УДК 346.9
DOI https://doi.org/10.32837/apdp.v0i86.2436

Є. І. Рогова

ТЕОРЕТИЧНІ ОСНОВИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Постановка проблеми. Теоретичні основи правового забезпечення інформаційної безпеки в науковій літературі розкриваються неоднозначно. У великій чисельності джерел зазначено, що поняття «інформаційна безпека» виникає з появою засобів інформаційних комунікацій між людьми. Забезпечення інформаційної безпеки України є найважливішою функцією держави, справою всього Українського народу з огляду на те, що теоретичні основи правового забезпечення інформаційної безпеки підлягають більш точному визначенню та тлумаченню як у науковій літературі, так і на законодавчому рівні.

Стан дослідження. Вказаній проблематиці присвячено значну кількість досліджень таких вітчизняних та зарубіжних вчених, як А.Г. Арсеєнко, М.В. Банчук, О.І. Доронін, Ю.І. Когут, Б.А. Кормич, І.Б. Лук'янець, А.І. Марущак, С. Миллер, Д. Прескот, А.Й. Одінцов, А.Г. Шаваев, В.Й. Ярочкін та інші.

Попри їх вагомий внесок у сферу теоретичних основ правового забезпечення інформаційної безпеки, вважати, що всі питання у зазначеній сфері вирішені, не можна.

Мета дослідження – аналіз теоретичних основ правового забезпечення інформаційної безпеки.

Виклад основного матеріалу. Відповідно до Закону України «Про національну безпеку України» інформаційна безпека держави – це стан її захищеності, за якого 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 завдає суттєвої шкоди національним інтересам.

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

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.

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 з огляду на сутність цього закону поняття «інформаційна безпека» полягає у реалізації запобіжних заходів проти нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. Однак сьогодні 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». Звернемо увагу на дослідження категорії «інформаційна безпека» різними науковцями. Була здійснена спроба розроблення Кодексу інформаційного законодавства України (варіанти пропонували В.С. Цимбалюк, В.А. Ліпкан, Г.М. Красноступ). Термінологію в галузі інформаційної безпеки розробляли В.М. Бегма, В.П. Малінка, К.В. Рубель, А.І. Марущак. У своїх працях вони обґрунтовували досить широкий спектр термінів, уживаних у контексті інформаційної безпеки.

Кореневим у проблематиці інформаційної безпеки є поняття «інформація». 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 [1].

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

На цей час відсутні визначення багатьох взаємопов'язаних понять інформаційної сфери: «державна інформаційна політика», «інформаційний ресурс», «інформаційна безпека», «кібернетична безпека» тощо. Перша спроба розмежувати інформаційну та кібернетичну сфери у нормативно-правовій базі була зроблена у 2015 році в положеннях чинної Стратегії національної безпеки України, в якій окремо були визначені загрози інформаційній безпеці, загрози кібербезпеці і безпеці інформаційних ресурсів (хоча самі ці поняття на той час не були визначені).

Найбільш ґрунтовим є визначення інформаційної безпеки, що подається у Юридичній енциклопедії: інформаційна безпека України – це один із видів національної безпеки, важлива функція держави, вона означає: законодавче формування державної інформаційної політики; створення відповідно до законів України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної влади, громадянами та об'єднаннями громадян, іншими суб'єктами

права в Україні; гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України; всебічний розвиток інформаційної структури; підтримка розвитку національних інформаційних ресурсів України з урахуванням досягнень науки та техніки й особливостей духовно-культурного життя народу України; створення і впровадження безпечних інформаційних технологій; захист права власності держави та стратегічні об'єкти інформаційної інфраструктури України; охорону державної таємниці, а також інформації з обмеженим доступом, що є об'єктом права власності або об'єктом лише володіння, користування чи розпорядження державою; створення загальної системи охорони інформації, зокрема охорони державної таємниці, а також іншої інформації з обмеженим доступом; захист національного інформаційного простору України від розповсюдження спотвореної або забороненої для поширення законодавством України інформаційної продукції; встановлення законодавством режиму доступу іноземних держав або їх представників до національних інформаційних ресурсів на основі договорів з іноземними державами; законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території.

