Насамперед, кодифікації підлягає ідентифікація юридичної особи в Єдиному Державному Реєстрі юридичних осіб України – ЄДРПОУ із заповненням відповідних форм наслідками яких є одержання особистого ідентифікаційного коду організації. Другою важливою кодифікацією є реєстрація організаційно-правової форми господарювання за КОПФГ. На прикладі Харківського обласного громадського формування з ОГП і ДК таким кодом є група – «інші організаційно-правові форми» з кодом 995. Важливим кодом є код класифікатора по визначенню інституційного сектору економіки за КІСЕ. На наш погляд, таким ідентифікатором для ГФ є код – S.15 Некомерційні організації. Кодується також місцезнаходження за класифікатором КОАТУУ. Однак, найбільш важливішим є кодування видів діяльності ГФ за класифікатором КВЕД – 2010. Для Харківського обласного громадського формування з охорони громадського порядку і державного кордону, а тобто і для всіх формувань, які є його членами визначаються види діяльності за КВЕД – 2010:

84.24 Діяльність у сфері охорони громадського порядку та безпеки;

84.11 Державне управління загального характеру;

94.99 Діяльність інших громадських організацій, Н.В.І.У;

Вищенаведена система кодів гарантує організацію належне правове поле для усунення перешкод у створенні, функціонуванні та розвитку щодо її діяльності за змістом спеціальної правосуб'єктності надане їй законодавством України. Системна кодифікація дозволяє визначити діяльність ГФ як суб'єктів держави громадянського партнерства та збудувати правові засади розвитку недержавного сектору безпеки. Вибудова дієвої правоохоронної громадської технології Харківським обласним ГФ з ОГП і ДК привела до розробки сучасної мережної системи інформаційно-аналітичного моніторингу охорони громадського порядку і державного кордону з інтеграцією в єдиному просторі всієї міжвідомчої інформації. Також заплановано організувати разом з місцевим самоврядуванням мережі консультативно-дорадчих центрів правової допомоги функціонуючи на базі пунктів охорони правопорядку, громадських приймалень, штабів ГФ, тощо. Студенти юридичних національних закладів, члени ГФ можуть ефективно вносити свій вклад в роботу цих центрів, скоординувавши їх діяльність.

Галинська Каріна Юріївна

здобувач кафедри адміністративного права та адміністративної діяльності Національного юридичного університету імені Ярослава Мудрого (Україна, м.Харків)

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СЛУЖБОВОЇ ІНФОРМАЦІЇ В УКРАЇНІ: ПРАВОВІ АСПЕКТИ

Інститут службової таємниці є одним з найбільш складних в інформаційних правовідносинах. Його розвиток супроводжується постійними змінами у термінології, практики застосування відповідних нормативно-правових норм та захисті інформації, що відноситься до службової таємниці.

На цей час в українському законодавстві не можна знайти однозначного визначення службової інформації. Закон України «Про інформацію» у ст. 21 поділяє інформацію з обмеженим доступом на три категорії [3]: а) конфіденційну інформацію, б) таємну інформацію, в) службову інформацію. У свою чергу відповідно до ст. 9 Закону України «Про доступ до публічної

інформації», до службової інформації може належати, окрім зібраної в процесі оперативно-розшукової, контрозвідувальної діяльності та у сфері оборони країни, лише 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 [2].

Крім цього слід зазначити, що п. 3 ст. 21 Закону «Про інформацію» встановлено, що «порядок віднесення до таємної або службової інформації, а також порядок доступу до неї регулюються законом» [3]. Попри це, порядку віднесення інформації до службової законодавчо не встановлено. Натомість Закон «Про доступ до публічної інформації» визначає (п. 2 ст. 6) три загальні умови обмеження доступу до інформації [2]: виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя; розголошення інформації може завдати істотної шкоди цим інтересам; шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Провівши аналіз нормативно-правової бази, можна виявити зміст і основні принципи віднесення інформації до службової. За своїм змістом, службова інформація - це інформація, доступ до якої обмежений органами державної влади на підставі законодавства і не підлягає розголошуванню, окрім жорстко обкреслених випадків.

