Список використаних джерел:

1. Бевзенко В.М. Інститут процесуальної співучасті в адміністративному судочинстві України: сутність та правове регулювання. *Держава і право*. 2010. № 47. С. 223.

2. Ківалов С.В. Понятійно-правова характеристика сторін як учасників адміністративного судочинства. *Наукові праці Національного університету «Одеська юридична академія»* : збірник наук. праць / редкол.: С.В. Ківалов (голов. ред.), М.В. Афанасьєва (заст. голов. ред), В.М. Дрьомін [та ін] ; відп. за вип. В.М. Дрьомін ; МОН України, НУ «ОЮА». Одеса : Юрид. л-ра, 2015. Т. 15. 22 с.

3. Постанова Великої Палати Верховного Суду від 18 грудня 2018 р. в справі № 9901/657/18 (П/9901/657/18). URL: http://reyestr.court.gov.ua/Review/78977396

4. Грось Л.А. Институт процессуального соучастия: связь между процессуальным и материальным правом. *Российская юстиция*. 1998. № 3. С. 35.

5. Сангаджиев Б.В. Особенности организационно-правового обеспечения деятельности федеральных судов общей юрисдикции Российской Федерации. *Вестник РУДН. Серия: юридические науки*. 2011. № 3.

УДК 346.9
DOI https://doi.org/10.32844/2618-1258.2019.6.37

РОГОВА Є.І.

ХАРАКТЕРИСТИКА ПОНЯТІЙНИХ КАТЕГОРІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В умовах сучасних глобальних та регіональних інформаційних протистоянь, деструктивних комунікативних впливів, зіткнення різновекторних національних інформаційних інтересів, поширення інформаційної експансії та агресії захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними стратегічними завданнями сучасних держав у системі глобальних інформаційних відносин. Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою і для України, яка часто є об'єктом зовнішньої інформаційної експансії, маніпулятивних пропагандистських технологій та руйнівного інформаційного вторгнення. В умовах російсько-українського конфлікту захист національного інформаційного простору від негативних інформаційно-психологічних впливів, операцій та війн, гарантування інформаційної безпеки та інформаційного суверенітету набувають особливого значення і стають чинниками збереження національної ідентичності України та функціонування її як суверенної та незалежної держави.

У світлі сучасних процесів значення інформації у суспільстві швидко зростає. Також і просування України до європейського співтовариства ставить перед нею важливе або можливо навіть і необхідне завдання – зайняття міцних позицій в усіх сферах суспільного життя, в тому числі і в інформаційній.

У сучасному світі інформація визначається як рушійна сила та домінуюча галузь, яка ставить за завдання впровадження передових інформаційних технологій в усі сфери суспільної діяльності. Тож інформаційна безпека є одним із найважливіших понять у науці і різних сферах людської діяльності. Сутність і комплексність цього поняття характеризує сучасне інформаційне суспільство. Враховуючи те, що питання інформаційної безпеки в умовах глобалізації носять гострий характер, необхідно визначити оптимальні шляхи усунення інформаційних загроз і небезпек і мінімізації впливу негативних наслідків у сфері інформаційної діяльності держави.

© РОГОВА Є.І. – аспірантка кафедри адміністративного права і процесу та митної безпеки (Національний університет державної фіскальної служби України)

У статті розкрито зміст поняття «інформаційна безпека» та проаналізовано підходи до визначення цієї категорії у різних нормативних актах. Разом із цим проаналізовано поняття «інформація». Здійснено спробу виокремлення видів інформаційної безпеки та інформації.

Ключові слова: *інформація, інформаційна безпека, інформаційні ресурси, державна безпека, інформаційний простір.*

In the context of modern global and regional information conflicts, destructive communicative influences, clashes of multi-vector national information interests, spread of information expansion and aggression, protection of the national information space and guaranteeing information security are the priority strategic tasks of modern states in the system of global information relations. The preservation of information sovereignty, the formation of an effective security system in the information sphere is also a pressing issue for Ukraine, which is often the subject of external information expansion, manipulative propaganda technologies, and destructive information invasion. In the context of the Russian-Ukrainian conflict, protecting the national information space from negative information-psychological influences, operations and wars, guaranteeing information security and information sovereignty are of particular importance and become factors for preserving Ukraine's national identity and functioning as a sovereign and independent state.

