

підходу відкривають нові можливості для збереження і управління різними типами даних, зберігаючи при цьому звичні табличні структури. На відміну від чисто об'єктних баз даних, перехід до об'єктно-реляційних систем не вимагає масового перепрограмування.

Найбільш важливими новими об'єктно-реляційними можливостями є: визначені користувачами типи; визначенні користувачами функції; інфраструктура (методи індексації і доступу, а також вдосконалені способи оптимізації).

Все це показує перспективність подальшого розвитку об'єктно-реляційних систем баз даних, відкриває нові можливості для збереження і управління різними типами даних, дозволяючи використовувати їх в різних нетрадиційних предметних областях, зберігаючи при цьому звичне представлення даних.

Висновки:

Положення, сформульовані у даній статті, доповнюють науково-практичну систему знань щодо методів і принципів розробки баз даних для оперативного управління промисловим виробництвом.

Результати статті можуть бути використанні при створенні обґрунтованої методології розробки баз даних для ІАСУ організаціями.

1. Бойко В.В., Савинков В.М. Проектирование баз данных информационных систем. – М.: Финансы и статистика, 1989. – 351 с.
2. Куликовский Л.Ф., Мотов В.В. Теоретические основы информационных процессов. – М.: Высш. шк., 1987. – 248 с.
3. Мерстюк В.Г., Иоадесян А.Н. Автоматизация управления финансами, сущность и проблематика //Вестник ХГТУ. – 2002. - №1(14). – С. 151 – 155.
4. Мартин Дж. Организация баз данных в вычислительных системах. – М.: 1980. – 662 с.
5. Четвериков В.Н. Базы и банки данных. – М.: Высш. шк., 1987. – 248 с.
6. Шолье Ж. Банки данных: Использование электронной вычислительной техники / Пер. с франц., под ред. Б.А. Щукина. – М.: Энергоиздат, 1981. – 72 с.

Ісмайлов Карен Юрійович
к.ю.н., завідувач кафедри
кібербезпеки та інформаційного
забезпечення Одеського державного
університету внутрішніх справ

ДЕЯКІ ПИТАННЯ ІНФОРМАЦІЙНО-ПРАВОВОЇ ВІДПОВІДАЛЬНОСТІ В УКРАЇНІ

Актуальність питання про формування нового різновиду юридичної санкції у вигляді інформаційно-правової відповідальності обумовлена тим, що у юриспруденції, до цього часу, означений різновид державного примусового заходу не розглядався вченими в системі теорії юридичної відповіда-

льності, як самостійний.

Сучасне інформаційне право в Україні набуває від цілого комплексу інших галузей певні правові інститути, в тому числі й інститут інформаційно-правової відповідальності, що формується з норм, які розташовані в адміністративному, цивільному, кримінальному праві та в самому інформаційному праві і відповідно інформаційному законодавстві. З одного боку це дає додаткових підстав відносити інформаційне право до комплексної галузі права. З другого – це підтверджує комплексний характер інформаційного права та наявність тісних взаємозв'язків між різними галузями права і законодавства. Відтак, логічно передбачати, що головна мета інформаційно-правової юридичної відповідальності – максимальний захист та відновлення порушеного права на інформацію суб'єктів інформаційно-правових відносин.

На питання про інформаційно-правову відповідальність в національній юриспруденції в своїх публікаціях вже звертали увагу такі науковці, Л.П. Коваленко, В.А. Ліпкан, Г.М. Писаренко, А.А. Письменицький, О.О. Тихомиров, О.К. Тугарова.

Так, В.А. Ліпкан сформулював в своїх дослідженнях цілу низку відповідних інформаційно-правових категорій: Інформаційна деліктологія — самостійна підгалузь інформаційного права, що містить сукупність знань про інформаційні делікти і деліктність як масове негативне явище, що містить в собі детермінанти протиправної поведінки делінквента, їхньої особистості з метою вироблення і використання адекватних заходів для протидії інформаційних правопорушень [1].

Л.П. Коваленко вбачає в широкому розумінні, інформаційно-правову відповідальність, як вид юридичної відповідальності, якому притаманні всі ознаки останнього, вона є складовою частиною державного примусу, це накладення на правопорушників (фізичних і юридичних осіб), загальнообов'язкових правил, які діють в інформаційній сфері, стягнень, що тягнуть за собою для цих осіб обтяжливі наслідки юридичного характеру.

