ISSN 1995-6134

УДК 340:659.4.327.88(477)

С.О. ЛИСЕНКО,
канд. юрид. наук, доц., Міжрегіональна академія управління персоналом
ORCID: http://orcid.org/0000-0002-7050-5536
ResearcherID: http://www.researcherid.com/rid/B-8113-2017

АДМІНІСТРАТИВНО-ДЕЛІКТНЕ ПРАВО СТОСОВНО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В УКРАЇНІ

Ключові слова: *інформаційна безпека, адміністративно-деліктне право, адміністративно-правове забезпечення, інформаційне право, національна безпека, інформація*

Під час здійснення адміністративного регулювання інформаційних відносин, інформація визнається об'єктом інформаційних відносин. Право власності на інформацію, згідно Закону України «Про інформацію», є об'єктом охорони, тобто інформаційної безпеки [1].

Однак, в Кодексі України про адміністративні правопорушення не визначенна інформація в якості об'єктів протиправних посягань. В КУпАП адміністративно-деліктне законодавство об'єднало даний об'єкт з іншими адміністративними правопорушеннями за критеріями, що не завжди входять в сферу впливу інформаційної безпеки підприємств [2]. У такому разі істотно знижується ефективність діяльності з профілактики таких деліктів, втрачається правовий і функціональний зв'язок між деліктами і нформаційної безпеки та встановленою відповідальністю за їх вчинення. В дослідженні адміністративні інформаційних правопорушеня розглядатимуться, як система однорідних деліктів, вчинених в межах здійснення інформаційної безпеки, згідно з їх ознаками та властивостями.

Серед українських науковців проблемі адміністративних деліктів приділяли увагу І.В. Арістова, Г.В. Виноградова, В.Н. Колпаков, Б.А. Кормич, О.А. Заярний, В.С. Цимбалюк, які вказували на необхідність систематизації і розширення кола суб'єктів адміністративно-деліктних відносин в інформаційній сфері. На відміну від них, автор наголошує на введення підприємства до складу спеціальних суб'єктів, а також про надання спеціальних повноваженнь суб'єктам інформаційної безпеки щодо сбору матеріалів та документування інформаційних адміністративних правопорушеннь.

Правова природа адміністративних правопорушень, скоєних при забезпеченні інформаційної безпеки підприємств, постає інструментом систематизації знань у сфері адміністративної деліктології, а також виконує пояснювальну, евристичну та прогностичну функції.

Невід'ємною частиною адміністративно-деліктної процедури є відповідальність та заходи примусу за скоєння правопорушеннь інформаційної системи безпеки підприємств. Адміністративний примус – це система заходів психологічного та психічного впливу на свідомість та поведінку людей з метою досягти чіткого виконання визначених обов'язків, розвитку суспільних та корпоративних відносин у межах прийнятих на підприємстві норм, для забезпечення правопорядку і законності. Одночасно, він є одним із видів державного примусу, якому притаманні застосування засобів примусового характеру з метою забезпечення потрібної поведінки осіб, а також застосовання для охорони суспільних відносин, які виникають під час взаємодії держави та підприємства, для встановлення порядку застосування відповідних примусових заходів. Порядок застосування примусових заходів регулюється нормами адміністративного права, що виключають адміністративно-правові норми актів виконавчих органів. Систему заходів адміністративного примусу утворюють: заходи адміністративного запобігання; заходи адміністративного припинення; адміністративні стягнення (заходи відповідальності за порушення інформаційної безпеки підприємств).

ISSN 1995-6134

Законодавець формулює зміст адміністративно-деліктних норм відповідно до суб'єкту складів адміністративних правопорушень норм інформаційної безпеки підприємств, визначає через особу, до якої застосовуються адміністративні стягнення за вчинене правопорушення. Юридичний склад адміністративного правопорушення, будучи встановленою нормами права системою ознак, включає в себе конструктивні ознаки, які характеризують особу, що вчинила протиправні дії чи бездіяльність, як суб'єкт адміністративного проступку системи інформаційної безпеки підприємств [3].

Ознаки, які характеризують суб'єкта адміністративних правопорушень в системі інформаційної безпеки підприємств, можна розділити на загальні та спеціальні. Якщо винна особа в момент вчинення правопорушення системи інформаційної безпеки підприємства не була наділена спеціальними правами чи повноваженнями, або вчиняла протиправне діяння не як посадова чи службова особа, то вона відноситься до загальних суб'єктів. В інших випадках особа відноситься до спеціальних суб'єктів. Традиційно до ознак, які характеризують учасника інформаційних відносин як загального суб'єкта адміністративних інформаційних правопорушень, належать вік та осудність порушника [4].

