z wyróżnionych pojęć, nad którymi poświęcone są rozważania w niniejszym artykule to ,,społeczeństwo informacyjne». Pojęcie to wprowadził w 1964 roku Japończyk Tadlo Umesao w artykule na temat ewolucyjnej teorii społeczeństwa, w którym to gospodarka została przedstawiona w oparciu o przemysł informacyjny. W ujęcie tej koncepcji społeczeństwo informacyjne to społeczeństwo, którego podstawę komunikacji międzyludzkiej stanowią komputery[16]. Na przestrzeni dekad, pojęcie to zmieniało i rozszerzało swoje znaczenie. Z kolei w dokumencie «e-Polska-Strategia rozwoju społeczeństwa informacyjnego w Polsce na lata

[16] M. Galka, *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2008, s. 79.

2001-2006» owe społeczeństwo informacyjne zostało sprecyzowane jako modernistyczny system społeczeństwa, który formułuje się w krajach wykazujących wysoki stopień rozwoju technologicznego, gdzie czynność, jakość i szybkość przepływu zarządzania informacją stanowią główny czynnik konkurencyjności w klasyfikacji działów gospodarki. Z kolei ich stopień rozwinięcia obliguje do korzystania z technik akumulowania, a następnie analizy, użytkowania i dalszego przekazywania danych informacji[17]. Podobną definicję przedstawia dokument «Nauka, nowoczesne technologie i społeczeństwo informacyjne 2007-2013». W tym dokumencie, społeczeństwu nadano przyrostek informacyjnego, kiedy osiąga odpowiedni poziom rozwoju, a także skomplikowania procesów społecznych i gospodarczych, które wymagają wprowadzenia technik gromadzenia, przetwarzania i użytku dużych ilości informacji. W takim społeczeństwie wyróżnić można następujące cechy charakterystyczne[18]:

– siłę roboczą tworzą przede wszystkim pracownicy informacyjni,

– informacja, wiedza i technologia są fundamentalnymi determinantami wytwórczymi, a z kolei wszechstronne elementy rozwoju stanowią działanie w zakresie teleinformatyki,

– zdecydowana większa część dochodu narodowego brutto tworzona jest w oparciu o szeroko rozumiany tzw. sektor informacyjny.

Analizując definicje z kilku innych dokumentów i opracowań, stwierdzić można powielanie się trzech podstawowych cech charakteryzujących współczesne społeczeństwo informacyjne. Są one następujące:

– istotna funkcja wiedzy, informacji oraz technologii, postrzegany jest jako podstawowy czynnik wytwórczy;

– sektor informacyjny stanowi główny element tworzenie produktu narodowego brutto;

[17] www.nauka.gov.pl, s. 62 (dostęp: 20.09.2016)

[18] *Społeczeństwo informacyjne w Polsce- wstęp do formułowania założeń polityki państwa*, Krajowa Rada Radiofonii i Telewizji, Warszawa 1996, www.nauka.gov.pl (dostęp: 29.09.2016)

– pracownicy zatrudnieni w sektorze informacyjnym dominują w strukturze siły roboczej.

Patrząc krytycznie na przyjęte analizy można stwierdzić, że zaprezentowana ekspozycja zdecydowanie lepiej pasuje do gospodarki opartej na wiedzy, niżeli do pojęcia społeczeństwa informacyjnego.

Czym zatem jest społeczeństwo informacyjne? Zasadne w tym przypadku wydaje się być wyróżnienie takich cech społeczeństwa informacyjnego, jak[19]:

– Internet jako środek informacji publicznej oraz podstawowa komunikacja międzyludzka;
– ogólnodostępna edukacja;
– powszechność dostępu ludzi do informacji.

W niniejszym artykule nie ma możliwości oraz potrzeby przeprowadzenia dalszego przeglądu definicji, czy też dokonywania krytycznej analizy w obszarze społeczeństwa informacyjnego oraz gospodarki opartej na wiedzy.

Zdecydowanie większe zainteresowanie wzbudza problem określenia stopnia zaawansowania rozwoju gospodarki, która oparta jest na wiedzy oraz społeczeństwa informacyjnego. Bazując na współczesnej ekonomii powołać można się na tradycyjną analizę modelowo-ilościową, na przykładzie której wskazać można zestaw mierników i wskaźników, które między innymi pozwalają na:

1. oszacowanie stopienia poziomu rozwoju określonej gospodarki opartej na wiedzy;
2. dokonanie zestawienia porównawczego stopnia zaawansowania informacyjnego określonej gospodarki;
3. dokonanie zestawienia porównawczego w przestrzeni i czasie zaawansowania stopnia informacyjnego danych gospodarek i społeczeństw;
4. rozpoznanie i określenie oczekiwanych kierunków procesu ewolucji współczesnej gospodarki;
5. sporządzenie narzędzi wykonawczych i celów adekwatnej polityki danego państwa;

[19] S. Czaja, A. Becla, M. Celińska, *Informacja a współczesna gospodarka i społeczeństwo,* Wydawnictwo PWSZ w Głogowie, Głogów 2011, s. 79.

6. ocenę dokonanych przemian w obszarze społeczno-gospodarczym (ewolucja informatyczno-informacyjna).

Celem niniejszego artykułu jest przybliżenie zagadnienia metody KAM (Knowledge Assessment Methodology), którą wykorzystuje się do pomiaru poziomu zaawansowania badanej gospodarki opartej na wiedzy. W dalszej części Autor artykułu przedstawia elementy metody, jej zalety i wady- co połączone zostało z uwagami na temat problemów metodologicznych w obszarze pomiaru rozwoju zaawansowania gospodarki opartej na wiedzy i społeczeństwa informacyjnego.

2. Istota metodologii KAM- wady i zalety

Dokonanie pomiaru poziomu zaawansowania rozwoju danej gospodarki, która oparta jest na wiedzy stwarza wiele problemów, a wśród nich przede wszystkim problemy obrachunkowe oraz natury metodologicznej. Można wyróżnić następując wady metody KAM:

1. Dobór mierników i wskaźników oddających różne aspekty wymiaru informacyjnego danej gospodarki opartej na wiedzy i społeczeństwa informacyjnego.
2. Niedobór w obszarze dokładnej i umożliwiającej się kwantyfikować definicji gospodarki opartej na wiedzy i społeczeństwa informacyjnego. Dobór właściwego podejścia metodologicznego w celu mierzenia stopnia poziomu rozwoju gospodarki opartej na wiedzy i społeczeństwa informacyjnego.
3. Wybór adekwatnego zestawu mierników i wskaźników biorąc pod uwagę kryteria pokrycia informacyjnego danego badanego problemu, jak i ograniczanie wydatków związanych z pozyskiwaniem tych informacji.

Konieczność posługiwania się dokładnymi i umożliwiającymi się kwantyfikować definicjami stanowi podstawę do rozpoczęcia metodycznej weryfikacji danych zagadnień oraz znalezienie odpowiedzi na następujące pytanie: na jakim etapie rozwoju znajduje się w danym czasie określone społeczeństwo i jego gospodarka oraz czy wykazany poziom zaawansowania jego rozwoju można uznać za usytuowany na dostatecznym poziomie? Innymi słowy poszukuje się odpowiedzi na następujące pytania: Czy badane społeczeństwo można nazwać społeczeństwem informacyjnym? Czy stworzona przez to społeczeństwo gospodarka jest gospodarką opartą na wiedzy?

Poszukiwanie odpowiedzi na powyższe pytania tworzy konieczność dokonania wyboru adekwatnego podejścia metodologicznego w obszarze kierunku ewolucji oraz pomiaru stopnia poziomu gospodarki opartej na wiedzy i społeczeństwa informacyjnego[20]. W związku z powyższym oznacza to konieczność doboru oczekiwanych cech, tak aby można było społeczeństwo określić społeczeństwem informacyjnym, a jego gospodarkę gospodarką w pełni opartą na wiedzy. Kwestia ta odnosi się do każdej podjętej w badaniach zmiennej uznanej za: stymulanta, destymulanta, czy też dominanta.

Z kolei dobór mierników i wskaźników oddających różne aspekty wymiaru informacyjnego danej gospodarki opartej na wiedzy i społeczeństwa informacyjnego jest na domiar istotnym i ciekawym zadaniem metodologicznym. Dotychczasowa wiedza umożliwia na opis procesów, które charakteryzują społeczeństwo w ujęciu informacyjnym oraz jego gospodarkę opartą na wiedzy. Wraz ze wzrostem poczucia niedostatku tej wiedzy, wzrastają również kontrowersje z powodu dokonania wyboru mierników i wskaźników. Jednakże z drugiej strony na podstawie danych zmiennych można pojąć i sprecyzować wiedzę o gospodarce opartej na wiedzy i społeczeństwo informacyjne. Należy również podkreślić, że wybór cech oraz opisujących je zmiennych jest wyrazem posiadanej i ciągle rozwijanej wiedzy o badanym zagadnieniu oraz stanowi zamierzenie poznawcze.

Proces, który nie wątpliwie stanowi rozwój wiedzy, wymaga przede wszystkim selekcjonowanych informacji, co stanowi podstawę do prowadzenia dalszych badań. Istnieją specyficzne rodzaje informacji, dla których nieuniknione jest wdrążanie mechanizmów, umożliwiających: gromadzenie pożądanych danych, a następnie ich przetwarzanie i wykorzystywanie.

3. Przedstawienie metody KAM w ujęciu badań empirycznych

Metoda KAM (Knowledge Assessment Methodology) powstała w 1998 roku, na zlecenie Instytutu Banku Światowego. Ze

[20] A. Becla, S. Czaja, M. Hałasa, *Etapy rozwoju (zaawansowania) społeczeństwa informacyjnego. Wybrane zagadnienia,* [w:] *Społeczeństwo informacyjne. Uwarunkowania społeczne i kulturowe,* red. P. Setlak, P. Szumlich, PWSZ w Tarnobrzegu, Tarnobrzeg 2010, s. 41-52.

względu na czynniki deskrypcyjno-poznawczo-interpretacyjne analizy KAM, w krótkim czasie została ona jedną z najbardziej popularnych analiz służących do prowadzenia badań nad gospodarką opartą na wiedzy i społeczeństwie informacyjnym. Analiza KAM wykorzystywana jest przez analityków z obszaru wszystkich rozwiniętych krajów świata. Jednakże pomimo jej użytkowności i popularności nie jest włączona do ogólnego systemu statystyk społeczno-ekonomicznych, który opiera się obliczeniach narodowych SNA (System of National Accounts).

W podejściu analizy KAM wyszczególnić można dwa warianty, są one następujące[21]:

- wariant zredukowany;
- wariant rozszerzony.

Wariant zredukowany bazuje przede wszystkim na 14-u wskaźnikach. W praktyce umożliwiają one prowadzenie kalkulacji indeksu wiedzy, jak i indeksu gospodarki wiedzy. Pierwszy z nich, indeks wiedzy wykorzystywany jest do określania miary zdolności kraju, jego gospodarki i społeczeństwa, do tworzenia, wdrążania oraz upowszechniania wiedzy. Indeks wiedzy obliczany jest za pomocą średniej arytmetycznej poszczególnych wskaźników cząstkowych tj. technologie teleinformatyczne, edukacja i innowacyjność. Z kolei zadaniem indeksu gospodarki wiedzy jest weryfikacja postawionej hipotezy- w jakim stopniu rozpatrywana gospodarka sprzyja efektywnemu korzystaniu z dostępnej wiedzy w celu rozwoju gospodarki. Indeks gospodarki wiedzy obliczany jest za pomocą średniej arytmetycznej wskaźników z następujących tematyk:

1. siła bodźców instytucjonalnych i gospodarczych (np. reguły prawa, bariery celne);
2. edukacja;
3. innowacyjność (np. wyrażana w przychodach i wydatkach na honoraria autorskie, zgłoszenia patentowe w przeliczeniu na 1 milion obywateli, liczbę artykułów i publikacji naukowych w przeliczeniu na 1 milion obywateli, licencje);
4. technologie informatyczne (np. mierzone liczbą telefonów, czy też komputerów przypadających na 1 tysiąc mieszkańców).

[21] E. Dworak, *Metody mierzenia gospodarki opartej na wiedzy; Gospodarka w praktyce i teorii*, 2008, 4(21), s. 54.

Ponad to analizując metodę KAM nie można pominąć uznanych i akceptowanych wskaźników społeczno-ekonomicznych, wyrażonych poprzez średni roczny wzrost PKB (Produkt Krajowy Brutto), a także indeksu HDI (Human Development Index). PKB stanowi najpopularniejszy wskaźnik wykorzystywany do kalkulacji w systemie rachunków narodowych SNA. Stanowi on miarę produkcji generowanej poprzez elementy produkcji w obrębie terytorium danego państwa, bez względu na to kto jest ich właścicielem[22]. Miara ta często określana jest mianem makrowskaźnika, w którym rzutuje kilka użytecznych cech, takich jak:

– zastosowanie metod analizy rachunkowej i ekonomicznej;

– powiązanie ze sobą poszczególnych wielkości ekonomicznych;

– duży stopień porównywalności określonych danych w danym czasie i przestrzeni;

– powiązanie ze sobą wielkości pewnych wielkości ekonomicznych.

Jednakże z drugiej strony PKB, jak i inne makromierniki, wzbudzają również pewnego rodzaju uwagi i kontrowersje. PKB wskazuje na miarę podaży usług i dóbr w danym roku, aczkolwiek nie odzwierciedla on rzeczywistych warunków życia danego społeczeństwa, jak i innych czynników zewnętrznych, które stanowią elementy egzystowania społeczeństwa opartego na wiedzy oraz jego gospodarki. W obrębie takich wskaźników nie uwzględnia się również czynników społecznych, które bezpośrednio związane są z rewolucją informatyczno-informacyjną. Niewątpliwie w środowisku analityków cechy te postrzegane są jako negatywne, ponieważ ograniczają użyteczność makromiernika PKB do analizy społeczeństwa opartego na wiedzy i jego gospodarki.

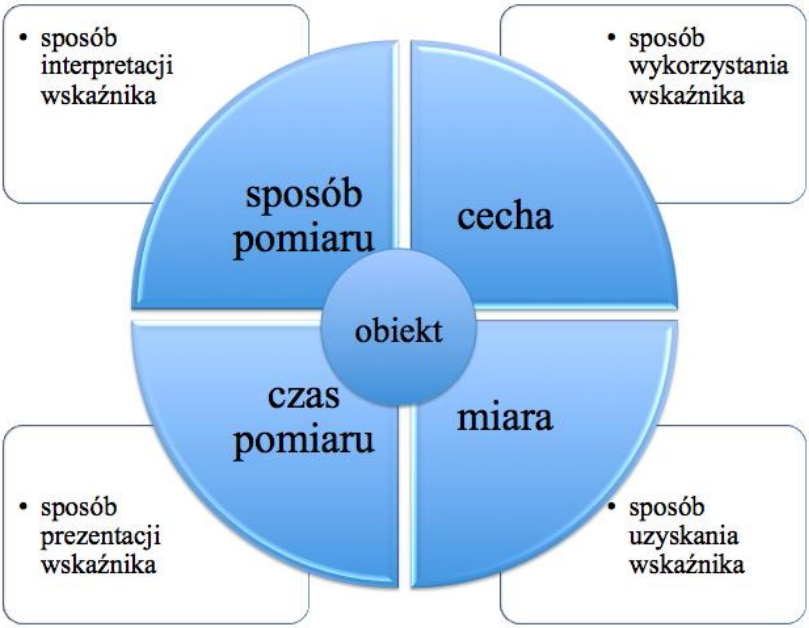
Indeks HDI stworzony został na zlecenie Organizacji Narodów Zjednoczonych przez zespół A. Sena. We wskaźniku tym można również wyróżnić wiele wad i zalet. Przede wszystkim indeks HDI uwzględnia rozwój gospodarczy, bazując na poprawie jakości życia danego społeczeństwa, z uwzględnieniem trzech innych czynników:

[22] A. Becla, S. Czaja i in., *Elementy makroekonomii*, Wydawnictwo I-BIS, Wrocław 2002, s. 30.