Не дивлячись на практично повну відсутність нормативного регулювання у сфері віднесення відомостей до службової інформації та забезпечення її безпеки, нормативні положення щодо обігу службової інформації можна знайти у більшості законодавчих актів України. Тому, правове регулювання у вигляді окремого закону дозволило б закласти правовий фундамент для формування системи обігу і забезпечення безпеки певної категорії відомостей, що відносяться до службової інформації, забезпечити ефективнішу реалізацію конституційних принципів в аспекті дотримання балансу прав громадян на доступ до інформації та обмежень таких прав з метою оборони, безпеки держави, прав громадян на захист приватного життя.

Слід зазначити, що категорія службової інформації не є виключно породженням вітчизняної юридичної доктрини. За даними низки досліджень, більшість юрисдикцій розвинених держав використовують систему обмеження в доступі до інформації з такою (або схожою) назвою для захисту внутрішньо системної інформації у своїх державних адміністраціях. До таких держав, зокрема, відносяться Іспанія, ФРН, Франція і США. Так, у Німеччині факти, відомості, що потребують збереження секретності, незалежно від форми їх оформлення (вирішенням державних установ або по їх розпорядженню) можуть мати гриф секретності «VSnurfurdendienstgebrauch» («для службового користування»).

У США під режим службової інформації підпадають і відомості, складові комерційної таємниці, а також інформація про різні ноу-хау, що отримується посадовою особою у процесі здійснення своїх посадових повноважень, досліджень або розслідувань, з доповіді або звіту тощо. У цих державах за неправомірне розповсюдження таких відомостей встановлена кримінальна відповідальність.

В українському законодавстві наступне. Відповідальність за порушення порядку розкриття інформації на фондовому ринку (ст. 163^{11} КУпАП); незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових повноважень (ст. 172^{8} КУпАП);

розголошення відомостей про заходи безпеки щодо особи, взятої під захист (ст. 185^{11} КУпАП); порушення порядку подання або використання даних державних статистичних спостережень (ст. 186^{3} КУпАП); порушення законодавства у сфері захисту персональних даних (ст. 188^{39} КУпАП); повідомлення неправдивих відомостей державним органам реєстрації актів цивільного стану та несвоєчасна реєстрація народження дитини (ст. 212^{1} КУпАП);порушення права на інформацію (ст. 212^{3} КУпАП); порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, які містять конфіденційну інформацію, що є власністю держави (ст. 212^{5} КУпАП); здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем (ст. 212^{6} КУпАП) [1].

Підводячи підсумки, слід сказати, що формальних вимог до забезпечення безпеки (захисту) службової інформації немає, оскільки не існує такого юридичного поняття. Як захищати службову інформацію і що взагалі мати розуміти під даним поняттям, - питання залишається відкритим. Труднощі у захисті конфіденційних даних (службової інформації, комерційної таємниці або персональних даних) сьогодні полягають не стільки у технічній площині (як захистити), скільки в організаційно-правовій. З метою забезпечення безпеки та надійного захисту службової інформації достатньо лише розробити політику інформаційної безпеки та запровадити процес моніторингу її дотримання і актуалізації. Також існує необхідність у розробці та прийнятті низки нормативно-правових актів щодо поняття, режиму віднесення відомостей до службової інформації, режиму доступу до неї, способів захисту службової інформації та механізмів реалізації цих законодавчих норм.

Науковий керівник: *д.ю.н., проф. афедри адміністративного права та адміністративної діяльності Національного юридичного університету імені Ярослава Мудрого Настюк Василь Якович.*

Гаращук Володимир Миколайович
д.ю.н., професор кафедри адміністративного права Національного юридичного університету імені Ярослава Мудрого (Україна, м.Харків)

ЗАКОННІСТЬ ТА РАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО ЯК ЧИННИКИ КОРПОРАТИВНОЇ І ПРИВАТНОЇ БЕЗПЕКИ

Як держава, так і її громадяни зацікавлені в стабільності, тобто постійній підтримці в державному управлінні та в суспільстві режиму законності і дисципліни. Законність – атрибут існування та розвитку демократично організованого суспільства, вона є обов'язковою для всіх елементів державного механізму. Законність необхідна для забезпечення свободи і реалізації прав громадян, демократії, утворення і функціонування громадянського суспільства, науково обґрунтованої розбудови і раціональної діяльності державного апарату. Законність водночас виступає важливим чинником корпоративної та приватної безпеки.

У своєму початковому вигляді законність створюється разом з першими правовими нормами давніх людських цивілізацій і знаходить своє зовнішнє відображення в перших письмових спробах законодавчого регулювання суспільних відносин – аналогах сьогоднішніх нормативних актів. Передумовою законності були моральні,