Керуючись вищевказаним, до загальних суб'єктів адміністративних інформаційних правопорушень відносяться фізичні, осудні особи, які досягли шістнадцятирічного віку, не перебувають на державній службі або службі в органах місцевого самоврядування, не є посадовими чи службовими особами підприємств та організацій, не здійснюють самостійно підприємницьку діяльність в інформаційній сфері [4].

На думку кількох українських вчених, однією з особливостей адміністративно-деліктних відносин в межах інформаційної безпеки є те, що вони виникають у зв'язку з порушенням норм матеріального права, а документуються та припиняються у сфері дії норм адміністративно-процесуального права, у зв'язку з його правовою кваліфікацією, а також через застосування заходів адміністративного примусу до правопорушника. Зрозуміло, що відносини, які виникли у зв'язку з вчиненням адміністративних правопорушень інформаційної безпеки підприємств, виникають в наслідок порушення матеріальних норм інформаційного права та одержують правову кваліфікацію з боку уповноважених органів адміністративної юрисдикції, згідно з нормами адміністративно-деліктного права. Зв'язок інформаційної безпеки та адміністративно-деліктних відносин на підприємстві, в разі вчинення адміністративного інформаційного правопорушення вказує на те, що загальним суб'єктом цих деліктів є передусім учасник інформаційних відносин, тобто особа, наділена інформаційною та адміністративно-деліктною правосуб'єктністю [5].

У визначенні суб'єктів інформаційних відносин Закон України «Про інформацію» надав розуміння цього поняття через цілі правового регулювання інформаційних відносин, де ключове значення мають не внутрішні ознаки суб'єктів інформаційних відносин – їх соціальний та майновий стан, організаційно-правова форма чи внутрішня структура підприємства, а динамічні властивості їх правового статусу, які виражаються в їх правосуб'єктності [1].

Стосовно підприємств-учасників інформаційних відносин встановлена законодавча прогалина, яка частково заповнюється шляхом системного тлумачення положень ст.ст.218 та 238 Господарського кодексу України. Одночасно питання про визнання за підприємством ознак спеціального суб'єкта, має вирішуватися не до підприємства в цілому, а залежно від того, в якому статусі діє такий суб'єкт у конкретних відносинах, у межах яких вчинено інформаційне правопорушення [6].

Спеціальних ознак підприємство може набути загалом двома способами: 1) нормативним – отри-мання державного дозволу, ліцензії, делегування повноважень, наявність яких робить можливим скоєння правопору-

ISSN 1995-6134

шення; 2) фактичним – набуття певних реальних ознак (монопольне становище на ринку), не пов'язаних із державним дозволом, але за відсутності яких конкретне правопорушення вчинене бути не може [6].

Наведені способи мають у своїй основі окрему групу спеціальних ознак, яким відповідають лише окремі юридичні особи, як учасники процесу забезпечення інформаційної безпеки, суб'єкти адміністративних інформаційних правопорушень, за відсутності яких вчинення того чи іншого проступку фактично є неможливим.

Керуючись науково визначеними видами інформаційної діяльності, усі адміністративні правопорушення інформаційної безпеки підприємств, в залежності від об'єкта протиправних посягань, також і змісту відносин такої діяльності, можна розділити на такі підвиди: у сфері забезпечення права доступу громадян та юридичних осіб до публічної інформації; в галузі інформатизації; в галузі реклами; в галузі формування та використання інформаційної інфраструктури; у сфері електронного урядування; в галузі індустрії програмної продукції; у сфері забезпечення інформаційної безпеки та захисту інформації; в медіасфері; в галузі видавничої та бібліотечної справи; в галузі науково-технічної та освітньої діяльності; у сфері виборчого процесу та процесу референдуму; в галузі формування та використання національних інформаційних ресурсів; що посягають на встановлений порядок інформаційного забезпечення діяльності суб'єктів владних повноважень; в галузі статистики та архівної справи.