1. produktu krajowego brutto;
2. poziomu wykształcenia ludności (mierzonego liczbą osób dorosłych, które posiadają wykształcenie podstawowe (waga 2/3) oraz średniej ilości lat osób uczęszczających do szkoły (waga 1/3);
3. prognozowanej ilości lat życia ludzi w chwili ich urodzin.

Indeks HDI stosowany jest do dokonywania porównań w obszarze zamożności jednostek w obrębie badanego społeczeństwa oraz do prowadzenia rankingu państw z całego świata pod kątem oceny poziomu rozwoju społeczeństw. Jego wartość została przyjęta w przedziale liczbowym wyrażanym od 1 do 100 (gdzie 80-100 pkt. to rozwój wysoki, 50-80 pkt. to rozwój średni, a poniżej 50 pkt. to rozwój skrajnie niski, czyli kraje ubogie, zacofane).

Każdy ze wskaźników można zaprezentować w formie pięciu czynników: sposobu pomiaru, czasu pomiaru, jednostki pomiaru, obiektu i cechy mierzonej. Sposób prezentacji wskaźników ilustruje rysunek nr 1.



Rysunek nr 1. Zależności wskaźnika i jego charakterystyka
Źródło: Opracowanie własne.

Wskaźniki można podzielić na: względne i absolutna. Pierwsza grupa wskaźników jest łatwiejsza w porównaniu ze wskaźnikami analogicznymi do innych gospodarek i okresów. Z kolei grupa wskaźników względnych, to wskaźniki o bardziej złożonej strukturze elementów użytkowania. Do najbardziej skomplikowanych należą sposoby uzyskiwania i prezentacji wskaźników oraz sposoby ich interpretacji. Duże wyzwanie stanowi sposób wykorzystania wskaźników. Koniecznością jest, aby omawiane elementy dopierane były do każdego wskaźnika w sposób indywidualny i adekwatny do niego.

W skład obecnej wersji analizy KAM wchodzi ponad 100 wskaźników cząstkowych, które ze względu na obszar tematyczny pogrupowane są w 8 zbiorów. Wśród nich wyróżnić można: ogólny stan gospodarki; siła oddziaływania bodźców gospodarczych i instytucjonalnych; zarządzanie gospodarką; system innowacji; edukacja; praca; równość płci; technologie informatyczne. Tabela nr 1 przedstawia grupy i adekwatne do nich wskaźniki KAM wraz z jednostką przeliczeniową.

Tabela nr 1. Wskaźniki KAM

GRUPY	WSKAŹNIKI	JEDNOSTKA
OGÓLNY STAN GOSPODARKI	Przeciętny roczny wzrost PKB	%
	PKB per capita	$ (według PPP)
	PKB	$ (mld)
	Wskaźnik rozwoju społecznego HDI	
	Wskaźnik ubóstwa HPI	
	Wieloczynnikowy wskaźnik ryzyka	
REŻIM BODŹCÓW GOSPODARCZYCH I INSTYTUCJONAL-NYCH	Wskaźnik akumulacji kapitału brutto	% PKB
	Handel	% PKB
	Bariery celne i pozacelne	
	Ochrona praw własności intelektualnej	(1-7)
	Solidność banku	(1-7)
	Eksport towarów i usług	% PKB
	Różnice stóp procentowych	
	Intensywność lokalnej konkurencji	(1-7)
	Krajowe kredyty w sektorze prywatnym	% PKB
	Koszty rejestracji firmy	% DNB per capita
	Liczba dni niezbędnych do założenia firmy	
	Koszty wyegzekwowania kontraktu	% długu

GRUPY	WSKAŹNIKI	JEDNOSTKA
ZARZĄDZANIE GOSPODARKĄ	Jakość regulacji Reguły i zasady prawa Efektywność państwa Prawo głosu i wiarygodności Stabilność polityczna Kontrola nad korupcją Wolność pracy	
SYSTEM INNOWACJI	Bezpośrednie inwestycje zagraniczne (wpływ)	% PKB
	Bezpośrednie inwestycje zagraniczne (napływ)	% PKB
	Płatność za prawa autorskie i licencje	mln $
	Płatność za prawa autorskie i licencje (na 1 mln mieszkańców)	$
	Otrzymane honoraria za prawa autorskie i licencje	mln $
	Otrzymane honoraria za prawa autorskie i licencje (na 1 mln osób)	$
	Opłaty i przychody za honoraria autorskie i licencje	mln $
	Opłaty i przychody za honoraria autorskie i licencje (na 1 mln osób)	$
	Stopień udziału studentów nauk ścisłych i technicznych	%
	Stopień udziału studentów nauk ścisłych	%
	Naukowcy w sektorze B+R	
	Naukowcy w sektorze B+R (na 1 mln mieszkańców)	
SYSTEM INNOWACJI	Ogólne wydatki na B+R	% PKB
	Handel towarami	% PKB
	Współpraca badawcza pomiędzy przedsiębiorstwa, a uczelniami	(1-7)
	Liczba artykułów w czasopismach naukowych i technicznych	
	Liczba powyższych artykułów (na 1 mln osób)	
	Dostępność venture capital	(1-7)
	Zgłoszenia patentowe przyznane przez biuro patentowe	
	Zgłoszenia patentowe przyznane przez biuro patentowe (na i mln mieszkańców)	
	Eksport wysokich technologii	% eksport towaru
	Wydatki na B+R sektora prywatnego	(1-7)
	Absorpcja technologii na poziomie firm	(1-7)
	Obecność łańcucha wartości	(1-7)

GRUPY	WSKAŹNIKI	JEDNOSTKA
	Import brutta dóbr kapitałowych	mln $
	Eksport brutta dóbr kapitałowych	mln $
	Artykuły naukowe i techniczne z zagranicznym współautorem	%
	Średnia liczba cytatów na artykuły naukowe i techniczne	
EDUKACJA	Stopa alfabetyzacji dorosłych	% osób powyżej 15 lat
	Średnia lat pobierania nauki szkolne	
	Udzielanie osób odbierających edukacje na poziomie średnim do ogółu populacji w wieku uczniów szkół średnich	
	Udział osób odbierających edukacje na poziomie wyższym do ogółu populacji w wieku studentów szkół wyższych	
	Oczekiwania długości życia w dniu narodzi	
	Dostęp do Internetu w szkołach	(1-7)
	Wydatki publiczne na edukacje	% PKB
	Wyniki testów matematycznych (2 stopień)	
	Wyniki testów z nauk ścisłych (2 stopień)	
	Wyniki testów matematycznych (8 stopień)	
	Wyniki testów z nauk ścisłych (8 stopień)	
	Jakość edukacji w zakresie nauk ścisłych i matematyki	(1-7)
	Jakość kształcenia menedżerów	(1-7)
	Umiejętności matematyczne 15-latków	
	Umiejętności z nauk ścisłych 15-latków	
PRACA	Stopa bezrobocia	% siły roboczej
	Zatrudnienie w przemyśl	%
	Zatrudnienie w usługach	%
	Profesorowie i technicy	% siły roboczej
	Zakres szkoleń personelu	(1-7)
	Drenaż mózgów	(1-7)
	Współpraca w stosunkach pracowników-pracodawca	(1-7)
	Elastyczność ustalania płac	(1-7)
	Płace i wydajność	(1-7)
	Zaufanie do profesjonalnego zarządzania	(1-7)
	Lokalna dostępność	(1-7)

GRUPY	WSKAŹNIKI	JEDNOSTKA
PRACA	specjalistycznych usług badawczych Trudność z indeksem zatrudnienia Trudność z indeksem zwalniania Koszty zwalniania (tygodniowe wynagrodzenie) Podatek dochodowy i składki emerytalne Wskaźniki zatrudnienia ludności (powyżej 15 roku życia) Wskaźniki zatrudnienia ludności w wielu 15-24 lata Udział bezrobotnych z wykształceniem wyższym Udział bezrobotnych z wykształceniem średnim Wysokość udziału siły roboczej Siła robocza z wyższym wykształceniem Siła robocza ze średnim wykształceniem Firmy oferujące formalne szkolenia	 % % % % całości % całości % firm
RÓWNOŚĆ PŁCI	Indeks rozwoju płci GDI Kobiety w sile roboczej Miejsca w parlamencie zajmowane przez kobiety Skolaryzacja brutto na poziomie średnim kobiet Skolaryzacja brutto na poziomie średnim kobiet	 % siły roboczej % całości % brutto % brutto
TECHNOLOGIE TELEINFORMATYCZNE	Liczba telefonów na 1000 osób Główne linie telefoniczne na 1000 osób Telefony komórkowe na 1000 osób Komputery na 1000 osób Gospodarstwa domowe posiadające telewizory Gazety codzienne na 1000 osób Przepustowość międzynarodowego Internetu Użytkownicy Internetu na 1000 osób Koszyk cen za Internet Elektroniczny dostęp do usług publicznych Zakres wykorzystania Internetu w działalności gospodarczej Wydatki na technologie teleinformatyczne	 % $ na miesiąc (1-7) (1-7) % PKB

Źródło: www.wordlbank.org (dostęp: 01.10.2016)

Metoda KAM bazuje na kilku istotnych założeniach. Pierwszy z nich to odpowiedni dobór wskaźników merytorycznie opisujących analizowane zjawisko, w którym ma miejsce rozwój (ewolucja) gospodarki opartej na wiedzy. Drugie założenia dotyczy normalizacji zmian ujętych w przedziale <0,10>. Trzecim ważnym czynnikiem jest to, że wszystkie elementy rozpatrywane są jako jednakowo ważne dla gospodarki opartej na wiedzy. Omawiane trzy założenia poddane głębszej analizie wzbudzają pewne kontrowersje. Poprawnie dobrane wskaźniki muszą zostać przyporządkowane w taki sposób, aby zachowany był ścisły związek z rozwojem gospodarki opartej na wiedzy. Jednakże główny problem tkwi w odpowiednim rozpoznaniu samego rozwoju gospodarki, mechanizmów i potencjalnym kierunków dalszego rozwoju. Właściwy wybór wskaźników powinien wpłynąć na realizacje przyjętych zadań.

4. Podsumowanie

Scharakteryzowana i oceniona w niniejszym artykule metoda KAM należy do jednych z najpopularniejszych sposobów do przeprowadzenia analizy zaawansowania poziomu rozwoju (ewolucji) badanej gospodarki opartej na wiedzy oraz społeczeństwa informacyjnego. Taki stan można określić efektem dużej pojemność informacyjnej, która wykorzystywana jest w obrębie ich wskaźników, jak i zalet deskrypcyjnych, poznawczych i implementacyjnych danych indeksów. Z kolei do zalet z obszaru technicznego metody KAM należą: łatwość w interpretacji wskaźników, powiązanie ze sobą wskaźników z systemem statystyki społeczno-ekonomicznej, rozwojowy charakter grup użytkowanych wskaźników, co wpływa na szeroko rozumiane rozszerzenia prowadzące do wzrostu wiedzy.

Aczkolwiek, jak zostało to udowodnione w części głównej niniejszej publikacji, metoda KAM posiada również pewne wady, które nierzadko dotyczą jej podstaw metodologicznych (brak zróżnicowania roli informacji, liczne uogólnienia oraz uproszczenia obrachunkowe). Wśród pozostałych wad metody KAM wyróżnić można: bariery pojęciowe oraz informacyjne. Nie wszystkie czynniki można włączyć do mechanizmu analizy KAM, ze względu na to, że procesy zachodzące w gospodarce opartej na wiedzy i jej

społeczeństwie informacyjnym nie są dostatecznie sprecyzowane i nie można ich wyrazić w przełożeniu na dane statystyczne. Należy dążyć do jak najdokładniejszego sprecyzowania warstwy pojęciowej, co przełoży się na łatwość dopasowania metody KAM do ciągle to nowych wymagań. Należy jednak w tym miejscu podkreślić, że nie uniknie się kontrowersji związanych z ta problematyką, ponieważ jest to cecha współczesnych analiz ekonomicznych.

Metoda KAM nie jest jedyną metodą modelowo-ilościową, służącą do prowadzenia badań nad społeczeństwem informacyjnym i gospodarką opartą na wiedzy. Jednakże bez wątpienia posiada ona największe perspektywy rozwoju w tym kierunku.

Literatura

1.M. Galka, *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2008, s. 79.

2.S. Czaja, A. Becla, M. Celińska, *Informacja a współczesna gospodarka i społeczeństwo,* Wydawnictwo PWSZ w Głogowie, Głogów 2011, s. 79.

3.A. Becla, S. Czaja, M. Hałasa, *Etapy rozwoju (zaawansowania) społeczeństwa informacyjnego. Wybrane zagadnienia*, [w:] *Społeczeństwo informacyjne. Uwarunkowania społeczne i kulturowe,* red. P. Setlak, P. Szumlich, PWSZ w Tarnobrzegu, Tarnobrzeg 2010, s. 41-52.

4.E. Dworak, *Metody mierzenia gospodarki opartej na wiedzy; Gospodarka w praktyce i teorii*, 2008, 4(21), s. 54

5.A. Becla, S. Czaja i in., *Elementy makroekonomii,* Wydawnictwo I-BIS, Wrocław 2002, s. 30.

Źródła internetowe:

1.www.nauka.gov.pl, s. 62 (dostęp: 20.09.2016)

2.www.wordlbank.org (dostęp: 01.10.2016)

Клапків Ю.М.
доцент кафедри фінансів ім. С.І. Юрія,
Тернопільського національного економічного університету,
кандидат економічних наук

НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ФУНКЦІОНУВАННЯ СТРАХОВИХ КОМПАНІЙ

Домінуючою на сьогодні тенденцією розвитку міжнародної фінансової сфери є інтеграція та вихід на нові ринки інституцій що надань фінансові послуги, в тому числі і страхові послуги. Проте, в організаційно-правова форма інституції що надають навіть ідентичні по страховому покритті страхові послуги у кожній європейській країні може відрізнятись.