Інформаційну безпеку розглядають за трьома основними характеристиками: стан захищеності інформаційного середовища, суспільні відносини та захищеність установлених законом правил [2].

У науковій літературі поки бракує єдиного консолідованого погляду на зміст поняття «інформаційна безпека». Для одних воно відображає стан, для інших – процес, діяльність, здатність, систему гарантій, властивість, функцію. Це ще раз підтверджує необхідність в угрупуванні визначення аналізованого поняття. Найбільш прийнятним є інтегральний підхід, за якого інформаційна безпека визначатиметься за допомогою окреслення найбільш важливих її сутнісних ознак з урахуванням постійної динаміки інформаційних систем. Інформаційну безпеку слід розглядати через єдність ознак, таких як стан, властивість, а також управління загрозами і небезпеками, за яким забезпечується обрання оптимального шляху їх усунення і мінімізації впливу негативних наслідків. Невірним є зведення інформаційної безпеки до захисту інформації, це поняття є більш широким за своєю суттю. Це багатогранна сфера діяльності, що вимагає системно-комплексного підходу. Зробимо спробу узагальнити визначення цієї правової категорії. Отже, інформаційна безпека – це складник національної безпеки, процес управління загрозами та небезпеками, державними і недержавними інституціями, окремими громадянами, за яким забезпечується інформаційний суверенітет України, відбувається вдосконалення державного регулювання розвитку інформаційної сфери, йде впровадження новітніх технологій у цій сфері; внутрішній і світовий інформаційний простір наповнюється достовірною інформацією про Україну; засоби масової інформації залучаються до боротьби з корупцією, іншими явищами, що загрожують національній безпеці України; дотримання конституційного права громадян на свободу слова, доступу до інформації; невтручання будь-якого у діяльність засобів масової інформації; відсутність дискримінації в інформаційній сфері; захист національного інформаційного простору та протидій монополізації інформаційної сфери України. Це визначення є оптимальним та відображає усі аспекти взаємодії суб'єктів інформаційних відносин.

Здійснимо класифікацію видів інформаційної безпеки. За сферами суспільного життя існує інформаційна безпека в економічній, політичній, оборонній, екологічній та соціальній сферах тощо. Ця класифікація закріплена Законом України «Про Концепцію Національної програми інформатизації» та Доктриною інформаційної безпеки України. За аспектами розуміння інформаційної безпеки є інформаційно-психологічна безпека, інформаційно-технологічна (технологічна) безпека, інформаційна безпека у сфері прав і свобод людини. За видами інформаційної діяльності існує одержання інформації у встановленому порядку; забезпечення можливостей використання інформації; законне поширення інформації; належне зберігання інформації; захист інформації.

Окремо класифікуємо види інформаційної безпеки за змістовими елементами її забезпечення. Виділяють інформаційну безпеку особи, суспільства, держави – за об'єктами інформаційної безпеки. За суб'єктами забезпечення інформаційної безпеки існує: її міжнародне забезпечення (сприяння міжнародному співробітництву в галузі інформації, гарантування інформаційного суверенітету держави; сприяння задоволенню інформаційних потреб громадян за кордоном); державне забезпечення (діяльність державних організацій, спрямована на забезпечення інформаційної безпеки); недержавне забезпечення (діяльність громадських організацій та індивідів, спрямована на забезпечення інформаційної безпеки).

За характером предмета діяльності по забезпеченню інформаційної безпеки існує: протидія негативним процесам та явищам (загрозам небезпекам); сприяння посиленню позитивних процесів; сприяння трансформації нейтральних процесів у позитивні.

За засобами забезпечення інформаційної безпеки існує: правова регламентація; контрольно-наглядова діяльність; інженерно-технічне забезпечення; матеріально-технічне забезпечення.