У вузькому розумінні, інформаційно-правова відповідальність - це вид юридичної відповідальності, який полягає в застосуванні до фізичних і юридичних осіб, які вчинили інформаційні проступки, особливих санкцій - інформаційних стягнень [2].

Г.М. Писаренко зазначає, що у теорії права існує думка, що нині приступити до вивчення юридичної відповідальності з позиції інформаційних відносин важко, оскільки визначення інформаційної відповідальності не існує на законодавчому рівні, а також відсутній єдиний кодифікований нормативно-правовий акт, у якому містився б перелік інформаційних правопорушень і визначалася б специфічність санкцій інформаційного права [3].

Найбільш комплексним є підхід до питання про інформаційно-правову відповідальність у публікаціях і монографіях доцента А.А. Письменицького, який розробив в Україні, ще з 1993 року, фактично основу теорії інформаційного права. Зокрема його бачення категорії інформаційно-правової відповідальності було оформлено в одній із наукових публікацій 2017 року у наступній дефініції: Інформаційно-правова відповідальність – це система заходів

примусового характеру, передбачених чинним законодавством, що призводять до претерпівання порушником інформаційного законодавства певних обмежень в інформаційних правах і свободах та не охоплюються іншими видами юридичної відповідальності. Правові наслідки інформаційно-правової відповідальності проявляються у тому, що суб'єктом інформаційних правовідносин втрачаються чи обмежуються можливості щодо: пошуку, одержання, створення, використання, зберігання, поширення або захисту інформації у будь-який вільно обраний спосіб і не залежно від кордонів [4].

Останнім часом найбільш поширена практика застосування примусових заходів інформаційно-юридичного характеру в сфері діяльності таких органів державної влади, як Рада національної безпеки і оборони України та Національна рада з питань телебачення та радіомовлення.

Упродовж 2015 року Національною радою з питань телебачення і радіомовлення проводився моніторинг програм іноземного виробництва. Через виявлення порушень із Переліку іноземних програм, зміст яких відповідає вимогам Європейської конвенції про транскордонне телебачення [6] і законодавства України було вилучено 10 телеканалів Російської Федерації: «24 Техно», «МИР 24», «Страна», «Русский иллюзион», «Дом кино», «Оружие», «Многосерийное ТВ», «Школьник ТВ», «Феникс+кино», «Иллюзион +». В даному випадку було застосовано положення Європейської конвенції про транскордонне телебачення, що встановлює порядок, за яким у випадках, якщо порушення має очевидний, серйозний і тяжкий характер, а також призводить до виникнення складних громадських проблем.

В ефірі згаданих вище російських мовників також було зафіксовано трансляцію: телевізійних фільмів та серіалів, які заборонені для розповсюдження і демонстрування на території України Державним агентством України з питань кіно; передач, у яких популяризувалися стратегічні об'єкти Російської Федерації, а також висвітлювалися найновітніші види російського озброєння і засоби ведення бою; сюжетів новин і фрагментів передач, які містили заклики до зміни конституційного ладу у країні, рекламу миротворчих сил Російської Федерації, пропаганду війни та порушення територіальної цілісності України; передач з інтерактивними конкурсами, зміст яких суперечить вимогам частини третьої статті 6 Закону України «Про телебачення і радіомовлення» [5, ч.3 ст.6]. Зокрема, 2015 року до п'яти провайдерів програмної послуги було застосовано санкцію «оголошення попередження» у зв'язку з ретрансляцією програм, не передбачених відповідним актом Національної ради.

Так, Рішенням Ради національної безпеки і оборони України від 25.01.2015 року «Про надзвичайні заходи протидії російській загрозі та проявам тероризму, підтримуваним Російською Федерацією», затвердженої Указом Президента України [6] було передбачено «ужити за участю Національної ради України з питань телебачення і радіомовлення невідкладних заходів щодо припинення російської інформаційної агресії, здійснюваної з використанням іноземних та вітчизняних засобів масової інформації» [7, п. 1. 5].