Проблема організації ефективного регулювання та нагляду за діяльністю фінансових інституцій є предметом дослідження багатьох зарубіжних та вітчизняних авторів: Р. Бернда, О. Дзюблюка, Ед. Доллана, И. Кожевникової, Л. Конопатської, В. Кротюка, Ж. Матука, А. Мороза, С. Мочерного, А. Пересади, Дж. Селбі, Дж. Сороса, Дж. Синки, Т. Уїльямсон та ін. Засади функціонування інституцій страхування постійно знаходяться в полі зору вітчизняних науковців і практиків страхового бізнесу, зокрема Т. Артюх, В. Базилевича, Д. Гвасалії, О.Залєтова, Л. Куделі, О. Ковтуна, С. Осадця, О. Кнейслер, В.Тринчука, Т. Яворської та інших.

Аналіз існуючих методичних матеріалів, а також наукових публікацій з питань страхової справи засвідчує, інтеграція та відкриття кордонів стимулює поширення страхових послуг, що надаються інституціями різних видів оминаючи кордони держав та не акцентуючи увагу на валюті надання послуги, що має важливе значення для розвитку парабанківської системи України. Проте вона недостатньо розроблена в теоретичному й методичному планах, та в перспективі потребує вдосконалення.

Формулювання цілей статті. Метою статі є дослідження основних правових форм діяльності страхових компаній, притаманних вимог до фінансових інституцій такого типу, компаративний аналіз форм страхових інституцій представлених

у європейських країнах, що в перспективі можуть реалізовувати страхові послуги громадянам України.

Виклад основного матеріалу. Діяльність страхових акціонерних товариств найчастіше регулюється через діючі в національних правових системах законодавчі норми в основному в галузі страхування.

Водночас, на відміну від основних сфер, яким притаманна форма акціонерного товариства, страхові компанії що діють в цій формі мають ряд підвищених вимог: значніші вимоги до капіталу, фінансування ліквідності, резервів, інвестування резервів, розподіл прибутку, а також інший рівень нагляду часто виокремлений з системи національного банку.[6]

Існуючі визначення акціонерного товариства, у тому числі, зокрема, ті організаційно-правові форми в яких може бути утворена страхова компанія дещо відрізняються в різних країнах.

В Україні страхові послуги можуть надавати фінансові установи, які створені у формі:

- акціонерних,
- повних,
- командитних товариств
- товариств з додатковою відповідальністю.

Їх особливості визначаються Законом України «Про господарські товариства», та основною характерною рисою є мінімальна кількість учасників в обсязі три особи, та одержання ліцензій на здійснення страхової діяльності.

В даному аспекті законодавство багатьох країн Європи є більш лаконічним, так польське законодавство визначає лише акціонерне товариство, яке енциклопедія менеджменту визначає акціонерне товариство, як фінансову інституцію, створену засновниками для, щоб законодавчо допустимої діяльності. Вона є юридичною особою і її статутний капітал формується із внесків акціонерів, який вказується в статуті і ділиться на акції рівної номінальної вартості. Акція є підставою набуття прав акціонера (акціонерів), може мати характер іменний або на пред'явника, звичайний або привілейований що стосується права

голосу, дивіденди або розподілу майна у разі ліквідації акціонерного товариства. [2]

Окрім того, регулятор для страхових компаній у формі страхових товариств виставляє додаткові вимови в тому числі щодо бенефіціантів. Суб'єкт, який придбав акції або права по акціях або вступив в акції, або права з акцій, у кількості, що перевищує 10 відсотків загального числа акцій, зобов'язаний повідомити міністра у справах фінансових установ, протягом 7 днів з моменту цієї події. Крім того, особа, що має намір придбати акції або права по акціях або прийняти акції або права за акціями, кількість яких перевищує, відповідно, 25%, 50%, чи 75% загального числа голосів на загальних зборах зобов'язаний отримати дозвіл міністра у справах фінансових установ для проведення цієї операції.

Рішення може бути негативним у випадку, якщо:

– юридична особа, яка має намір набути або обійняти, не дає гарантії ведення справ у страховій компанії у спосіб, що належним чином захищає інтереси застрахованих,

– кошти призначені на придбання походять з кредиту або позики або іншим чином обтяжені,

– це суперечить економічним інтересам держави.

Окремі вимоги Українське законодавств виставляє до статутного капіталу (мінімальний розмір статутного капіталу страхової компанії, що займається видами страхування, іншими, ніж страхування життя, встановлюється в сумі 1 млн. євро, а страхової компанії, що займається страхуванням життя, - 1,5 млн. євро в гривневому еквіваленті. Статутний капітал страхової компанії повинен бути оплачений виключно в грошовій формі. Допускається формування статутного капіталу страхової компанії цінними паперами, що випускаються державою, за їхньою номінальною вартістю в порядку, встановленому Національною комісією, що здійснює державне регулювання у сфері ринків фінансових послуг, але не більше 25 відсотків загального розміру статутного капіталу).[7]

Вимоги щодо менеджменту страхової компанії стосуються досвіду роботи, керівництва та певного технічного забезпечення (Голова виконавчого органу та його перший заступник повинні

мати вищу юридичну або економічну освіту, а головний бухгалтер - вищу економічну освіту. Також страховик та його відокремлені підрозділи повинні бути забезпечені комп'ютерною технікою і програмним забезпеченням і комунікаційними засобами, які відповідають встановленим вимогам. Дані вимоги не встановлені Законом про страхування, однак передбачені Розпорядженням про ліцензійні умови.

Енциклопедії англомовні визначаючи акціонерне товариство, найчастіше, з'єднують аспект власності та функціональний, зазначаючи, що акціонерне товариство це підприємство, яке функціонує з метою отримання прибутку, що є власністю акціонерів і ними ж управляється [1].

Німецька наукова школа, визначає акціонерне товариство в якості фінансової компанії, яка має статус юридичної особи (яка є юридичною особою), якою володіють дарувальники капіталу акціонери. [3].

Узагальнюючи можемо прийти до висновку, що інституція, у якій зосереджено формування та надання страхових послуг це - страхова компанія у формі акціонерного товариства, метою якої є приносити прибуток власникам (акціонерам), діяльність яких заснована на припущенні взаємність та системою поділу повноважень власників через акціонерів,що передали частину власності в обмін на участі в прийнятті рішень, пов'язаних з функціонуванням та поділом прибутків від основної діяльності.

Таблиця 1

Форми акціонерних товариств у окремих країнах та форми акціонерних товариств, що можуть надавати страхові послуги

N	Країна	Дозволені форми акціонерних товариств	Акціонері товариства, що можуть бути страховими компаніями
1.	**2.**	**3.**	**4.**
1	Австрія	die Aktiengesellschaft	Die Aktiengesellschaft
2	Бельгія	– la société anonyme	De naamloze vennootschap
3	Болгарія	акционерно дружество	акционерно дружество

N	Країна	Дозволені форми акціонерних товариств	Акціонері товариства, що можуть бути страховими компаніями
1.	**2.**	**3.**	**4.**
4	Кіпр	Δημόσιες εταιρείες περιορισμένης ευθύνης με μετοχές, δημόσιες εταιρείες περιορισμένης ευθύνης με εγγύηση που διαθέτουν μετοχικό κεφάλαιο	Акціонерні компанії із вартістю акцій (€ 683,440 ризикового страхування, € 1.025.160 для страхування життя, € 1.710.000 для перестрахування) і мінімальним гарантійним фондом € 3,000,000 з коректівою на інфляцію
5	Данія	aktieselskaber	aktieselskaber
6	Естонія	aktsiaselts	aktsiaselts
7	Фінляндія	julkinen osakeyhtiö/publikt aktiebolag	Publikt aktiebolag
8	Франція	la société anonyme	la société anonyme
9	Греція	ανώνυμη εταιρία	Ανώνυμη εταιρία
10	Іспанія	la sociedad anónima	La sociedad anónima
11	Нідер-ланди	de naamloze vennootschap	De naamloze vennootschap
12	Ірландія	public companies limited by shares / public companies limited by guarantee having a share capital	Public companies limited by shares
13	Литва	akcinė bendrovė	akcinė bendrovė
14	Люксем-бург	la société anonyme	la société anonyme
15	Латвія	akciju sabiedrība	Akciju sabiedrība
16	Мальта	kumpannija pubblika/public limited liability company, kumpannija privata/private limited liability company	компанії з розділеними портфелями та інкорпоровані компанії з розділеними портфелями*

N	Країна	Дозволені форми акціонерних товариств	Акціонері товариства, що можуть бути страховими компаніями
1.	**2.**	**3.**	**4.**
17	Німеччина	die Aktiengesellschaft	Die Aktiengesellschaft
18	Португалія	a sociedade anónima	a sociedade anónima
19	Чеська Республіка	akciová společnost	akciová společnost
20	Румунія	societate pe acțiuni	societate pe acțiuni
21	Швеція	aktiebolag	Aktiebolag
22	Словач-чина	akciová spoločnosť	akciová spoločnosť
23	Словенія	delniška družba	delniška družba
24	Україна	акціонерні товариства, товариства з обмеженою відповідальністю, товариства з додатковою відповідальністю, повні товариства, командитні товариства	акціонерні товариства, товариства з додатковою відповідальністю, повні товариства, командитні товариства.
25	Угорщина	részvénytársaság	Részvénytársaság
26	Велико-британія	public companies limited by shares, public companies limited by guarantee having a share capital	public companies limited by shares
27	Італія	la società per azioni	la società per azioni

Побудовано автором.

*1 лютого 2011 р. набули чинності «Положення про інкорпорованих компаніях з розділеними портфелями, які здійснюють страхову діяльність, до Закону «Про компанії»« (Companies Act (Incorporated Cell Companies Carrying on Business of Insurance) Regulations), що визначають можливість реєстрації інкорпорованих компаній з розділеними портфелями (ИКРП).

Актуальність вивчення існуючих форм акціонерних товариств та дозволених для фінансових інституцій таких як страхова компанія обумовлений інтеграцією. Відкритістю надання фінансових послуг в середині Європейського співтовариства, та можливістю надання страхових послуг страховиками - нерезидентами в Україні, на даний момент лише за наявності відповідних ліцензій виданих вітчизняним регулятором постійним представництвам у формі філій іноземних страхових компаній. [5]

Висновки. Отже, варто відзначити що функціональна і організаційна складова надання страхових послуг страховими компаніями, безпосередньо жодним чином не пов'язані з власністю (юридичним відношенням власності), хоча їх поєднання в одній особі (страховика і одночасно акціонера) можливо. Звідси можливість існування товариств взаємного страхування, та пов’язання між клієнтом (страхувальником) і страховою компанією, частіше у страховій справі присутні лише відносини купівлі-продажу страхової послуги, не пов'язані з набуттям права власності [4].

В процесі розвитку єдиного фінансового ринку Європи нормативно-правові засади функціонування страхових компаній підлягали змінам та в більшості країн уніфікувались до єдиної акціонерної форми, де форма власності та прийняття управлінських рішень дозволяє найкраще контролювати фінансові та технічні резерви, платоспроможність та менеджмент інституції. Даний тим переважаючої інституції найближчий що акціонерного товариства із дещо вищими вимогами до статутного капіталу, менеджменту та мінімальної кількості засновників.

Список літератури

1.Encyclopedia of banking & finance/ Munn, Glenn G., Ferdinand Lawrence Garcia, and Charles J. Woelfel. – St. James Press, 1991. – S. 533.

2.Encyklopedia zarządzania: podstawowe kategorie i terminy.// Penc, Józef/ Wyższa Szkoła Studiów Międzynarodowych, 2008.

3.Farny Dieter Versicherungsbetriebslehre / Farny Dieter. – Verlag Versicherungswirtsch., 2006. – S.945.

4.Mehr R. Principles of insurance// Mehr, Robert Irwin, and Emerson Cammack / RD Irwin, 1972. – S. 527.

5. Закон України Про страхування (Відомості Верховної Ради України (ВВР), 1996, N 18, ст. 78// http://zakon5.rada.gov.ua/laws/show/85/96-вр

6. Клапків Ю.М. Різновиди поділу та детермінанти майнових ризиків / Юрій Клапків // Соціально-економічні перспективи розвитку України в XXI столітті: збірник тез доповідей II міжнародної науково практичної Інтернет-конференції (Тернопіль, 27 травня 2014 року). – Вектор. – Тернопіль, 2014. – С. 14-18.

7.Клапків Ю.М. Фінансовий механізм консолідації банківсько-страхового бізнесу України.// Ю.М. Клапків / Наука й економіка. Науково-теоретичний журнал Хмельницького економічного університету. – 2009. – Випуск 4(16) Том 1. – С. 57-64.

Лиско Г. О. –
адвокат, помічник народного депутата
директор ГО «Львівський центр медіації»

ЕФЕКТИВНЕ УПРАВЛІННЯ КОНФЛІКТАМИ В ІТ-КОМПАНІЯХ

Для успішної діяльності будь-якої ІТ – компанії важливою є не лише створення якісного та конкурентноздатного технологічного продукту, але й ефективна організація міжособистісних відносин. Мова йде про успішну побудову горизонтальних та вертикальних відносин всередині організації (між працівниками, різними відділами, проектним менеджером та керівництвом компанії) та системи комунікації із зовнішнім світом (зокрема, клієнтами, партнерами тощо).

Важливим для кожної компанії, яка претендує на успіх, є налагодження способів комунікації та швидкого вирішення конфліктів. Одним із можливих інструментів є медіація (англ. *mediation* – посередництво). Медіація – це вид переговорів за допомогою одного або кількох нейтральних посередників (медіаторів) з метою прийняття сторонами взаємоприйнятного рішення. Варто зауважити, що зазвичай медіація визначається як альтернативний судовому спосіб вирішення конфліктів. Проте, як правильно стверджує американський професор Джордж Сідел, медіацію не варто визначати лише як спосіб вирішення конфліктів, оскільки, як свідчить практика, медіація може також застосовуватись і у безконфліктних відносинах,

зокрема, при укладенні угод та прийнятті рішень [2] (наприклад, рішення керівника щодо розподілу ресурсів між двома відділами компанії) тощо.

Характерною рисою медіації є те, що медіатор не приймає рішення за сторони, не має права радити та давати власну оцінку ситуації. Завданням медіатора є:

– налагодити процес спілкування між сторонами;

– допомогти сторонам глибше зрозуміти їх позиції та віднайти інтереси;

– стежити за дотриманням процедури ведення переговорів;

– стимулювати кожну із сторін до продукування власних пропозицій у напрямку конструктивного прийняття рішення;

– уточнювати та контролювати готовність сторін виконувати запропоновані дії.

Важливою особливістю медіації є те, що вона ґрунтується на стратегії ведення переговорів та управління конфліктами на основі інтересів та є реалізацією партнерського підходу. Ця стратегія передбачає взаємне прагнення сторін до позитивного взаємодії в рамках моделі «win - win».

Основні особливості переговорів на основі інтересів детально описані у книзі «Досягнення згоди» Р. Фішером і У. Юрі:

– учасники спільно аналізують проблему і спільно шукають варіанти її вирішення, демонструючи іншій стороні, що є її партнером, а не суперником;

– увага концентрується не на позиціях, а на інтересах конфліктуючих сторін, що передбачає їх виявлення, пошук спільних інтересів, пояснення власних інтересів і їх значимості опонентові, визнання інтересів іншої сторони частиною вирішуваної проблеми;

– учасники переговорів орієнтовані на пошук взаємовигідних варіантів вирішення проблеми, що вимагає не звужувати розрив між позиціями в пошуках єдиного правильного рішення, а збільшувати кількість їх можливих варіантів;

– конфліктуючі сторони прагнуть використовувати об'єктивні критерії, що дозволяє виробити розумне угоду, а тому повинні відкрито обговорювати проблему і взаємні аргументи, не повинні піддаватися можливому тиску;

– в процесі переговорів передбачено чітке розмежування взаємин опонентів і самої проблеми, важливим є вміння поставити себе на місце опонента і спробувати зрозуміти його точку зору, наполегливість в бажанні розібратися з проблемою і шанобливе ставлення до людей;

– досягнуту угоду має максимально враховувати інтереси всіх учасників переговорів [1].