З огляду на викладене можна виділити два найважливіші види інформаційної безпеки:

1) інформаційна безпека особистості – це захищеність психіки й свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо. Застосування Інтернет-технологій може викликати значні структурні та функціональні зміни у свідомості та психічній діяльності людини;

2) інформаційна безпека держави – це міра захищеності держави (суспільства) та стійкості основних сфер її життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) від дестабілізуючих інформаційних впливів. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.

Інформаційну безпеку можливо класифікувати відповідно до загроз, а саме:

– забезпечення безпеки діяльності, пов'язаної із забезпеченням свободи слова та доступу громадян до інформації;

– протидія поширенню засобами масової інформації культу насильства, жорстокості, порнографії;

– протидія намагання маніпулювання суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації;

– протидія комп'ютерній злочинності та комп'ютерному тероризму;

– забезпечення безпеки інформаційно-телекомунікаційних систем загального призначення;

– захист національних інформаційних ресурсів, у тому числі тих, доступ до яких здійснюється з використанням мережі Інтернет;

– забезпечення безпеки інформаційно-телекомунікаційних систем органів державної влади та місцевого самоврядування, інформаційно-телекомунікаційних систем, які функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави кредитно-банківських та інших сфер економіки держави, систем управління життєзабезпеченням;

– захист інформації, що становить державну та іншу, передбачену законом таємницю, конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства та держави.

Визначимо основні ознаки інформаційної безпеки держави:

– інформаційна система вступає як ознака стабільного, стійкого стану системи органів виконавчої влади, яка у разі впливу внутрішніх та зовнішніх загроз та небезпек зберігає суттєво важливі характеристики для власного існування;

– сама система інформаційної безпеки повинна мати такі характеристики: доступність – можливість за короткий час отримати необхідну інформаційну послугу будь-яким суб'єктом виконавчої влади; цілісність – актуальність і несуперечливість інформації, її захищеність від руйнування та несанкціонованої зміни; конфіденційність – захист від несанкціонованого ознайомлення;

– повинні бути забезпечені такі рівні інформаційної безпеки: нормативно-правовий – закони, нормативно-правові акти тощо; адміністративний – дії загального характеру, що вживаються органами виконавчої влади; процедурний – конкретні процедури забезпечення інформаційної безпеки; програмно-технічний – конкретні технічні заходи забезпечення інформаційної безпеки;

– інформаційна безпека – це вид інформаційної діяльності певних суб'єктів. Це така сфера державної діяльності, що пов'язана з безпекою людини, суспільства, а отже і держави за законодавчо визначеними параметрами (бажаний чи небажаний стан у просторі, часі й колі осіб);

– інформаційна безпека виявляється у співвідношенні між напрямами діяльності різних суб'єктів щодо інформації, вона постійно змінюється під впливом загроз, викликів, небезпеки, а тому є динамічним суспільним явищем;

– статус, обсяг, зміст інформаційної безпеки визначається Конституцією України, тут же визначається її пріоритет серед інших напрямів державної діяльності;

– інформаційна безпека особи, соціальних спільнот, держави є складником національного суверенітету;

– через створення кодексів можливе державне регулювання інформаційної сфери суспільства;

– держава повинна мати компетенцію щодо безпеки в інформаційній сфері суспільства, в подоланні конкуренції між різними гілками влади стосовно регулювання інформаційних процесів у соціальних відносинах;

– багатовекторною має бути політика у сфері інформаційної безпеки, що зумовлюється об'єктивною різнорідністю суспільних відносин щодо інформації [3].

Отже, можемо зазначити, що до суттєвих ознак інформаційної безпеки можна віднести конфіденційність (стан інформації, за якого доступ до неї отримують тільки суб'єкти, які мають на це право), цілісність (запобігання несанкціонованій або незаконній модифікації інформації) та доступність (запобігання тимчасового або постійного приховування інформації від користувачів, які отримали право на доступ). Можна виділити і такі ознаки, які не є обов'язковими, а саме: відмовостійкість (здатність посвідчити дію, яка мала місце, або подію так, що ці події не могли бути пізніше відкинуті), підзвітність, достовірність, автентичність.