Аналогічно, керуючись буквальним змістом адміністративно-деліктних норм, правопорушення інформаційної безпеки підприємств, у залежності від характеру протизаконних дій, можна класифікувати на такі: що вчиняються шляхом надання інформації в неповному обсязі, або недостовірної, неповної інформації; внесення до державних реєстрів кадастрів, баз даних, архівних фондів, каталогів неповної або недостовірної інформації, а також внесення інформації з порушенням установлених законом строків; безпідставне розкриття або засекречення інформації з обмеженим доступом; незаконне копіювання баз даних, реєстрів чи окремої інформації, що в них міститься; незаконне використання комерційної таємниці чи іншої інформації з обмеженим доступом з метою обмеження економічної конкуренції, заподіяння шкоди честі, гідності чи діловій репутації підприємства; поширення неправдивих чуток, недостовірних відомостей; умисне розкриття інсайдерської інформації з метою укладення неправомірних угод, протиправне втручання в роботу, несанкціонований доступ, блокування роботи інформаційно-телекомунікаційних систем тощо [3, 5, 7–11]. Наведений перелік підвидів адміністративних правопорушень інформаційної безпеки підприємств не є вичерпним, оскільки в умовах триваючої адаптації законодавства України до положень і стандартів законодавства ЄС у національному правовому просторі постійно встановлюються нові склади деліктів, що розглядаються.

Як основний засіб комунікації між різноманітними особами, інформація розповсюджується, змінюється, обробляється, захищається або знищується активними діями учасників процесу забезпечення інформаційної безпеки підприємств, тому порушення чинних в інформаційній сфері правових обмежень, дозволів чи заборон стає можливим у разі активної поведінки суб'єктів інформаційного права. Але деякі дослідники зауважують, що «об'єктивна сторона правопорушення в інформаційній сфері виявляється переважно у формі бездіяльності (невиконання або неналежне виконання вимог Закону про надання інформації), а саме: у неправомірній відмові в наданні інформації, несвоєчасному або неповному наданні інформації, наданні інформації, що не відповідає дійсності» [11]. Хоча не слід перебільшувати кількість вчинених правопорушень в інформаційній сфері шляхом протиправної бездіяльності.

Чинне адміністративно-деліктне законодавство не вказує на те, що робити в разі допущення порушенн при складанні протоколу та інших матеріалів про адміністративне правопорушення. Враховуючи практику діяльно-

ISSN 1995-6134

сті органів адміністративно-деліктної юрисдикції виявлено, що посадові особи, уповноважені розглядати справи, дуже рідко знайомлять із матеріалами про адміністративне правопорушення осіб учасників, для усунення недоліків. Аналогічно не береться до уваги та не використовується досвід і можливості суб'єктів, що забезпечують інформаційну безпеку на підприємстві, під час документування та фіксації адміністративного делікту. Хоча це в рази підвищило якість та об'єктивність розгляду матеріалів у суді.

Під час підготовки до розгляду матеріалів суб'єкт адміністративно-деліктної юрисдикці, відповідно до ст.278 КУАП повинен забезпечити сповіщення осіб-учасників, про час і місце розгляду справи. Важливо дотримуватися таких процесуальних дій у разі, коли відповідно до ч.2 ст.268 КУАП при розгляді окремих категорій справ про адміністративні правопорушення, присутність особи, яка притягається до адміністративної відповідальності, є обов'язковою. Чинні норми КУАП не роз'яснюють порядок такого сповіщення, що є суттєвим упущенням.

Зазвичай, особи сповіщаються при складанні протоколу про адміністративне правопорушення шляхом отримання підпису про повідомлення про час розгляду справи про адміністративне правопорушення з підписом правопорушника в кінці протоколу; шляхом направлення повістки про необхідність явки до органу адміністративної юрисдикції для розгляду справи про адміністративне правопорушення; шляхом усного повідомлення правопорушника про день, місце та час розгляду справи. Зауважуєм, що законодавство не бере в рахунок можливості суб'єктів забезпечення інформаційної безпеки підприємств для цієї мети. Хоча участь цих осіб, у посадових інструкціях яких прямо вказано на обов'язок документувати та викривати правопорушення, була би для всіх сторін корисною. Звичайне сповіщення особи, яка притягується до відповідальності, простіше робити саме через осіб, які викрили та забезпечили документування [4].

Щоб уникнути зловживань від суб'єктів забезпечення інформаційної безпеки підприємств, необхідно законодавчо закріпити в КУАП випадки, в яких допускається збір матеріалів саме суб'єктами, коли вони можуть бути викликані в якості свідків для участі в розгляді справи та для інших процесуальних дій. Крім випадків, коли про виклик свідків клопоче особа, яка притягається до адміністративної відповідальності, потерпілий чи їх законні представники, адвокат чи прокурор. Аналогічно, коли в матеріалах справи немає письмових пояснень свідків, а особа, яка притягається до адміністративної відповідальності, заперечує свою причетність до вчиненого правопорушення [3, 11].