Застосування медіації має чимало переваг, основною з яких є швидкість процедури та реальна можливість отримати результат за порівняно невеликий проміжок часу. Це корисно як для внутрішніх відносин в компанії, так і для вирішення конфліктних ситуацій з зовнішніми контрагентами. Медіація допомагає зберегти здорову атмосферу в колективі та підвищити ефективність та результативність роботи цілої компанії.

Ще однією важливою перевагою є конфіденційність процедури.

Медіатор не має права розголошувати інформацію, що відноситься до процедури медіації і стала йому відомою під час її проведення, без згоди сторін.

Крім того, гнучкість та неформальність процедури дає сторонам можливість реально впливати на результат та приймати рішення відповідно до своїх інтересів, а не бути пасивним учасником процесу під час якого третя стороння особа замість сторони приймає важливе для неї рішення. Щодо того, хто все ж таки може бути медіатором – особа з вищою освітою, яка пройшла спеціальні навчання на розвиток навичок медіатора. Для вирішення конфліктів та прийняття рішень в межах компанії, окрім аутсорсингу, доцільним є оволодіння навичками медіації деяких з працівників (юрист, HR, проектного менеджера чи ін.), що уможливить швидке та ефективне вирішення конфліктів та допоможе у прийнятті важливих рішень.

Таким чином, медіація є одним із практичних та ефективних інструментів, який сприяє успішній організації міжособистісних відносин в компаніях, а отже і підвищує їх продуктивність.

Список літератури

1.Fisher, R., Ury, W. and Patton, B. (1991). Getting to Yes: negotiating Agreement Without Giving In. Second Edition. New York: Penguin Books

2.Successful Negotiation: Essential Strategies and Skills//George Siedel, Thurnau Professor of Business Law, University of Michigan//[Електронний ресурс]-Режим доступу: https://www.coursera.org/learn/negotiation-skills/home/welcome

Мізюк Б.М. –
завідувач кафедри Туризму і готельно-ресторанної справи,
Львівський торговельно-економічний університет,
доктор економічих наук, професор

КОНЦЕПЦІЯ ІНФОРМАЦІЙНОЇ ДУГИ В ПРОЦЕСІ ПРИЙНЯТТЯ РІШЕНЬ

Прийняття обґрунтованих рішень становить важливий елемент ефективної діяльності керівників усіх рівнів системи управління. Справність процесу прийняття рішень на всіх рівнях управління в кінцевому підрахунку визначає конкурентну позицію організації. Важливо, що кожне рішення приймається в рамках певного обсягу інформації, що отримується в обмеженому інтервалі часу. Причому основою успішного управління виступає повнота, достовірність та своєчасність отримуваних особою приймаючою рішення (ОПР) даних. Інформаційна підтримка набуває особливого значення при розв'язанню стратегічних завдань.

Забезпечення розвитку діяльності підприємств повинно базуватись на постійному моніторингу стану відповідного сегменту ринку. Чинники зовнішнього і внутрішнього середовища, що постійно змінюються суттєво впливають на стан суб'єктів господарювання. В цьому випадку розробка відповідних стратегій виступає важливим інструментом

зміцнення їх конкурентних позицій. Тому питання стратегічного розвитку підприємств і організацій досліджуються протягом багатьох десятиріч. Основні результати досліджень в цій області відображені в працях І. Ансофера, М. Портера, А. Томпсона, Дж. Стрікленда, А. Чандлера, Д. Бодді, Р. Пейтона та ряду вітчизняних вчених таких як Е. Шершньова, А. Довгань, А. Наливайко та інших. В дослідженнях відомих науковців достатньо повно розкривається концепції альтернатив і вибору оптимальної стратегії та способи її імплементації. Проте прискорення змін як у зовнішньому так і внутрішньому середовищі підприємств зумовлює потребу в більш глибокому розумінні та вирішення проблеми ефективного інформаційного забезпечення кожного кроку прийняття стратегічних рішень.

Постановка завдання

Стаття має на меті дослідження ролі інформаційного забезпечення в процесі прийняття стратегічних рішень. Завдання полягає у формуванні такої системи раннього розпізнавання ситуації, яка б надавала можливість звузити ступінь інформаційної невизначеності і тим самим підвищення обґрунтованість стратегічних рішень.

Виклад основного матеріалу дослідження

Систематизована послідовність викладу включає чотири етапи:

А – структуризація процесу прийняття рішень;

Б – характеристичні риси стратегічних рішень;

В – інформаційна невизначеність прийняття стратегічних рішень;

Г – система раннього розпізнавання ситуації в процесі прийняття стратегічних рішень.

А. Управління організацією представляє собою складний набір дій пов’язаних з послідовним виконанням найкращих та доступних на даний час опцій. Їх вибір пов'язаний як з використанням доступних на даний час засобів. Підставою для цього є прийняття обґрунтованих рішень відповідно до прийнятого критерію оптимального співвідношення між витратами та отримуваними ефектами. Їх праця зосереджується на визначенні та ідентифікації проблеми, пошуку альтернативних варіантів їх вирішення, вибору найкращого

варіанту та встановлення способів його реалізації, що приведе до розв'язку проблеми. Виходячи з цього прийняття рішення можемо визначити як детерміновану реалізацію певних дій, раціональність здійснення яких залежить від продуманої поведінки особи приймаючої рішення (ОПР). В структурному відношенні процес прийняття рішень можна схематично представити наступним чином:

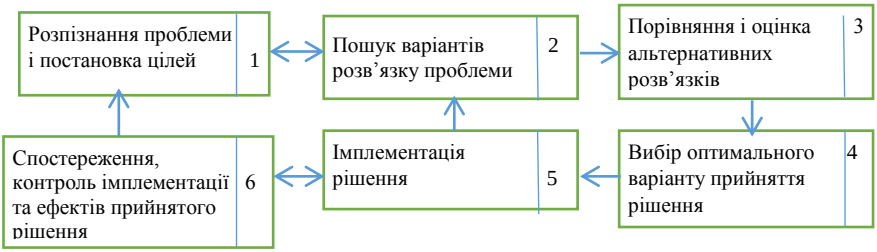


Рис. 1. Структура процесу прийняття рішень

Процес прийняття рішень характеризується високою динамічністю, а ключову роль в ньому відіграє інформація. Як видно зі схеми процес прийняття рішень складається з 6-ти блоків, кожен з них має свої особливості:

1. Розпізнання проблеми і постановка цілей – необхідність фіксації негативних подій та загроз, що появляються в зовнішньому або внутрішньому середовищі та вказують на розбіжність між фактично виникаючою та очікуваною ситуацією. Це вимагає перегляду цілей, що були поставлені до виникнення проблеми у відповідності до зміни обставин і усунення небажаного становища.

2. Пошук варіантів розв'язку проблеми – полягає в знаходженні шляхів виходу з небажаної ситуації, враховуючи при цьому силу загроз та сильні сторони власного потенціалу. Причому розробляється декілька варіантів побудови сценаріїв розрішення проблеми виходячи із адекватності наявної інформації до гостроти проблеми.

3. Порівняння і оцінка альтернативних розв'язків – базується на суб'єктивній оцінці ОПР ступеню виникаючої. При цьому враховується ймовірність реалізації кожного варіанту ,

можливі наслідки від цього та ступінь відповідності до поставлених цілей.

4. Вибір оптимального варіанту прийняття рішень – є визначальним в процесі прийняття рішень. Полягає у визначенні ОПР напрямку та послідовності дій з врахуванням діапазону наявних засобів. Основою вибору виступає критерій згідно якого даний варіант є найкращим. Результатом акту вибору є рішення, в якому відображено алгоритм, згідно якого вказується хто має діяти, як має діяти в якій послідовності і з допомогою яких засобів та ресурсів.

5. Імплементація рішення – полягає в реальному впровадженні прийнятого рішення з абстрактної площини в практичні операційні дії, які повинні здійснюватись в умовах, що визначаються в попередньому блоці.

6. Спостереження і контроль імплементації та ефектів прийнятого рішення – завершальний етап прийняття рішення, який полягає в постійному моніторингу здійснюваних операцій, оцінці отримуваних результатів, їх порівнянні із запланованими, часом виконанням та впливу на кінцевий розв'язок проблеми.

Раціональність здійснення описаного процесу прийняття рішень залежить від набору певних обмежень, що відносяться до ситуації, при якій виникла проблема, її складності, часу відведеному на аналіз і прийняття рішення і т.п. В залежності від обмежень ОПР змушений діяти в умовах неповної, недостовірної і часто несвоєчасної інформації, що знищує рівень обґрунтованості рішення. В залежності від ступеня інформаційного забезпечення можна виділити три моделі прийняття рішення:

– детерміновану, що відповідає умовам чіткого усвідомлення ситуації та причин виникнення проблеми;

– ризикову, коли приймати рішення потрібно в умовах неповної інформації, а достовірність даних, що є відомі, викликає сумнів;

– стратегічну, коли ОПР не може знати про майбутній перебіг подій і відповідно подальший розвиток проблеми.

Б. Третя модель, що відображає процес прийняття стратегічних рішень, має складний характер, оскільки пов'язана

з непевністю отримання запланованих результатів в перспективі. Стратегічні рішення носять комплексний характер і відносяться до всіх рівнів управління організацією. Вони ініціюють тактично-оперативні рішення і власне від ступеня їх обґрунтованості залежить ефективність та повнота виконання завдань на низових рівнях. Стратегічні рішення визначають напрямок і темп розвитку організації її довготермінове функціонування. Від низ залежить встановлення тв. Використання стратегічних переваг та способів і методів реалізації обраної стратегії.

Процес прийняття стратегічних рішень включає послідовність дій, що мають на меті звузити розбіжності між встановленими стратегічними цілями і фактичними результатами використання своїх стратегічних переваг перед конкурентами. Мова йде про звуження так званої «стратегічної дуги» що виражає співвідношення між організацією і бізнес-середовищем і відображає відмінність між фактичною і бажаною конкурентною позицію організації. В певному сенсі «стратегічна дуга» виступає мірою ступеня незбалансованості фактичного стану організації до умов середовища.

Особливістю прийняття стратегічних рішень є те, що джерела проблем, які виникають для організації, знаходяться поза її межами в зовнішньому середовищі і тому контроль над ними є обмеженим. Це пов’язано з прискоренням змін, що відбуваються в оточенні організації та викликають непевність його становища і відповідно збільшують величину «стратегічної дуги». Вона є похідною від «дуги інформаційної», і тому завдання полягає в мінімізації останньої.

В. ОПР, що стоїть перед необхідністю прийняття рішення, як правило володіє обмеженим набором інструментарію розв’язку проблеми. Це пов’язано з обсягом і якістю інформації, що є в його розпорядженні та власним баченням змісту та суті самої проблеми. Особливість та якість інформації беззаперечно впливає на процес прийняття рішення. Розв’язок проблеми вимагає постійного отримання актуальних даних, але в умовах змін їх обсяг є меншим від необхідного.

Різницю між бажаним і якісним обсягом даних і тими даними які є в наявності та можуть бути отримані в подальшому

назвемо «інформаційною дугою». Власне це той недостаток інформації, який не дозволяє повністю зрозуміти суть та причини виникнення проблеми. Він має суб'єктивний характер і певні властивості:

– відноситься до конкретного суб'єкту (брак інформації відчувається різними ОПР по різному);

– вразливість до часу (з плином часу «інформаційна дуга» може скорочуватись або збільшуватись);

– розмитість ліній (важко окреслити величину розходжень між фактичними та необхідними даними);

При прийнятті рішень ОПР знаходиться під впливом двох чинників: 1) обмеження в засобах; 2) обмеження часі, а це утруднює пошук необхідних для обґрунтованого рішення даних. Чим більше часу і засобів, тим вища якість і раціональність пошуку необхідної інформації, краще розуміння ситуації та зменшення непевності.

Проілюструвати «інформаційну дугу» з позиції понесених витрат на отримання даних і поступу у встановленні ситуації на основі отриманої інформації можна наступним рисунком (рис. 3):

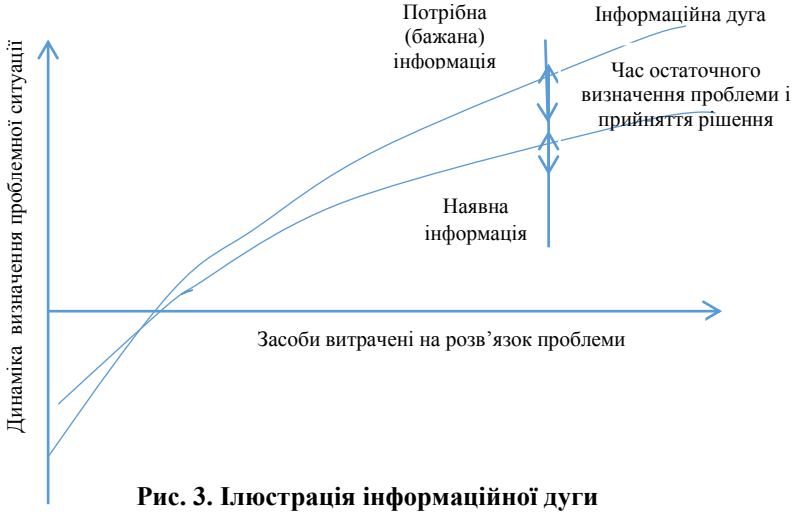


Рис. 3. Ілюстрація інформаційної дуги в процесі прийняття рішень

Процес прийняття рішення починається від моменту появи розходження між стратегічними цілями і дійсним станом в якому знаходиться організація. Проблема, як правило, виникає раптово і чим більше часу відводиться на її осмислення, тим більше вона робиться зрозумілою. Після усвідомлення проблеми і причин її виникнення відбувається прийняття відповідних рішень. А це потребує засобів, інформації та часу на її здобуття. Пошук відбувається в умовах більшого чи меншого ризику, який залежить від величини «інформаційної дуги». Збільшення обсягу інформації проводить до зменшення ризику прийняття необґрунтованого рішення і навпаки, чим менше інформації тим більша вірогідність прийняття невірного рішення. Чим досконаліші способи пошуку даних, тим більша кількість і якість необхідної інформації і краще можна зрозуміти суть проблеми. Разом з тим фактично добута інформація не перевищуватиме всієї повноти необхідної. Тому зменшення «інформаційної дуги» є можливим лише в суб'єктивному сенсі.