In the light of current processes, the value of information in society is growing rapidly. Also, Ukraine's promotion to the European Community puts before it an important, or perhaps even necessary, task – taking strong positions in all spheres of public life, including information. In today's world, information is defined as the driving force and dominant industry that sets itself the task of introducing advanced information technology into all spheres of public activity.

Therefore, information security is one of the most important concepts in science and in various fields of human activity. The essence and complexity of this concept characterizes the modern information society. Given that the issues of information security in the context of globalization are acute, it is necessary to determine the optimal ways to eliminate information threats and dangers and minimize the impact of negative consequences in the field of information activities of the state.

The article describes the content of the concept of information security and analyzes approaches to the definition of this category in various regulations. At the same time, the concept of "information" is analyzed. An attempt was made to isolate types of information security and information.

Key words: *information, information security, information resources, state security, information space.*

Вступ. Відповідно до Закону України «Про національну безпеку України» інформаційна безпека держави – це стан її захищеності, при якому спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдають суттєвої шкоди національним інтересам. Державна безпека – це захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенціальних загроз невоєнного характеру. Національна безпека України – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних і потенційних загроз.

Постановка завдання. Метою статті є здійснення правового аналізу інформаційної безпеки та надання характеристики понятійним категоріям інформаційної безпеки.

Результати дослідження. Перша спроба законодавчого визначення категорії «інформаційна безпека» була зроблена в концепції Національної програми інформатизації. Відповідно до цього нормативно-правового акту інформаційна безпека – це комплекс нормативних документів з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу, комплексу державних стандартів із документування, супроводження, використання сертифікаційних випробувань програмних засобів захисту ін-

формації, банк засобів діагностики, локалізації та профілактики комп'ютерних вірусів, нові технології захисту інформації з використанням спектральних методів, високонадійні криптографічні методи захисту інформації [1].

У Законі «Про інформацію» інформаційна безпека розглядається як «захищеність життєво важливих інтересів суспільства, держави і особи, якою виключається заподіяння шкоди через неповноту, несвоєчасність, недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок розповсюдження інформації, забороненої для розповсюдження законами України [2].

У законодавчому полі України, на жаль, відсутній рамковий закон про інформаційну безпеку держави. Сутність інформаційної безпеки визначена в Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». Між тим інші законодавчі акти, що набрали чинності після цього закону, не подають іншого тлумачення, уточнення або заперечення цього поняття. Тому, виходячи із сутності закону, поняття «інформаційна безпека» полягає у реалізації запобіжних заходів проти нанесення шкоди через неповноту, невчасність та невірогідність інформації, яка використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. Однак залишається нерозв'язаною задача розроблення теоретичних основ забезпечення інформаційної безпеки України. Є потреба удосконалення чинного законодавства України, зокрема базового термінологічного положення щодо визначення поняття «інформаційна безпека».

Кореневим у проблематиці інформаційної безпеки є поняття «інформація». Воно зустрічається у трьох нині чинних загальнодержавних документах прямої дії: Законах України: «Про інформацію», «Про телекомунікації», а також державному стандарті України ДСТУ 2226-93 «Автоматизовані системи. Терміни та визначення». Ось як подається це визначення:

– інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

– інформація – відомості, подані у вигляді сигналів, знаків, рухомих або нерухомих зображень чи в інший спосіб;

– інформація – відомості про об'єкти, процеси та явища [3].

Проводячи аналіз цих понять, можна зазначити, що всі визначення є різними, їх об'єднує тільки поняття «відомостей».

Не роз'яснюють на достатньому рівні поняття «інформаційна безпека» і нові нормативно-правові акти, викликані сьогоденням, боротьбою з російським агресором на сході держави: оновлена Воєнна доктрина України та Стратегічний оборонний бюлетень України. Все це свідчить про термінологічну невпорядкованість у різних офіційних документах, невідповідність їх законодавчому визначенню поняття інформаційної безпеки і потребує вдосконалення чинного законодавства України.