У 2015 році до п'яти провайдерів програмної послуги було застосовано

санкцію «оголошення попередження» у зв'язку з ретрансляцією програм, не передбачених цим актом Національної ради з питань телебачення і радіомовлення. Також 2015 року було тимчасово припинено розгляд питань щодо визнання змісту програм адаптованим до вимог законодавства України, власники (виробники) яких підпадають під юрисдикцію Російської Федерації. Таке рішення було прийнято, зважаючи на ведення бойових дій на сході України, військову та інформаційну агресію проти України, визнання законодавством України Російської Федерації державою-окупантом та державою-агресором, беручи до уваги антиукраїнську позицію цієї держави щодо територіальної цілісності, суверенітету України в цілому, з метою забезпечення інформаційної безпеки та захисту територіальної цілісності України [8].

17 травня 2017 року, набув чинності Указ Президента України Петра Порошенка про введення санкцій відносно ряду російських інформаційних продуктів, зокрема соцмережі «ВКонтакте» і «Однокласники», ІТ-компаній, «Яндекса» (та його української «дочки») і поштового сервісу Mail.ru, а також бухгалтерської програми 1С [9].

У цьому акті значними для інформаційної безпеки і кібербезпеки України є не лише кількість осіб, щодо яких застосовано санкції (1228 фізичних та 468 юридичних осіб), а й види застосованих обмежень [10].

Щодо заборони інтернет-провайдером надання послуг з доступу користувачам мережі інтернет до ресурсів/сервісів на певних доменах, то це захисний інструмент чинного законодавства, що застосовується на загальнодержавному рівні вперше. Одночасно, це є й одним з видів нової генерації юридичної відповідальності, що сучасні науковці визначають як інформаційно-правову.

Так, стаття 4. Закону України «Про санкції» дає перелік видів санкцій і у пункті 9 передбачає, що окремим різновидом такого державного примусу є обмеження або припинення надання телекомунікаційних послуг і використання телекомунікаційних мереж загального користування [11]. Це, в свою чергу, відсилає нас до іншого закону – Закону України «Про телекомунікації», що визначає телекомунікаційну мережу загального користування, як телекомунікаційну мережу, доступ до якої відкрито для всіх споживачів. В свою чергу саме поняття телекомунікаційної мережі, Закон характеризує, як комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням [12].

Усі вище перераховані приклади підтверджують широке застосування владними органами заходів примусового характеру, що спрямовуються на обмеження прав допуску суб'єктів професійної інформаційної діяльності до інформації, заборону їм поширювати певну інформацію, обмеження прав на розповсюдження певної інформації, та призупинення інформаційної діяльності. Всі ці заходи мають певні спільні ознаки, що виокремлюють означені санкції серед різновидів юридичної відповідальності в самостійну групу. Зок-

рема, всі ці приклади застосування інформаційно-юридичного впливу, здебільше, вимагали прийняття окремих нормативно-правових актів, починаючи від Законів України і до окремих рішень Національної ради з питань телебачення і радіомовлення. Це було обумовлено, переважно, відсутністю у національному законодавстві, до того часу, необхідних важелів примусового впливу на суб'єктів інформаційних відносин, які систематично, або з важкими наслідками порушують права інших суб'єктів на інформацію і раніше не несли за це ніяких правових наслідків у вигляді обмежень, або втрат в інформаційній свободі. Вектор спрямування означених санкцій направлений не на матеріальний прояв прав і свобод сторін у інформаційних відносинах, а саме, на їх право на інформацію. Тобто, якщо стороною відносин здійснювалось зловживання правом на інформацію, в певному аспекті, що обмежувало це право у інших сторін, то санкціями здійснювалось обмеження або скасування саме цієї частини права на інформацію винного суб'єкта.

Таким чином, інформаційно-правова відповідальність – це система заходів примусового характеру, передбачених чинним законодавством, що призводять до претерпування порушником інформаційного законодавства певних обмежень в інформаційних правах і свободах.

Зазначена характеристика і розуміння інформаційно-правової відповідальності дає підстави вважати, що основною метою такого виду відповідальності виступає забезпечення більшої повноти реалізації інформаційних прав і свобод іншим суб'єктам інформаційних правовідносин.

1. Ліпкан В.А. Вікіпедія. Електронна інтернет-енциклопедія // [Електронний ресурс]. - Режим доступу: <https://uk.wikipedia.org/wiki/18.10.2017>.

2. Коваленко Л.П. Юридична відповідальність за правопорушення у сфері інформаційної діяльності / Л.П. Коваленко // Проблеми законності. - 2012. - Вип. 120. - С. 165-172.