Г. Важливість прийняття рішень стратегічного характеру витікає із необхідності появи у зовнішньому середовищі серйозних загроз і проблем, що вимагає швидкої реакції. Це в свою чергу ставить питання про виділення в інформаційному полі власне інформації стратегічного характеру, яка відрізняється від рутинної інформації необхідної в поточному управлінні для прийняття рішень операційного характеру. Її особливістю є те, що вона проявляється у формі слабких сигналів, що формуються у зовнішньому середовищі незамітно, посилюються з плином часу і в певний момент відображають появу проблеми. Разом з тим завданням стратегічного управління є не тільки розв'язок проблеми, а насамперед її упередження і не допущення. Тому на перший план виступає питання створення інструментарію, який би надавав ОПР можливість вчасно отримувати слабкі сигнали та підготуватись до появи нейтралізації проблеми.

В ролі такого інструментарію може служити система раннього розпізнавання ситуації (СРРС). Вона виступає частиною інформаційної системи організації. Її завданням є виявлення за допомогою сканування та моніторингу слабких сигналів в оточенні організації та фіксування змін і зменшення

«інформаційної дуги». Структурними елементами СРРС виступають: люди, канали зв'язку, комп'ютерні засоби, алгоритми обробки даних і технічно-організаційна інфраструктура. СРРС по суті виконує роль раннього застереження загроз і одночасно сприяє розробці планів та способів, які з успіхом можна використати при формуванні та реалізації нових стратегій розвитку.

Функціонування СРРС пов'язане з покращенням процесу прийняття стратегічних рішень (рис. 2) і спрямоване на пониження рівня невизначеності ситуації за рахунок пониження «інформаційної дуги» (рис. 3).

СРРС замикає в своїх рамках процеси пов'язані з виявленням та ідентифікацією «слабких сигналів», які в майбутньому можуть мати суттєвий вплив на становище та діяльність організації. Необхідність такої системи пов'язана з формуванням у ТОП-менеджменту бачення і відчуття появи у середовищі стратегічних змін. Таке бачення приймає форму сценаріїв майбутнього розвитку. Останні розробляються для трансформації стратегічно важливої інформації в інноваційне відображення майбутнього. Варіанти сценаріїв представляють різні можливі версії розвитку і їх наслідки. СРРС, однак, не є засобом конкретного розв'язку виникаючої несподіваної проблеми, але виступає в ролі механізму, що попереджує при можливості загрози і надає відомості для прийняття обґрунтованих рішень. Здатність СРРС бути основою прийняття стратегічних рішень витікає з такої організації інформаційної технології яка б забезпечила функції:

1) сприйняття;
2) експлуатації;
3) комунікації.

1. Функція сприйняття пов'язана з пошуком відомостей, які б сигналізували про можливу появу загроз в оточенні організації. При цьому ці відомості відображають слабкі сигнали , що напряму не ідентифікують можливих загроз і шансів, що появляються в оточенні. Завдання полягає у їх вчасній ідентифікації, що дасть змогу збільшити час на розуміння суті проблеми і прийняти відповідні рішення.

2. Функція експлуатації пов’язана з діагностикою проблеми появи слабких сигналів, усвідомлення ступеню її стратегічності і бачення її суті. Отриманні відомості обробляються, оцінюються і екстраполюються на наступний період. Мова іде про встановлення причин проблеми, напругу, межі часу і силу впливу на стан організації. Це приводить до розробки сценаріїв, які є основою можливих альтернативних напрямків вирішення проблемних ситуацій.

3. Функція комунікації позволяє доводити до відома заінтересованих осіб сутність виявленої проблеми таким чином, щоб вони могли вчасно зреагувати на загрозу, встановити своє бачення ситуації і прийняти рішення щодо недопущення негативних наслідків.

Сумлінне виконання вказаних трьох функцій має суттєве значення на початковій фазі прийняття рішення і свідчить про значний потенціальний вплив СРРС на прийняття стратегічних рішень. Він проявляється в наступному:

1. Розпізнання проблеми та встановлення цілей. Завдання СРРС організація відбирає слабкі сигнали, які засвідчують при розбіжності між сподіваним перебігом подій і фактичним, за рахунок змін у середовищі, що може привести до неочікуваних негативних наслідків. Слабкі сигнали збуджують відповідних менеджерів до дії. Тим самим СРРС ідентифікує, комуні кує та ініціює процес прийняття рішень.

2. Пошук варіантів розв’язку проблеми. Зідентифіковані слабкі сигнали змушують розробляти альтернативи майбутніх подій, в яких вказувалось би на появу майбутніх загроз. Одночасно потрібно відслідковувати зміни в оточенні організації та отримувати релевантну до можливої проблеми інформацію.

3. Порівняння і оцінка альтернатив і вибір оптимального рішення. СРРС з однієї сторони поставляє інформацію про проблему, яку потрібно негайно вирішувати, а з другої – розробляти сценарії майбутнього, пов’язані зі зміною зовнішнього середовища. А це приводить до зменшення «інформаційної дуги» і прийняття більш обґрунтованого рішення.

4. Імплементація рішення, спостереження і контроль виконання. Послідовне спостереження за змінами середовища, що покладене на СРРС, дозволяє в імітаційному режимі відслідкувати, які з розроблених сценаріїв були найбільш адекватні до реальних ситуацій і якщо прийняті рішення були дочасними, то появляється резерв часу на їх коригування і видозміну майбутніх дій.

Висновок

Висновки і перспективи подальших досліджень. Функціонування і розвиток організації є результатом усвідомленого вибору і раціонального виконання стратегічної програми дій керівництва. Постійно існуюче напруження на лінії «організація – зовнішнє середовище» і виникаючі з цього проблеми не можуть бути вирішені автоматично. Це можливо лише на основі комплексу продуманих і обґрунтованих рішень, які скеровані на виконання прийнятої стратегії та посилення конкурентної позиції. Побудова вдалої конкурентної переваги вимагає повного розуміння проблемної ситуації, що затримуються недобором та звуженням інформаційного поля. Власне створення інформаційної системи і, зокрема системи раннього розпізнавання ситуації на стратегічному рівні допомагає керівництву організації в ідентифікації і оцінці виникаючих загроз, дає змогу ідентифікувати потенційні проблеми та ініціювати процес прийняття відповідних рішень.

Література

1. Аакер Д. Стратегичесное рыночное управление / Д. Аакер: пер. с англ. под. ред. Ю.Н. Каптуревеного. – СПс. – Питер. – 2002. – 554 с.
2. Ансофф И. Стратегическое управление / И. Ансофф; сопр. пер. с англ. – М.: Экономика, 1989. – 519 с.
3. Аакер Д. Стратегическое рыночное управление / Д.Аакер: пер. с англ. Под. Ред. Ю.Н. Каптуревсного. –СПс. Питер. – 2002. – 554 с.
4. Гладун В.П. Планирование решений . – К.: Наукова думка, 1987. – 168 с.
5. Глушков В.М. Введенние в кибернетику. – К.: 1964.
6. Гремилов А.А. Как принять наилучшее решение в реальних условиях. – М.: Радио и свіязь, 1991. – 320 с.
7. Гордон Ян. Целевая конкуренція / Ян Гордон пер. с англ. – М.: Вершина, 2006. – 368 с.
8. Поспелов Д.А. Ситуационное управление. Теория и практики. – М.:Наука, 1986. – 288.

9. Смирнов Э.А. Управленческие решения / Э.А.Смирнов. – М.:ИНФРА-М, 2001.-264 с.
10. Хасса Д. Стратегия и планирование / Д. Хасси; пер. с англ.. – СПб: Питер.2001. – 384 с.
11. Bak J. Controlling asystem woresnego ostrzegania [w:] Nalepka A(red). Organizacja komercyjne i niekomercyjne wobec wzmozonej konkurenji oraz wzrastajacyen Wymagan konsumentow. Wyzsra Srkola Bisnesu/ Tarnow 2002/
12. Griffin R/W/ Podstawy zarzadsania organisacjami. PWN, Warsawa 2004.
13. Hateh M., Teoria organisacji, PWN, Warszawa 2002.

Федоронько Н.І. –
кандидат економічних наук, старший викладач кафедри міжнародних економічних відносин і міжнародної інформації Тернопільського національного економічного університету

ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗЕД ПІДПРИЄМСТВА

Вихід українських підприємств на європейський ринок, з одного боку, значно розширює можливості підприємств щодо збільшення доходів, а з іншого боку – зумовлює виникнення додаткових витрат. Особливе значення має оцінка ефективності зовнішньоекономічної діяльності підприємства в сучасних умовах, коли господарська самостійність і незалежність неминуче мають привести до підвищення відповідальності й обґрунтованості прийнятих управлінських рішень. Економічне обґрунтування прийнятих рішень щодо управління зовнішньоекономічною діяльністю підприємств розробляється із метою підвищення ефективності зовнішньоекономічної діяльності та досягнення стратегічних цілей господарювання.

Питанням оцінки економічної ефективності ЗЕД підприємства займаються ряд вчених: метою методики Дем'яненко А. Г. є визначення впливу окремих факторів на ефективність ЗЕД, що створює можливість кількісної оцінки дії кожного з них [1, с. 23-24]; Миролюбова Т. В. запропонувала таку сукупність показників, як абсолютна ефективність експорту, економічна ефективність реалізації експортних товарів на зовнішньому ринку, ефективність використання виробничих та оборотних фондів при експорті [2, с. 8];

Відкритою залишається проблема вибору доречних критеріїв аналізу ЗЕД, що дозволять окремим підприємствам в залежності від виду, масштабів їх діяльності адекватно оцінити її ефективність та визначити шляхи подальшого розвитку.

Мета дослідження полягає у розвитку методичних засад дослідження та визначення економічної ефективності зовнішньоекономічної діяльності суб'єктів господарювання в умовах інтеграції.

Розрахунок економічної ефективності проводиться шляхом зіставлення досягнутого економічного результату (ефекту) з витратами ресурсів на отримання цього ефекту. Під результатами розуміють грошову, вартісну оцінку отриманого прибутку для підприємства: грошові надходження за відправлену продукцію, виконані роботи та послуги, вартість отриманого товару, робіт, послуг та ін. Під витратами розуміють грошову вартісну оцінку виробничих ресурсів, які залучилися у господарський обіг: вартість сировини, матеріалів, енергії, трудових ресурсів, послуг сторонніх організацій, обов'язкові відрахування в різноманітні державні фонди та інші витрати, без яких торгова угода не може бути здійснена. Економічні результати та витрати ресурсів мають кількісний вимір. А тому й економічна ефективність може вимірюватися кількістю, тобто мати критерій ефективності.

Критерій – це головна ознака, що відрізняє його від інших класифікаційних одиниць. Критерій економічної ефективності не є однаковим для різних рівнів зовнішньоекономічної діяльності. Кожному рівню оцінювання відповідає свій вид економічних інтересів і свій критерій ефективності.

Визначення ефективності зовнішньоекономічних операцій зумовлює ступінь зацікавленості підприємства у виході на світовий ринок, дає змогу обґрунтувати окремі пропозиції щодо закупівлі та продажу певних товарів. Одержані дані можуть бути використані при розробці планів експорту та імпорту підприємства, при оцінюванні структури та напрямків зовнішньоторговельного обігу.

Розрахунок показників економічної ефективності здійснюється за такими принципами [4, с. 32]:

– найповніший облік усіх складових витрат і результатів. Неповний облік витрат та отриманих результатів може спотворити висновки про оцінку ефективності того чи іншого рішення;

– необхідність порівняння з базовим варіантом. За базовий варіант може бути прийнятий стан справ до прийняття рішення. Неправильний вибір бази порівняння може призвести до спотворення оцінок;

– приведення витрат і результатів до однієї бази зіставлення;

– приведення різних за часом витрат і результатів до одного моменту часу;

– наявність достовірності інформації, системи збору та аналізу інформації.

Для загальної характеристики експортної діяльності підприємства використовують такі показники: ефективність експорту, рентабельність експорту, економічний ефект експорту.

1. Ефективність експорту підприємства (Е*еф.е.*) розраховується за формулою:

$$Е_{еф.е.} = Н_{е} : ПВ, \quad (1)$$

де Н*е* – гривневі надходження від експорту, які розраховуються шляхом перерахування валютної виручки в гривні за курсом Національного банку України на день надходження валютної виручки;

ПВ – повні витрати підприємства на експорт, грн.

Показник ефективності експорту свідчить, наскільки ефективно підприємство проводить свою зовнішньоекономічну діяльність. Якщо цей показник буде більшим за одиницю і вищим, ніж показник ефективності реалізації на внутрішньому ринку, тоді реалізація товарів на зовнішньому ринку буде вигіднішою порівняно з реалізацією всередині країни.

2. Рентабельність експорту (Р*е*) розраховується за формулою:

$$Р_{е} = (Н_{е} : С_{е}) \times 100\%, \quad (2)$$

де С*е* – собівартість виробництва експортної продукції, грн.

Цей показник демонструє суму доходу від реалізації експортних товарів, що припадає на кожну витрачену фірмою гривню.

Наведені показники ефективності експорту необхідно порівняти з аналогічними показниками за минулий період, що дасть змогу встановити, як змінилася ефективність реалізації товарів у звітному періоді порівняно з минулим.

3. Економічний ефект експорту (Е*е*) розраховується за формулою:

$$Ее = Не – ПВ. \quad (3)$$

Для визначення економічної ефективності експортної діяльності на рівні підприємства пропонуємо розраховувати три показники економічної ефективності.

1. Показник ($Е_{еф.е.1}$) визначається діленням суми чистої виручки в іноземній валюті за реалізований товар, переведений у гривні за офіційним курсом на день надходження валютної виручки ($ЧВ_е$), на суму повних витрат підприємства на експорт продукції ($ПВ_е$).

$$Ееф.е.1 = ЧВе / ПВе \quad (4)$$

Він демонструє суму гривневого доходу від реалізації експортних товарів, що припадає на кожну витрачену фірмою гривню. Припустимим є його значення, що перевищує 1.

2. Показник ($Е_{еф.е.2}$) свідчить про доходність реалізації продукції на внутрішньому ринку і визначається як співвідношення вартості експорту у внутрішніх цінах ($В_{е.в.ц.}$) та виробничої собівартості експортних товарів ($СВ_е$).

$$Ееф.е.2 = Ве.в.ц. / СВе \quad (5)$$

Експорт відповідних товарів вигідний для підприємства за умови, що $Е_{еф.е.1} > 1$, а також, коли дохідність реалізації експортної продукції на зовнішньому ринку перевищує дохідність реалізації цієї ж продукції на внутрішньому ринку – $Е_{еф.е.1} > Е_{еф.е.2}$.

3. Показник ($Е_{еф.е.3}$) слугує для визначення ефективності використання виробничих фондів під час експорту та розраховується як добуток коефіцієнта експортного чистого прибутку та коефіцієнта оборотності активів.

$$Еф.е.З = \frac{ЧВе - ПВе}{ЧВе} \times 100\% \times \frac{ЧВе}{Ае}, \qquad (6)$$

Цей показник свідчить про рівень ефективності використання активів, причому перша частина формули вказує, який саме відсоток від результатів експорту підприємства становить прибуток від експорту, а друга частина формули визначає, скільки разів за досліджуваний період зміг обернутись авансований на експорт капітал. Таким чином, чим більші обидві частини формули, тим більше значення показника і вигідніший експорт цих товарів.