За методами забезпечення інформаційну безпеку підприємства можна об'єднати в три види:

– правова безпека;

– організаційна безпека;

– програмно-технічна безпека.

Правова безпека включає сукупність нормативно-правових актів, які регулюють відносини, пов'язані з використанням інформації в діяльності суб'єкта господарювання. Автор розглядає основні види такої інформації:

1) статистична інформація (офіційно документована державна інформація, що кількісно характеризує масові явища та процеси, які відбуваються в економічній, соціальній, культурній та інших сферах життя);

2) адміністративна інформація (це офіційно документовані дані, що характеризують явища та процеси, які відбуваються в економічній, соціальній, культурній та інших сферах життя і збираються, використовуються, поширюються та зберігаються органами державної влади, місцевого самоврядування, юридичними особами з метою виконання адміністративних завдань, що належать до їхньої компетенції);

3) масова інформація (публічно поширювана друкована та аудіовізуальна інформація);

4) інформація про діяльність державних органів влади та органів місцевого самоврядування;

5) правова інформація (сукупність документованих або публічно оголошених відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення);

6) інформація про особу (персональні дані);

7) інформація довідково-енциклопедичного характеру;

8) соціологічна інформація (це документовані або публічно оголошені відомості про ставлення окремих громадян і соціальних груп до суспільних подій і явищ, процесів, фактів).

За режимом доступу вирізняють відкриту інформацію та інформацію з обмеженим доступом. Інформація з обмеженим доступом поділяється на конфіденційну і таємну.

Конфіденційна інформація – це відомості, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їхнім бажанням відповідно до передбачених ними умов (наприклад комерційна таємниця). Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, отриманою за власні кошти, або такою, що є предметом їхнього професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушують передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність до категорії конфіденційної, та встановлюють для неї систему захисту. Виняток становить інформація комерційного і банківського характеру та інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків), а також інформація, приховування якої становить загрозу життю і здоров'ю людей.

Стосовно інформації, яка є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, то з метою її збереження може бути встановлено обмежений доступ, тобто надано статус конфіденційної. Порядок обліку, зберігання і використання документів та інших носіїв інформації, що містять зазначену інформацію, визначає Кабінет Міністрів України. Конфіденційною не може бути інформація, що містить відомості про:

1) стан довкілля, якість харчових продуктів і предметів побуту;

2) аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, що сталися або можуть статися і загрожують безпеці громадян;

3) стан здоров'я населення, його життєвий рівень, зокрема харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) справи із правами і свободами людини і громадянина, а також фактів їх порушень;

5) незаконні дії органів державної влади та місцевого самоврядування, їх посадових і службових осіб;

6) інша інформація, доступ до якої відповідно до законів України і міжнародних договорів та згода на обов'язковість яких надана Верховною Радою України, не може бути обмежена.

До таємної належить інформація, що містить відомості, які становлять державну чи іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі (наприклад державна таємниця, банківська таємниця).

Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до Закону про цю інформацію. Порядок і терміни оприлюднення таємної інформації визначаються відповідним законом ст. ст. 18–25 Закону України «Про інформацію».

Інформація з обмеженим доступом може поширюватися без згоди її власника, якщо вона є суспільно значущою, тобто є предметом громадського інтересу і право громадськості знати цю інформацію переважає над правом власника на її захист: Закон України «Про державну таємницю», ст. ст. 60–62; Закон України «Про банки і банківську діяльність», ст. 30; Закону України «Про інформацію». Отже, інформація є основним об'єктом інформаційної безпеки. Як об'єкт вона містить документи, ділові взаємовідносини, електронні носії інформації, технології виробництва, нові товари та послуги, знання.

Програмно-технічний вид інформаційної безпеки реалізується за допомогою засобів програмного та апаратного забезпечення. Організаційний вид полягає у забезпеченні збереження конфіденційної інформації суб'єктів господарювання шляхом формування корпоративної системи захисту [4].