3. Писаренко Г.М. Юридична відповідальність в інформаційній сфері: окремі аспекти становлення // Наук. вісник Ужгородського національного університету, 2016. Серія ПРАВО. Випуск 36. Том 2. – С. 55-58.

4. Письменицький А.А. До теоретико-правового концепту кібербезпеки та інформаційної юридичної відповідальності // Кібербезпека в Україні: правові та організаційні питання: матеріали всеукр. наук.-практ. конф., м. Одеса, 17.11.2017 р. – Одеса : ОДУВС, 2017. – С. 162-165.

5. Про телебачення і радіомовлення. Верховна Рада України. Закон від 21.12.1993 № 3759-XI // Відомості Верховної Ради України, 1994, N 10, ст. 43

6. Про рішення Ради національної безпеки і оборони України від 25 січня 2015 року "Про надзвичайні заходи протидії російській загрозі та проявам тероризму, підтримуваним Російською Федерацією".; Указ Президента України від 14.02.2015 № 85/2015 // [Електронний ресурс]. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/85/2015>.

7. Про надзвичайні заходи протидії російській загрозі та проявам тероризму, підтримуваним Російською Федерацією. Рішення Ради національної безпеки і оборони України від 25.01.2015 // [Електронний ресурс]. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/n0001525-15>

8. Звіт Національної ради України з питань телебачення і радіомовлення за 2015 рік // [Електронний ресурс]. – Режим доступу: <http://www.nrada.gov.ua/userfiles/file/2016/Zvitna%20informacia>

9. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів"

дів (санкцій)". Указ Президента України від 15.05.2017 № 133/2017 // Урядовий кур'єр від 17 травня 2017 року // [Електронний ресурс]. Режим доступу: <http://zakon3.rada.gov.ua/laws/show/133/2017>.

10. Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій). РНБО; Рішення від 28.04.2017 // [Електронний ресурс]. Режим доступу: <http://zakon3.rada.gov.ua/laws/show/n0004525-17/paran2#n2>.

11. Про санкції. Закон України; від 14.08.2014 № 1644-VII // Відомості Верховної Ради (ВВР), 2014, № 40, ст.2018.

12. Про телекомунікації. Закон України від 18.11.2003 № 1280-IV // Відомості Верховної Ради (ВВР), 2004, N 12, ст.155. Редакція від 04.06.2017, підстава 1834-19, 1983-19.

Коренюк Петро Іванович

д.е.н., проф., завідувач кафедри
менеджменту організацій
і адміністрування Дніпровського
державного технічного університету

Коренюк Людмила Володимирівна

к.е.н., доцент, доцент кафедри
фінансів та економічної безпеки
Дніпропетровського національного
університету залізничного
транспорту імені В. Лазаряна

ОСОБЛИВОСТІ ФОРМУВАННЯ КОНКУРЕНТНОЇ РОЗВІДКИ У КОНТЕКСТІ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

У сучасних ринкових умовах в бізнесі зростає значимість аналізу можливих ситуацій, з'ясування домінуючих тенденцій, розрахунок можливих ризиків при ухваленні господарських рішень. Недостатньо володіти інформацією у вигляді результатів маркетингових досліджень або бізнес-довідок про потенційних партнерів і конкурентів. Виникає потреба з метою виживання дати відповідь на питання: хто або що є причиною виникнення подій, звідки виходить або може виходити загроза, як її уникнути або мінімізувати? Нагальна потреба у вирішенні таких задач і стала причиною виникнення конкурентної розвідки. За сутністю та змістом конкурентна розвідка не є промисловим шпигунством, адже вона функціонує виключно в рамках чинного законодавства. Але джерела інформації для конкурентної розвідки завжди «відкриті» і загальнодоступні, хоча не завжди опубліковані.

Проблему фінансово-економічної безпеки та конкурентної розвідки прямо та опосередковано досліджена у працях О. Г. Білорус [1], О. Р. Бойкевич [2], Т. Г. Васильціва [2], В. І. Волошина [2], В. О. Голубєва [4], Т. В. Давидюк [3], В. В. Каркавчук [2], В. А. Ліпкан [6], О. В. Логінова [6], В. Г. Лукашевич [4], О. М. Марченко [5], І. П. Мойсеєнко [5], А. В. Товксиса [8],