Крім аналізу ефективності зовнішньоекономічної діяльності на регіональному рівні, необхідним є проведення досліджень й на мікроекономічному рівні. Це зумовлено тим, що з метою оцінки власних потенційних можливостей в конкурентній боротьбі на зовнішньому ринку і розробки заходів підвищення конкурентоспроможності та забезпечення максимального прибутку підприємству експортеру необхідно проводити комплексний економічний аналіз виробничо-господарської діяльності в цілому і зовнішньоекономічної діяльності зокрема.

Оцінку ефективності зовнішньоекономічної діяльності підприємства доцільно проводити на основі таких основних принципів:

- простота і точність розрахункових операцій;
- комплексність та інформативна повнота оцінки;
- взаємозамінність складових алгоритму оцінки.

Алгоритм оцінки ефективності зовнішньоекономічної діяльності підприємства повинен складатися з трьох етапів: підготовчий, розрахунковий етап і аналітичний.

Суть підготовчого етапу полягає у визначенні мети оцінювання, формулювання завдань, організації збору та систематизації інформації.

Дослідження на розрахунковому етапі доцільно проводити за двома напрямами.

1. Аналіз внутрішнього і зовнішнього середовища включає:

– оцінку ефективності ЗЕД підприємства (прибуток від реалізації, приріст обсягу збуту, збільшення частки ринку, коефіцієнт травматизму робітників, динаміка робочих місць, коефіцієнт автоматизації робіт);

– аналіз конкурентоспроможності продукції (розрахунок індексу відносної експортної конкурентоспроможності);

– маркетингове дослідження ринків збуту;

– аналіз діяльності конкурентів;

– оцінка рівня і якості виконання підприємством зобов'язань по контрактах з іноземними партнерами, дослідження ефективності, переваг і недоліків укладання контрактів і договорів.

2. Аналіз показників ефективності зовнішньоекономічної діяльності. Серед найбільш загальних показників ефективності зовнішньоекономічної діяльності підприємства доцільно виділити здатність підприємства досягти поставлену мету та виконувати власну місію в стратегічному вимірі сті, ліквідності.

3. Метою аналітичного етапу є:

– аналіз раціональності використання ресурсів з метою усунення небажаних відхилень від поставлених завдань виробничої програми;

– виявлення внутрішньогосподарських резервів підвищення ефективності зовнішньоекономічної діяльності;

– розробка заходів щодо залучення резервів у господарський обіг;

– контроль за реалізацією заходів.

Головна мета вище зазначеного алгоритму – підвищення ефективності зовнішньоекономічної діяльності суб'єкта господарювання і пошук резервів її зростання.

Систематична оцінка ефективності ЗЕД сприяє її оптимізації і забезпеченню високоприбуткової роботи підприємства. Підвищення ефективності ЗЕД підприємства, в першу чергу його експортних операцій, знаходиться у тісній залежності від удосконалення його загальної системи управління, що спрямовує на подальші наукові дослідження

Список літератури

1. Дем'яненко А. Г. Формирование модели комплексного анализа эффективности внешне-экономической деятельности предприятия / А. Г. Дем'яненко // Економіка, фінан- си, право. – 2005. – № 2. – С. 22-28.

2. Миролюбова Т. В. Совершенствование внешнеэкономической деятельности пред- приятий в условиях рыночной экономики: Автореферат диссертации на соискание уч. ст. канд.. эк. наук / Т. В. Миролюбова. – Екатеринбург, 1992. – 20 с.

3. Зовнішньоекономічна діяльність підприємств: Навчальний посібник / За ред.Ю.Г.Козака, Н.С.Логвінової –К: Освіта України, 2012. – 300с.

4. Зовнішньоекономічна діяльність підприємства: навч. посіб. / за ред. О. В. Шкурупій. – К. : Центр учбової літератури, 2012. – 248 с.

Штангрет А. М.
доктор економічних наук, професор, завідувач кафедри фінансово-економічної безпеки, обліку і оподаткування Української академії друкарства
Караїм М. М.
кандидат економічних наук, асистент кафедри фінансово-економічної безпеки, обліку і оподаткування Української академії друкарства

ОБЛІКОВО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ЯК ІНФОРМАЦІЙНИЙ БАЗИС УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Процес управління вітчизняними підприємствами, ускладнений швидкими і непередбачуваними змінами середовища функціонування, вимагає для прийняття адекватних до ситуації управлінських рішень формування якісного інформаційного підґрунтя. Економічна безпека підприємства, яка є важливою умовою існування, функціонування та розвитку кожного суб'єкта господарювання, потребує для цілей управління також інформаційної основи – обліково-аналітичного забезпечення.

Обліково-аналітичне забезпечення управління економічною безпекою підприємства повинно уможливлювати отримання достовірної, своєчасної та повної інформації з різних джерел про зміни у зовнішньому та внутрішньому середовищі, які б вказували на виникнення чи зростання впливу чинників на рівень безпеки, що вимагає подальшого наукового пошуку та

розроблення методичних засад, що відповідають умовам функціонування в національній економіці.

В умовах кризи світової й вітчизняної економік, коли підприємствам доводиться зіштовхуватись з перманентними загрозами й ризиками, які суттєво знижують поточний рівень їх економічної безпеки, проблема створення системи захисту, тобто комплексної системи економічної безпеки стала першочерговою. Потрібно визнати, що за таких обставин практично на всіх підприємствах України в ініціативному порядку були створені системи безпеки, які дозволяють їм з різним ступенем ефективності забезпечувати безпеку своєї діяльності. Зазначене пояснюється тим фактом, що головні зусилля українських підприємств спрямовані перш за все на забезпечення захисту території, виробничих і адміністративних об'єктів, засобів виробництва, сировини, готової продукції й транспортних засобів від противоправних зазіхань як зі сторони кримінальних угрупувань, так і в наслідок злочинних дій несумлінного персоналу. З однієї сторони функціонування такої системи дозволяє знизити ймовірність виникнення частини з можливих загроз, з іншої – потрібно взяти до уваги, що в сучасних умовах суттєво змінилася кількість та перелік ключових ризиків та загроз. Злочини в економічній сфері стали носити інтелектуальний характер, а їх сферами стали фінансова діяльність, політика й стратегія підприємства, механізми керування бізнесом, інформаційна сфера, право, інноваційна діяльність, техніка й технології й т. д. У злочинних схемах нерідко ключову роль відіграють корумповані чиновники й представники закордонних фірм, а відтак існуюча система безпеки не дозволяє забезпечувати надійний захист підприємств від сучасних загроз і ризиків. За таких умов для побудови й ефективного функціонування системи економічної безпеки необхідно задіяти в повному обсязі ресурси всіх структурних підрозділів підприємства, а також можливості зовнішніх організацій, у тому числі органів державної влади й управління, суб'єктів недержавної системи безпеки й т. д.

Важливим та необхідним етапом удосконалення управління економічною безпекою підприємства на більшості вітчизняних підприємств є дослідження, аналіз і коригування зовнішніх та

внутрішніх інформаційних потоків, які формують інформаційний базис для прийняття управлінських рішень.

З точки зору забезпечення безпеки, доцільно погодитися із визначенням інформації, яке пропонує М. Пушкар, згідно якого під цим терміном доцільно розуміти субстрат, необхідний і обов'язковий для того, щоб оцінити ситуацію, виробити можливі альтернативи управлінських рішень та відібрати найдоцільнішу з них для практичного використання [5, с. 54].

У відповідності до процитованого вище визначення, можна стверджувати, що інформація як сукупність даних про стан та зміну внутрішнього та зовнішнього середовища в системі економічної безпеки підприємства використовується для дослідження, оцінки і аналізу економічних явищ і процесів з метою розроблення й прийняття управлінських рішень для забезпечення необхідного для існування та розвитку рівня безпеки. Управління економічною безпекою підприємства – це неперервний процес (від заснування до ліквідації підприємства) моніторингу середовища функціонування з метою виявлення впливу усіх чинників на рівень безпеки як основа для розроблення, реалізації та контролю кожного управлінського рішення в межах підприємства.

Погляди вчених щодо формування інформаційного базису управління економічною безпекою підприємства суттєво різняться, в першу чергу терміном який можна взяти за основу. Так поширеними є поняття: «обліково-аналітичне забезпечення», «обліково-аналітична система», «обліково-інформаційне забезпечення», «інформаційне забезпечення».

Обліково-аналітичне забезпечення розглядається в наукових працях таких вчених як А. Загородній, О. Кравченко, Т. Камінська, Н. Голячук, В. Волощук. Для прикладу, А. Загородній дає визначення цьому терміну як форми організації всіх видів обліку й аналізу, метою якого є забезпечення менеджерів підприємства інформацією для прийняття поточних і стратегічних управлінських рішень та контролю за їхньою реалізацією [4, с. 31].

Обліково-аналітичну систему розглядають Я. Соколов, Е. Негашев, С. Барановська, Л. Усатова, О. Гудзинський, Г. Кірейцев, Т. Пахомова, Л. Попова, Б. Маслов, І. Маслова. Так,

С. Барановська визначає обліково-аналітичну систему як таку, що ґрунтується на даних оперативного, статистичного, фінансового і управлінського обліку, включаючи оперативні дані, і використовує для економічного аналізу статистичну, виробничу, довідкову та інші види інформації [1, с. 9].

Р. Бруханський приділяє увагу обліково-інформаційному забезпеченню, яке у його трактуванні повинно враховувати як внутрішні, так і зовнішні інформаційні сфери, відображаючи комплексну консолідовану інформацію про діяльність підприємства і його перспективи. Основними джерелами обліково-інформаційного забезпечення є фінансовий облік і звітність; управлінський облік і звітність; результати моніторингу бізнес-середовища [3, с. 32;33].

І. Бланк, В. Смирнова, А. Апостолов та М. Крамчанінова наголошують на важливості інформаційного забезпечення в управлінні системою економічної безпеки підприємства. І. Бланк визначає інформаційне забезпечення як процес безперервного цілеспрямованого підбору відповідних інформативних показників, необхідних для здійснення аналізу, планування і підготовки ефективних оперативних управлінських рішень по всіх аспектах фінансової діяльності підприємства [2].

На нашу думку, серед названих основних термінів, стосовно процесу гарантування економічної безпеки підприємства доцільно застосувати «обліково-аналітичне забезпечення». Попри те, що обліково-аналітичне забезпечення наявне на кожному підприємстві, але доволі часто його рівень не є достатнім для ефективного виконання завдань в системі економічної безпеки підприємства. Узагальнюючи напрацювання науковців [1-7] нами розроблено теоретичні засади формування обліково-аналітичного забезпечення на підприємстві (див. рис.).

Обліково-аналітичне забезпечення – це процес підготовки обліково-аналітичної інформації, який можна розділити на кілька ключових етапів:

– збір, реєстрація та узагальнення даних;
– перевірка інформації для забезпечення необхідної якості;
– аналітичне опрацювання;
– збереження та передача інформації;
– формування інформаційного базису для розроблення рішень.

Обліково-аналітичне забезпечення

якісне інформаційне обслуговування суб'єктів безпеки шляхом створення динамічної системи збору своєчасних, якісних, в необхідному обсязі і актуальних даних у зовнішньому та внутрішньому середовищі, їх узагальнення, систематизація, аналіз та перевірка на достовірність, зберігання та ефективне використання для прийняття відповідних управлінських рішень.

Мета

поєднання облікових та аналітичних процедур для формування інформації з такими характеристиками:

- ***поточної***, для визначення рівня економічної безпеки на певний момент часу;
- ***аналітичної***, для створення інформаційного підґрунтя прийняття управлінського рішення
- ***стратегічної***, для розроблення планів та прогнозів можливої зміни рівня безпеки

Базові засади формування:

- визначення основних та додаткових джерел інформації, які дозволяють чітко відстежувати найменші зміни у зовнішньому та внутрішньому середовищі та можуть бути використані для ідентифікації моменту виникнення та розвитку загроз та ризиків;
- розроблення критерії оцінки якості інформації, яка використовується в управлінні економічною безпекою підприємства;
- розроблення методики формування необхідного обсягу даних у системі обліку та послідовність подальшої трансформації облікованих даних в аналітичну інформацію;
- розроблення методики перевірки інформації з облікових даних та додаткових джерел.

Вимоги до формування:

- чітко та достовірно відображати всі господарські операції, що здійснюються на підприємстві;
- надавати інформацію щодо зміни зовнішнього середовища, які суттєво впливають або можуть в перспективі вплинути на рівень економічної безпеки підприємства;
- виявляти та відстежувати вплив окремих внутрішніх та зовнішніх чинників на рівень економічної безпеки підприємства;
- забезпечувати інформаційний супровід розроблення та прийняття рішень в управлінні економічною безпекою підприємства;
- забезпечувати незалежний контроль за функціонуванням усіх підрозділів підприємства;
- формувати інформаційний базис для складання планів та прогнозів розвитку підприємства.

Принципи функціонування системи обліково-аналітичного забезпечення:

- якість інформації забезпечується узагальненням даних з різних джерел та компетентністю працівників підрозділу безпеки під час аналізу та контролю;
- обсяг інформації повинен відповідати потребам суб'єктів безпеки;
- оперативність інформації визначає можливість прийняття превентивних захисних заходів та ефективність мінімізації втрат від зростання небезпеки;
- зменшення витрат на обліково-аналітичне забезпечення в управління економічною безпекою підприємства можливе через взаємодію підрозділу безпеки з іншими структурними одиницями.

Рис. Теоретичні засади формування обліково-аналітичного забезпечення на підприємстві

Обліково-аналітичне забезпечення будучи складовою системи управління економічною безпекою підприємства спирається на чітке об'єднання облікових та аналітичних операцій.

Основою обліково-аналітичного забезпечення є дані оперативного, статистичного, фінансового і управлінського обліку, а також виробнича, комерційна, фінансова, довідкова та інші види інформації щодо стану та зміни внутрішнього та зовнішнього середовища. Джерелами інформації є усі доступні засоби масової комунікації, зокрема періодичні видання, телебачення, Інтернет, а також інформація отримана шляхом конкурентної розвідки.

Поєднання облікової та іншої інформації повинно забезпечити як високу якість, так і контроль, відтак і підвищити ефективність реалізації управлінських рішень.

Постійні непередбачувані зміни зовнішнього середовища, необхідність посилення контролю за внутрішніми процесами підвищують вимоги до обліково-аналітичного забезпечення управління економічною безпекою, зокрема через поглиблення взаємозв'язків із іншими інформаційними системами управління підприємством. Часткове вирішення цієї проблеми забезпечується швидким зростанням можливостей і покращенням техніко-технологічних характеристик сучасних засобів обробки інформації та програмного забезпечення для збору, обробки і передавання значних обсягів даних. Водночас актуальною є проблема не лише отримання та передачі необхідної інформації, але і обмеженні тієї частини, яка в сфері безпеки називається «інформаційним шумом». Надлишкова, неякісна, несвоєчасна та недостовірна інформація не лише перевантажує інформаційні канали, вимагає додаткових витрат на її перевірку та опрацювання, але й збільшує ризик прийняття помилкових рішень. Безперечно, що один із базових принципів забезпечення безпеки на будь-якому рівні та сфері передбачає обов'язкове використання інформації з різних джерел та її перевірку на достовірність. Відтак не машинне опрацювання бази даних, а лише компетентність працівників підрозділу безпеки дозволяє із сукупності даних виділяти ті, які повинні

стати інформаційним базисом розроблення та прийняття управлінських рішень.