Варто зазначити, що інформаційна безпека суб'єктів господарювання має деякі особливості, наприклад основним регламентом початкового стану впровадження системи інформаційної безпеки суб'єкта господарювання є призначення відповідальних осіб за безпеку і розмежування сфер їх впливу. Важливим складником інформаційної безпеки суб'єкта господарювання

є інформаційно-аналітична робота, основним завданням якої є збирання всіх видів інформації, яка може мати вплив на суб'єкт господарювання.

Аналізуючи практику інформаційних відносин суб'єктів господарювання та беручи до уваги роль інформації в такій діяльності, можна говорити, що інформаційна безпека включає такі її види: комп'ютерну безпеку, інформаційно-психологічну безпеку, комунікаційну безпеку та документаційну безпеку.

Комп'ютерна безпека передбачає захист засобів комп'ютеризації, комп'ютерних технологій і інформації, що знаходиться на електронних носіях; отримання необхідної суб'єктом господарювання інформації із глобального інформаційного простору (мережі Інтернет) для формування їх інформаційного ресурсу; протидія інформаційним загрозам у середовищі електронної інформації (комп'ютерні віруси, шкідливі програми, комп'ютерний тероризм).

Інформаційно-психологічна безпека зосереджує свої зусилля у сфері інформації та її носіїв (працівників, клієнтів, споживачів продукції суб'єктів господарювання). Основними напрямами забезпечення інформаційної безпеки є захист такої інформації (організація захисту інтелектуальної власності, режиму використання інформації працівниками та іншими особами у процесі інформаційних відносин); збереження інформаційного здоров'я працівників суб'єктів господарювання в умовах інформатизації виробництва; розробка технологій отримання такої інформації (пошукові дослідження, конференції, семінари, курси, симпозіуми) для формування інформаційного ресурсу суб'єктів господарювання; протидія технологіям маніпулювання інформацією, індивідуальною та колективною свідомістю.

Комунікаційна безпека включає захист інформації в процесі взаємообміну (електронна пошта, мобільний зв'язок) та ділового спілкування (зустрічі, перемовини); проведення заходів в інформаційному середовищі суб'єктів господарювання; протидія поширенню негативної інформації засобами масової комунікації.

Документаційна безпека спрямована перш за все на захист документаційної інформації та носіїв через запровадження надійної системи загального і спеціального діловодства, розробки нормативних документів із питань інформаційної безпеки; запровадження технологій отримання необхідних даних із різного роду документів правових активів, звітів, звичайних публікацій, виступів, описів для формування інформаційного ресурсу суб'єктів господарювання; документальне супроводження протидії інформаційним загрозам та інформаційно-психологічному впливу щодо суб'єктів господарювання, їх діяльності та персоналу (документування фактів порушення інформаційного режиму, поширення неправдивої інформації чи маніпулювання нею, документальне спростування негативної інформації, документи щодо вимог відшкодування моральної шкоди) [5].

Висновки. Натепер інформаційна безпека в умовах глобалізації інформаційного простору потребує вироблення теоретико-правових, методологічних, концептуальних, доктринальних, стратегічних, тактичних та оперативних правових засобів, які будуть здатні врегулювати суспільні інформаційні відносини. Дослідження в юридичній науці підтверджують необхідність гармонізації законодавства про інформаційну безпеку у повному зв'язку з міжнародними правовими процесами. Інформаційна безпека в нормативно-правовому аспекті має конституційний статус. Відповідно до статті 17 Конституції України визначення інформаційної безпеки можна подати як функцію – це одна з найважливіших функцій держави, справа всього українського народу щодо захисту суверенітету України.

Список використаних джерел:

1. Марущак А.І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки, 2011. № 21. С. 92–95.

2. Безуглий Д.С. Інформаційна безпека України: огляд останніх тенденцій / Д.С. Безуглий // Фізико-математична освіта, 2018. Вип. 2. С. 13–17.

3. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. К. : МК – Прес, 2006. С. 201–205.

4. Камлик М.І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект. Навчальний посібник. К. : Атіка, 2005. С. 61–62.