Таким чином, суб'єкти адміністративно-деліктної юрисдикції при забезпеченні інформаційної безпеки підприємств повинні здійснювати максимальний комплекс заходів, націлений на всебічне, повного й об'єктивного вивчення всіх обставин, що мають значення для вирішення справи. Одночасно необхідно враховувати, що всіляка забезпечена чинним законом діяльність суб'єкта адміністративної юрисдикції щодо збору, перевірки та оцінки доказів повинна здійснюватися в межах цього закону, а тягар доказування може бути покладено, виключно, на державні органи, що здійснюють адміністративну юрисдикцію. Такий підхід надасть можливість розвантажити державні органи під час збору матеріалів, складе позитивну конкуренцію, що відобразиться на якості під час збору матеріалів. Окремо треба наголосити, що це надасть підстави для позитивного розвитку недержавних суб'єктів інформаційної безпеки, якість та користь яких підвищується рік від року на теренах прогресивного світу, які на цей час досить вдало займають місце в національній системі інформаційної безпеки України.

ЛІТЕРАТУРА

1. Закон України «Про інформацію» : від 02.10.1992 р., № 2657–XII // ВВР України. – 1992. – № 48. – Ст. 650.

2. Кодекс України про адміністративні правопорушення : від 07.12.1984 р., № 8073–X // ВВР УРСР. – 1984 – № 51. – Ст. 1122.

ISSN 1995-6134

3. Колпаков В. Н. Адміністративне право України : підруч. / В. Н. Колпаков, О. В. Кузьменко. – К. : Юрінком Інтер, 2003. – 544 с.

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

5. Задорожня Л. М. Питання вдосконалення законодавства України у сфері інформації та інформатизації // Додаток до наук. журналу «Правова інформатика» / Л. М. Задорожня, М. І. Коваль, В. М. Брижко. – К. : Академія правових наук, 2005. – 31с.

6. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Б. А. Кормич. – Х., 2004. – 42 с.

7. Бегишев И. Р. Информационное оружие как средство совершения преступлений / И. Р. Бегишев // Информационное право. – 2010. – № 4. – С. 23–25.

8. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади: дис. ... доктора юрид. наук : 12.00.07 / Арістова Ірина Василівна. – Х., 2002. – 476 с.

9. Ліпкан В. А. Національна безпека України : навч.посібник / Ліпкан В. А. – 2-ге вид. – К. : КНТ, 2009. – 576 с.

10. Бачило И. Л. Информационное право. Роль и место в системе права Российской Федерации / Бачило И. Л. // Государство и право. – 2001. –№о 2. – С. 5–14.

11. Заярний О. А. Суб'єкт адміністративних інформаційних правопорушенн: поняття та особливості / Заярний О. А. // Адміністративне право і процес. – 2015. – № 2 (12). – С. 86–104.

Лисенко С. О. Адміністративно-деліктне право стосовно інформаційної безпеки підприємств в Україні // Форум права. – 2017. – № 1. – С. 84–88 [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/j-pdf/FP_index.htm_2017_1_16.pdf

Розглядається адміністративно-правове регулювання інформаційних відносин. Аналізується вітчизняне законодавство у сфері інформаційної безпеки. На основі дослідження визначаються ознаки, які характеризують суб'єкт адміністративних правопорушень в системі інформаційної безпеки підприємств. На підставі науково-визначених видів інформаційної діяльності, надано класифікацію адміністративних правопорушень у сфері інформаційної безпеки підприємств.

***

Лысенко С.О. Административно-деликтное право относительно информационной безопасности предприятий в Украине

Рассматривается административно-правовое регулирование информационных отношений. Анализируется отечественное законодательство в сфере информационной безопасности. На основе исследования определяются признаки, характеризующие субъект административных правонарушений в системе информационной безопасности предприятий. На основании научно-определенных видов информационной деятельности, предоставлено классификацию административных правонарушений в сфере информационной безопасности предприятий.

***

Lysenko S.O. Administrative Tort Law with Respect to Information Security Companies in Ukraine

The article deals with the administrative and legal regulation of information relations. It was analyzed domestic legislation in the field of information security. On the basis of the study are determined by the features that characterize the subject of administrative violations in the information security companies. On the basis of scientific and specific information activities, given the classification of administrative offenses in the sphere of information security companies was made.