Узагальнена та перевірена інформація підлягає аналізу шляхом застосування аналітичних і економіко-математичних методів для дослідження динаміки, структури, взаємозв'язку між явищами та процесами, що визначають рівень безпеки.

Результатом функціонування обліково-аналітичного забезпечення повинні бути звіти, документи, довідки та вихідна інформація, що є основою для прийняття рішень і контролю за виконанням поставлених завдань.

Висновок. Узагальнюючи, доцільно ще раз підкреслити, що управління економічною безпекою підприємства вимагає якісного інформаційного забезпечення, формування якого вимагає застосування відповідного методичного забезпечення. Сьогодні в науковій літературі присутні суттєві відмінні точки зору щодо суті та процесу збору, обробки, аналізу інформації, що не сприяє вирішенню проблеми гарантування економічної безпеки вітчизняних підприємств.

Розроблені методичні засади визначають базові засади й вимоги формування та принципи функціонування системи обліково-аналітичного забезпечення, покликані сприяти вирішенню життєво важливої проблеми для вітчизняних підприємств – гарантування необхідних безпечних умов розвитку.

Подальшого дослідження потребує проблема ідентифікації моменту виникнення та розвитку внутрішніх та зовнішніх загроз шляхом застосування економіко-математичних методів.

Список літератури

1. Барановська С. П. Обліково-аналітичне забезпечення як невід'ємна складова управління підприємством / С. П. Барановська // Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку : [збірник наукових праць] / відповідальний редактор О. Є. Кузьмін. – Львів : Видавництво Львівської політехніки, 2012. – С. 8-11.

2. Бланк И.А. Энциклопедия финансового менеджера: в 4 т. Т. 1. Концептуальные основы финансового менеджмента / Бланк И. А. – 2-е изд., стереотип. – М. : Омега-Л, 2008. – 447 с.

3. Бруханський Р.Ф. Модернізація обліково-інформаційного забезпечення стратегічного менеджменту сільськогосподарських підприємств / Р. Ф. Бруханський // матеріали колективної монографії у 2 т. / за ред.

П. Й. Атамас [Сучасний бухгалтерський облік, аналіз і аудит: галузевий аспект, 1 т.]. – Дніпропетровськ: «Герда», 2013. – С. 21- 34.

4. Загородній А. Г. Оцінювання ефективності системи обліково-аналітичного забезпечення менеджменту підприємства / А. Г. Загородній // Матеріали міжнародної науково-практичної конференції [Стан і перспективи розвитку обліково-інформаційної системи в Україні], (Тернопіль, 23-24 квітня 2010р.) / М-во освіти і науки України, ТНЕУ. – Т.: Крок, 2010. – С. 31-32.

5. Пушкар М.С. Креативний облік (створення інформації для менеджерів): Монографія. – Тернопіль, Карт-бланш, 2006. – 334 с.

6. Теоретико-методичні засади формування організаційного забезпечення управління економічною безпекою машинобудівного підприємства : моногр. / О. В. Халіна, А. М. Штангрет, Л. Є. Сухомлин, О. В. Мельников ; за заг. ред. А. М. Штангрета. – Львів : Укр. акад. друкарства, 2016. – 220 с.

7. Фінансова безпека машинобудівного підприємства : Методичні засади формування та забезпечення : моногр. Х. О. Мандзіновська, А. М. Штангрет, Я. В. Котляревський, О. В. Мельников ; за заг. ред. А. М. Штангрета. – Львів : Укр. акад. друкарства, 2016. – 226 с.

Prof. Uwr Dr Hab. Anna Ćwiąkała - Małys
Dr Monika Mościbrodzka
Uniwersytet Wrocławski
Wydział Prawa, Administracji i Ekonomii
Instytut Nauk Ekonomicznych

INDEKS PRODUKTYWNOŚCI MALMQUISTA – NARZĘDZIEM W BADANIU ZMIAN EFEKTYWNOŚCI FINANSOWEJ – ZARYS METODY

W warunkach gospodarki rynkowej znaczącą rolę pełni analiza efektywności wykorzystania pozostających w dyspozycji jednostki zasobów. Kierowanie się efektywnością w ujęciu finansowym, rozumianą przez relację wygenerowanych wyników do poniesionych nakładów, jako kryterium podejmowania decyzji jest akceptowaną zasadą, która warunkuje przetrwanie i rozwój jednostki, ale tez maksymalizację korzyści. [i] Efektywność można określać w ujęciu ex post i ex ante. Obliczając efektywność ex ante-szacuje się oczekiwane wyniki przy zaangażowaniu konkretnych nakładów, zaś efektywność ex post- dotyczy określenia wyników konkretnych działań, które podejmuje jednostka w danym czasie.

Badanie efektywności finansowej jest zasadne nie tylko w stosunku do jednostek komercyjnych, dla których wygenerowanie zysku jest podstawowym celem działania, ale też do jednostek publicznych . Znaczącym wyznacznikiem efektywności finansowej jest racjonalne czyli efektywne wykorzystanie przez te jednostki zasobów. Uczelnie publiczne działają w dość specyficznych warunkach gospodarczych ale na rynku usług edukacyjnych. Z jednej strony otrzymują środki publiczne na realizację zadań w zakresie kształcenia i badań naukowych , z drugiej zaś zobligowane są do racjonalnego ich wykorzystania a niejednokrotnie nawet pomnażania.

Kierownictwo uczelni, jak i MNiSW powinno kierować się w procesie zarządzania informacją o pomiarze efektywności wykorzystania zasobów.

Rozwiązanie tego problemu nie jest łatwe , ponieważ są to obszary (kształcenie, nauka) , na które ponosi się wydatki, choć w zasadzie nie są podatne na stosowanie narzędzi pomiaru ich efektów. Zauważyć należy ,że nie jest łatwo ustalić zależności pomiędzy rozmiarami poniesionych wydatków a osiągniętymi wynikami , gdyż te ostatnie są dość często trudno mierzalne i pojawiają się z dość dużym opóźnieniem.

Typowe analizy wskaźnikowe nie rozwiązują tego problemu. Dzieje się tak dlatego , iż nie ma możliwości ustalenia jak duży nakład danego rodzaju został bezpośrednio wykorzystany w celu pozyskania danego efektu lub efektów. W praktyce takie obliczenia opierają się na bardzo szczegółowym materiału, którego zorganizowanie jest bardzo kłopotliwe.

Dlatego zasadne jest stosowanie metody Dea która wykorzystuje wielowymiarowe układy danych zarówno po stronie nakładów , jak i efektów. Zastosowanie takich programów jak EMS, Win4DEAP umożliwia rozwiązywanie zagadnień programowania liniowego dla każdej analizowanej jednostki , zwłaszcza gdy próba danych jest duża. Pomiar efektywności metodą DEA daje odpowiedź na pytania:

– o ile można zredukować nakłady, aby osiągnąć dotychczasowy poziom wyników,

– jakie można wygenerować wyniki, jeśli nakłady, którymi uczelnia dysponuje , wykorzystywałaby tak jak uczelnie uznane za efektywne

Pomiar efektywności finansowej można przeprowadzić dla danego okresu ale w teorii i praktyce znaczącym problemem jest porównanie zmian efektywności w czasie. W tym celu znajduje zastosowanie indeks produktywności Malmquista[ii].

Indeks produktywności Malmquista został zgłoszony jako indeks teoretyczny przez Caves'a, Christensen'a i Diewert'a[iii] oraz rozpropagowany jako indeks empiryczny przez R. Färe'a, S. Grosskopf'a, B. Lindgren'a, P. Roos'a[iv] . Nazwano go nazwiskiem szwedzkiego statystyka Stena Malmquista, który w 1953 roku w artykule pt. Index Numbers and Indifference Surfaces wprowadził indeks artykułów powszechnego użytku jako stosunek funkcji odległości. Znalazł zastosowanie w porównaniu osiąganej przez dana jednostkę relacji nakłady do wyników w dwóch różnych okresach. Zaletą indeksu Malmquista jest to, że interpretacja jego wartości jest stosunkowo prosta i nie wymaga znajomości poziomu cen oraz , że daje możliwość określenia, które czynniki wpływają na produktywność i ich zmiany[v]. Uzyskane obliczenia przy jego wykorzystaniu mogą stają się podstawą do analizy w trendzie czasowym zmian efektywności finansowej.

Iryna Shchyrba -
PhD, Assoc. Prof.
Tarnopolski Narodowy Uniwersytet Ekonomiczny

ZASTOSOWANIE METOD ANALITYCZNYCH W AUDYCIE SPRAWOZDANIA FINANSOWEGO

Najważniejszą funkcją audytora jest potwierdzenie o stosunkowo zadowalające funkcjonowanie ekonomicznych subiektów. Wykonanie tej funkcji bazuje się na wynikach sprawdzenia i zdolności audytora do fachowych myśli. Wniosek, fachowy osąd audytora wyznacza się jak punkt widzenia audytora, który jest założony na jego wiedzach, kwalifikacji i doświadczeniu pracy, co służy podstawą dla podjęcia subiektywnych decyzji w

okolicznościach, kiedy jednoznacznie i szorstko wyznaczyć tryb jego działań nie nadarza możliwym, ponieważ subiektywność aprobują się decyzji podczas audytorskiego sprawdzenia najpierw przypuszcza szerokie użycie analitycznych zdolności biegłego rewidenta.

Zwiększenie roli analitycznych metod w audycie wyznacza się również stosowaniem w audytorskiej działalności takich pojęć, jak ryzyko, istotność, wybieranie.

Według wyników badania, uważamy, że koniecznie wydzielić analityczne metody do poszczególnej grupy w ogóle ogólnej metod audytu. Niedocenienie doniosłości i znaczności analitycznych metod może doprowadzić do niebezpieczeństwa formalnego podejścia w audytorskiej pracy. To niebezpieczeństwo powstaje dlatego, że droga formalnej kontroli – droga najmniejszego oporu. Przecież łatwiej sprawdzić wygenerowane koszty albo dokonaną operację z punktu widzenia wymogów prawa, aniżeli przeanalizować jej finansową efektywność i celowość, wypowiedziawszy swoją opinię.

W zależności od rodzaju analitycznych procedur i etapu ich użycia audytor wykorzystuje różne metodyczne przyjęcia finansowej analizy. Finansowa analiza – to sposób gromadzenia, transformacji i użycia informacji finansowego charakteru w celu oceny finansowego stanu, prognozowania położenia przedsiębiorstwa na rynku kapitału, oceny możliwości mobilizacji źródeł kosztów i tym podobne. Zadania finansowej analizy zależą od celi użytkowników finansowej informacji.

Narzędziowy finansowej analizy, podobny do ekonomicznej analizy, jest bardzo duży. Lecz nie całe metody finansowej analizy mogą w równej mierze wykorzystywać się przy przeprowadzeniu audytu. Większość z ich jest ciężka i powodują straty, co nie sprzyja podwyższeniu efektywności audytu. Znaczna część metod ekonomicznej analizy, które mogą wykorzystywać się w audycie (metody matematycznej statystyki, matematycznego programowania, przyjęcia analizy stochastycznej) wymagają użycia komputerowych programów, co pozwala oszczędzać czas na przeprowadzenie analizy i obróbkę wyników. Toż koniecznie wyznaczyć te metody, które pozwalają przy znikomych kosztach czasu otrzymywać wierzytelne i dostateczne audytorskie dowody.

Naszym zdaniem do takich metod można odnieść następne:

1. Tradycyjne:

1.1. Porównanie – analiza współzależności zjawisk, wskaźników. Rozróżniają: porównanie z zeszłym okresem; porównanie z średnimi danymi; porównanie z innymi zjawiskami, wskaźnikami.

1.2. Ugrupowanie – klasyfikacja zjawisk za pewną oznaką, z uwzględnieniem przyczyn i czynników, które ich warunkują. Wykorzystują: strukturalne ugrupowania – dla badania struktury obiektu; typologie ugrupowania – dla badania jednorodnych zjawisk, wskaźników albo obiektów; analityczne ugrupowania, które ogarniają i strukturalne i typologie i wykorzystują się dla wyznaczenia związków wzajemnych między zjawiskami, obiektami, wskaźnikami.

1.3. Bilansowa metoda – bada zależność między oddzielnymi wskaźnikami za pomocą bilansowego równania.

1.4. Graficzna metoda – za pomocą grafików pozwala otrzymać model związków wzajemnych między zjawiskami albo wskaźnikami.

1.5. Metoda i względnych średnich.

2. Przyjęcia zdeterminowanej czynnika analizy :

2.1. Metoda różnic wykorzystuje się dla oceny wpływu czynników na efektywny wskaźnik.

2.2. Metoda łańcuchowych podstawień również wykorzystuje się dla rozliczenia wpływu oddzielnych czynników na integralny wskaźnik.

2.3. Integralna metoda – najbardziej dokładna metoda dla oceny wpływu czynników na efektywny wskaźnik.

2.4. Indeksowa metoda bazuje się na względnych wskaźnikach, które wyrażają stosunek poziomu danego zjawiska do poziomu jego w przeszłości albo do poziomu analogicznego zjawiska.

Oprócz tego, dosyć efektywne są metody ekonomiczne i matematyczne, na przykład, matematyczne modelarstwo [1; 4]. Metody elementarnej matematyki wykorzystują się przy dowolnej analitycznej procedurze.

Wybór metod analizy zależy od fachowego osądu audytora, lecz można ustalić pewną zależność wychodząc z możliwości stosowania tej czy innej metody, od celu i zadań audytu, czyli od

rodzaju analitycznych procedur. Naszym zdaniem, jej użycie pozwoli planować audytorskie sprawdzenie wychodząc z posiadania audytorem naprowadzanymi przyjęciami analizy.

Następne badania są skierowane na wyznaczenie metodologicznych zasad stosowania analitycznych procedur i praktycznych narzędziowych każdego etapu analizy finansowej sprawozdawczości.

Według wyników przeprowadzonych badań i przeglądu specjalnej literatury, wyznaczyliśmy cztery główne kierunki analizy w audycie:

- Analiza działalności przedsiębiorstwa.
- Analiza wskaźników finansowej sprawozdawczości.
- Analiza możliwości upadłości klienta.
- Analiza prognozującej i perspektywnej informacji.

Analiza działalności przedsiębiorstwa przeprowadza się na poprzednim etapie audytu w celu otrzymania pojęcia o biznesie klienta. W granicach tej analizy częściowo wykorzystują się analiza wskaźników finansowej sprawozdawczości zeszłych lat i pośredniej finansowej sprawozdawczości za okres, co sprawdza się.

Analiza działalności przedsiębiorstwa jest spokrewniona z analizą finansowego stanu, która z kolei jest jedna z aspektów analizy finansowej sprawozdawczości. Toż analizę działalności przedsiębiorstwa będziemy rozpatrywać przez pryzmat analizy finansowego stanu. Analiza finansowego stanu bazuje się na użyciu informacji z finansowej sprawozdawczości, a mianowicie bilansowi i sprawozdaniu o finansowych wynikach. Lecz analiza finansowej sprawozdawczości przy badaniu działalności przedsiębiorstwa dla planowania audytu bazuje się na studiowaniu biznesu klienta, wyznaczeniu jego organizacyjnej struktury. Więc oprócz finansowej sprawozdawczości za zeszłe okresy audytor powinien wykorzystywać inne źródła informacji : publikacje, statystyczne dane, statutowe dokumenty i in.

Więc za swoją treścią analityczne procedury, które przeprowadzają się na etapie planowania audytu i zapoznania się z biznesem klienta, można związać z ekspres-analiząfinansowego stanu, który włącza ocenę finansowego położenia i dynamiki rozwoju przedsiębiorstwa.

Badanie pozwoliło wydzielić cztery etapy ekspres-analizy w odpowiedniości w celu jego i zadaniami:

– Przygotowawczy etap – zapoznanie się z warunkami działalności przedsiębiorstwa, jego strukturą, wynikami poprzedniego audytu, ewidencyjną polityką (dla rozumienia metod oceny aktywów, zobowiązań, dochodów i kosztów), z statutowymi dokumentami (dla otrzymania informacji o kształtowaniu kapitału statutowego;

– Poprzedni przegląd finansowej sprawozdawczości – wyznaczenie informacji, która jest ciekawa z punktu widzenia analityka.

– Czytanie i analiza sprawozdawczości – rozliczenie analitycznych wskaźników i współczynników dla otrzymania ogólnej prowizorycznej oceny finansowego stanu przedsiębiorstwa.

– Sporządzenia sprawozdania po wynikom analizy.

Analiza finansowej sprawozdawczości przeprowadza się na trzecim etapie. Pod nim rozumieją ujawnienie związków wzajemnych między rozmaitymi wskaźnikami finansowej sprawozdawczości o finansowo-gospodarczej działalności przedsiębiorstwa. On włącza:

– Pozioma analiza – porównanie wskaźników finansowej sprawozdawczości za kilka okresów, wyznaczeń objętości i kierunku przemiany, wyznaczenia tendencji. Jednym z wariantów poziomej analizy jest budowa trendów.

– Pionowa analiza – wyznaczenie udzielnej wagi oddzielnych artykułów sprawozdawczości i ich zestawienia.

– Analiza współczynników – rozliczenie współzależności między oddzielnymi wskaźnikami sprawozdawczości na podstawie istniejących między nimi związków.

– Opracowanie prognoz.

W światowej praktyce analizy jest opracowana znaczna ilość wskaźników, które charakteryzują finansowy stan przedsiębiorstwa. Jednak na dzisiaj stopniowo odbywa się odejście od użycia współczynników dla diagnostyki finansowego stanu. To uwarunkowano ich statycznym, wskutek czego znaczne przemiany w działalności przedsiębiorstwa zostają bez uwaga analityka.

Gruntowne badania z tego problemu były przeprowadzone przez autorów [1; 2; 5; 6]. Jednak na etapie ekspres-analizy rozliczenie współczynników jest najbardziej możliwe do przyjęcia, ponieważ pozwala wyznaczyć problemy w działalności przedsiębiorstwa i skupić uwagę audytora na niezwykłych albo negatywnych tendencjach. Jesteśmy nie zgodne z myślą o tym, że na dzisiaj lista współczynników znajduje się w fazie kształtowania. Naszym zdaniem, nie może być jedynej listy takich współczynników, jak nie może być jednakowych gospodarek, przecież współczynniki charakteryzują rozwój przedsiębiorstwa w warunkach pewnej gospodarki. Istnieją różne podejścia do wyznaczenia ilości współczynników, lecz na ogół oni są podobne między sobą.

Opracowanie prognoz jest jedno z bardzo ciężkich etapów analizy finansowego stanu dla audytora. Na etapie planowania audytor musi ocenić dane finansowej sprawozdawczości za zeszły okres, pośrednią finansową sprawozdawczość, przeanalizować ewidencyjną politykę, która wykorzystuje się na przedsiębiorstwie i za pomocą metodycznych przyjęć ekonomicznej analizy złożyć prognozującą finansową sprawozdawczość wychodząc z ujawnionych tendencji działalności przedsiębiorstwa. Jednym z możliwych sposobów montażu takiej sprawozdawczości jest użycie metody odsetka od obrotu towarowego.

Podsumowując, tryb użycia analitycznych procedur na etapie planowania i prowizorycznej oceny działalności przedsiębiorstwa, naszym zdaniem, można przedstawić następnie: Zdobywanie informacji o działalności przedsiębiorstwa; Zapoznanie się z ewidencyjną polityką i statutowymi dokumentami. Przegląd finansowej sprawozdawczości zeszłych okresów i pośredniej finansowej sprawozdawczości. Wyznaczenia artykułów, które ciekawią audytora (artykuły strat, zaległego zadłużenia i tym podobne). Montaż analitycznych tablic; Na zapleczu pośredniej finansowej sprawozdawczości za pomocą trendów złożyć przybliżoną finansową sprawozdawczość za okres, co sprawdza się; Przeprowadzić pionową analizę pośredniej finansowej sprawozdawczości za potoczny rok, wyznaczyć przemiany w strukturze aktywów i pasywów przedsiębiorstwa; Przeprowadzić poziomą analizę finansowej sprawozdawczości za potoczny rok i

wyznaczyć przemiany po pozycjach; Na podstawie pionowej i poziomej analizy wyznaczyć znaczące artykuły sprawozdawczości (bilansowi i sprawozdaniu o finansowych wynikach); Obliczyć współczynniki na podstawie sprawozdawczości za zeszły okres i za okres, co sprawdza się. Porównać ich między sobą i wyznaczyć tendencje odchyleń; Jeśli są statystyczne dane, przeprowadzić porównanie między działalnością klienta i innych przedsiębiorstw danej branży, rozpatrując jak absolutne, tak i względne wskaźniki działalności; Wyciągnąć wnioski według wyników analizy i wyznaczyć główne kierunki audytu.

Analiza możliwości bankructwa przeprowadza się w granicach analizy zdolności przedsiębiorstwa dotrzymywać się zasady ciągłości działalności, jego metodykę rozpatrzymy w następnym pytaniu.

Analiza prognozującej i perspektywnej informacji może przeprowadzać się jak oddzielna usługa audytora, a także częściowo przy montażu prognoz na przestrzeni audytu i w zasadzie - na końcowej fazie, przy ocenie dalszych wypadków.

Więc rozpatrzymy użycie analitycznych procedur w trakcie audytu.

Przy przeprowadzeniu testowania, audytor wykorzystuje finansowe i niefinansowe dane, toż wybór metod i budowa procedury analizy zależy od każdego szczególnego wypadku. Można wyznaczyć, które możliwe warianty użycia analitycznych procedur spotykają się w praktyce. Przeprowadzona analiza pozwoliła nam wydzielić najbardziej popularne:

– Wyznaczenie możliwych rozmiarów odliczeń do budżetu: po VAT, innych podatkach i zebraniach.

– Rozliczenie pozostałości zapasów na koniec okresu, albo koszty własne zrealizowanych towarów.

– Rozliczenie możliwego utargu od realizacji produkcji.

– Rozliczenie dochodu albo kosztów od produkcji pewnego rodzaju produkcji albo nadania usług.

Oprócz tego, istnieją specyficzne wypadki użycia analitycznych procedur – przy skonsolidowanej finansowej sprawozdawczości i przy sprawdzeniu sprawozdawczości segmentów : filii firmy, filii.

Co dotyczy trybu przeprowadzenia analizy podczas testowania, to on składa się z:

– przedstawienia celu – wybór końcowego wyniku, który powinien być otrzymany;

– wyznaczenie zależności między wskaźnikami, które formują końcowy wynik;

– rozliczeniu końcowego wyniku (prognozie);

– porównanie zdobytego wyniku z ewidencyjnym i wyznaczenia odchyleń;

– szacunki odchyleń.

Rozliczenie końcowego wyniku, czyli realizacja analitycznej procedury odbywa się przez budowę prognozującego modelu na podstawie prezentowanych przez klienta albo otrzymanych podczas sprawdzenia danych. Czyli na podstawie liczebnej, pieniężnej, finansowej i niefinansowej informacji za pomocą sformalizowanych i logicznych metod finansowej analizy prognozuje się (rozlicza się) wynik tej czy innej operacji, salda rachunku i tym podobne. Potem on porównuje się z odzwierciedlonym w ewidencji i sprawozdawczości wynikiem. Na przykład, jednym z najrozpowszechnionych podejści do audytu finansowej sprawozdawczości w praktyce «Dużej czwórki» audytorskich firm jest montaż sprawdzającego bilansu na podstawie analitycznych procedur, po którym po artykułom ze znacznym odchyleniem od danych bilansu przedsiębiorstwa przeprowadzają się testy detaliczne.

Przy ocenie odchyleń między prognozującą i faktyczną informacją, koniecznie orientować się na kryterium istotność, ustalona po konkretnym saldzie rachunku albo klasy operacji. Jeśli odchylenie znajduje się w granicach istotności, ono ocenia się powtórnie w ogóle z innymi nieistotnymi odchyleniami dla wyznaczenia ogólnego odchylenia od ogólnej istotności. Jeśli odchylenie jest znaczące, koniecznie ustalić jego przyczyny i wyznaczyć ewentualne skutki. Jeśli odchylenie nieistotne koniecznie otrzymać pewność w tym, że otrzymane dane są wierzytelne (za pomocą alternatywnych procedur albo porównać do dowodów, otrzymanymi z innych źródeł) i ocenić ich wystarczanie (z punktu widzenia rozmiaru audytorskiego ryzyka w odpowiedniości z Programem audytu).

Teraz rozpatrzymy analityczne procedury, które wykorzystują się na końcowym etapie audytu, przed montażem audytorskiego wniosku. Analiza na danym etapie przeprowadza się przez analogię z ekspres-analizą, lecz analiza finansowej sprawozdawczości stoi już na pierwszym miejscu. Za swoją objętością, źródłami informacji i wynikami analiza finansowej sprawozdawczości na danym etapie przybliża się do detalizowanej analizy finansowego stanu. Detalizowana analiza nadaje bardziej dokładną charakterystykę majątkowego i finansowego położenia, rozwoju działalności i możliwości rozwoju przedsiębiorstwa na perspektywę. On konkretyzuje i uzupełnia dane ekspres-analizy i składa się 4 etapów:

Pierwszy etap. Budowa analitycznych tablic na podstawie finansowej sprawozdawczości (analiza wstępna).

Drugi etap. Analiza stanu finansowego, w granicach której przeprowadzają :

- Analiza płynności.
- Ocenę finansowej trwałości.

Trzeci etap. Ocena i analiza efektywności finansowo-gospodarczej działalności. On włącza:

- Analiza sprawności.
- Analiza rentowności (dochodowości).

Czwarty etap. Opracowanie środków po poprawie finansowo-gospodarczej działalności.

Analityczne procedury są jedne z najważniejszych metod audytu. Oni włączają nie tylko metodyczne przyjęcia ekonomicznej analizy i metodykę analizy finansowej sprawozdawczości, a wymagają wykorzystywać i inne, oprócz analizy, ogólne naukowe metody: syntezę, abstrahowanie, indukcję, dedukcję i tym podobne. Użycie analitycznych procedur odbywa się w ciągu całego procesu audytu, lecz cel ich stosowania i zdobyte wyniki są różne, co nadaje im wielobocznośći. Badaniu problemu użycia analitycznych procedur w audycie, jak i metodyce analizy finansowej sprawozdawczości, poświęcono wiele naukowych badań w literaturze. Jednak dotychczas jeszcze nie określony tryb użycia analitycznych procedur i metodyka oceny funkcjonowania przedsiębiorstwa, która jest jedna z najważniejszych zadań audytu.

LITERATURA

1. Analiza ekonomiczna w przedsiębiorstwie, red. M. Jarzemowska, Polskie Wydawnictwo Ekonomiczne, 2013.

2. Brammertz W., Akkizadis I., Breymann W., Entin R., *Unified Finantional Analysis. The Missing Links of Finance*, John Wiley & Sons, Ltd, 2009 i in.

3. Hayes R., Dassen R., Schilder A., Wallage P. *Principles of auditing; an introduction to Internal Standards of Auditing*, Second Edition, Prentice Hall, 2005, S. 335-338.

4. Gołębiowski G., Grycuk A., Tłaczała A., Wiśniewski P., *Analiza finansowa przedsiębiorstwa*, Difin, 2014.

5. *International Standard of Auditing 520, «Analytical Procedures»*, Handbook of International Quality Control, Auditing, Revue, Other Assurance, and Related Services Pronouncements. Edition 2016, Vol. 1.

6. Porter B., Simon J., Hatherly D. *Principles of External Auditing*. Second edition, John Wiley & Sons, LTD, 2003s. 228-229.

[i] S. Wrzosek, Znaczenie efektywności ekonomicznej w procesach decyzyjnych przedsiębiorstw, [w:] Efektywność źródłem bogactwa narodów , red. T.Dudycz, S.Wrzosek, WAE, Wrocław, s. 588 oraz A .Ćwiąkała-Małys, Pomiar efektywności procesu kształcenia w publicznym szkolnictwie wyższym, WUW, Wrocław 2010, s. 80

[ii] S. Malmquist, Index numbers and indifferences surfaces, Trabajos de Estastica 4, 1953, s.209-242

[iii] Caves D.W., Christensen L.R., Diewert W.E. 1982a: Multilateral comparisons of output, input and productivity using superlative index numbers, Economic Journal, vol. 92, 73-86. Caves D.W., Christensen L.R., Diewert W.E. 1982b: The economic theory of index numbers and the measurement of input, output and productivity, Econometrica, vol. 50, 1393-1414.

[iv] Färe R., Grosskopf S., Lindgren B., Roos P. 1994: Productivity developments in Swedish hospitals: A Malmquist Output Index Approach, [in:] A. Charnes, W.W. Cooper, A.Y. Lewin, L.M. Seiford (eds.), Data Envelopment Analysis: Theory, methodology and applications, Kluwer Academic Publishers, Boston.

[v] A. Bezat-Jarzębowska, Produktywność przedsiębiorstw z wybranego sektora przetwórstwa żywności – dekompozycja Indeksu Malmquista, Szkoła Główna Gospodarstwa Wiejskiego w Warszawie, Stowarzyszenie Ekonomistów Rolnictwa i Agrobiznesu Roczniki Naukowe , Tom XVI, Zeszyt 6

Н А У К О В Е В И Д А Н Н Я

ІТ ПРАВО:
ПРОБЛЕМИ І ПЕРСПЕКТИВИ РОЗВИТКУ В УКРАЇНІ

Збірник матеріалів
науково-практичної конференції
18 листопада 2016 р.

Упорядники –
Бачинський Т.В., Лозовицький Д.С., Радейко Р.І.

Матеріали опубліковано в авторській редакції

Комп'ютерна верстка
Пастух Г.І.

Друк
Кочкодан А.М.

Здано до набору 10.11.2016 р. Підписано до друку 14.11.2016 р.
Формат 60х84/16. Папір офсетний. Умовн. друк. арк. 23,02.
Зам. № 64-16. Тираж 100 прим.

Для заміток