Література

1. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навчальний посібник. Київ : Кондор, 2008. 384 с.

2. Марущак А.І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. *Державна безпека України.* 2011. № 21, С. 92–95.

3. Северина С.В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету.* 2016. № 1 (29), С. 155–161.

Анотація

Рогова Є. І. **Теоретичні основи правового забезпечення інформаційної безпеки.** – Стаття.

У статті проведено аналіз теоретичних основ правового забезпечення інформаційної безпеки. На основі проведеного аналізу сформовано висновки, що сьогодні інформаційна безпека в умовах глобалізації інформаційного простору потребує вироблення теоретико-правових, методологічних, концептуальних, доктринальних, стратегічних, тактичних та оперативних правових засобів, які будуть здатні урегулювати суспільні інформаційні відносини. Дослідження в юридичній науці підтверджують необхідність гармонізації законодавства про інформаційну безпеку у повному зв'язку з міжнародними правовими процесами.

На розгляд практиків можна запропонувати на обговорення таке формулювання інформаційної безпеки у правовому аспекті: розглядати інформаційну безпеку у триєдності – як сферу суспільних відносин, як підгалузь інформаційного права, як навчальну дисципліну; за правовим змістом розглядати інформаційну безпеку можна як сферу суспільних відносин щодо підтримки на нормативно визначеному рівні співвідношення прав і обов'язків особи, суспільства, держави в інформаційному просторі від загроз, викликів їх суверенітету.

Якщо розглядати інформаційну безпеку як соціальне явище, то можна запропонувати визначити поняття та сутність її таким чином: це суспільні відносини щодо створення і підтримання в належному стані режиму інформаційної системи, систем телекомунікації; комплекс заходів щодо охорони, захисту, запобігання і подолання природних і соціогенних загроз.

На цей час залишається нерозв'язаною задача розроблення теоретичних основ забезпечення інформаційної безпеки України. Водночас відсутні визначення багатьох взаємопов'язаних понять інформаційної сфери: «державна інформаційна політика», «інформаційний ресурс», «інформаційна безпека», «кібернетична безпека» тощо. Є потреба удосконалення чинного законодавства України, зокрема, базового термінологічного положення щодо визначення поняття «інформаційна безпека». Одним з варіантів вирішення вищевказаних проблем є розроблення Інформаційного Кодексу України. Крім того багатьма науковцями вже обґрунтовувався досить широкий спектр термінів, уживаних у контексті інформаційної безпеки.

Ключові слова: інформація, інформаційна безпека, теоретичні основи, правове забезпечення, інформаційний простір, кібернетична безпека.

Summary

Rogova E. I. **Theoretical fundamentals of legal provision of information security.** – Article.

The article analyzes the theoretical foundations of legal information security. Based on the analysis, it is concluded that today information security in the globalization of the information space requires the development of theoretical and legal, methodological, conceptual, doctrinal, strategic, tactical and operational legal means that will be able to regulate public information relations. Research in legal science confirms the need to harmonize information security legislation in full connection with international legal processes.

Theoretical foundations of legal information security in the scientific literature are revealed ambiguously. A large number of sources state that the concept of "information security" arises with the advent of information communication between people. Ensuring information security of Ukraine is the most important function of the state, the business of the entire Ukrainian people, based on this, the theoretical foundations of legal information security are subject to painless definition and interpretation, both in the scientific literature and at the legislative level.

Despite their significant contribution of practitioners and theorists in the field of theoretical foundations of legal information security, it is impossible to assume that all issues in this area have been resolved.

Practitioners can consider the following formulation of information security in the legal aspect: to consider information security in the trinity – as a sphere of public relations, as a sub-branch of information law, as a discipline; According to the legal content, information security can be considered as a sphere of public relations to maintain at a normatively defined level the relationship of rights and responsibilities of the individual, society, state in the information space from threats, challenges to their sovereignty.

If we consider information security as a social phenomenon, we can propose to define its concept and essence as follows: it is public relations to create and maintain in good condition the regime of the information system, telecommunications systems; a set of measures for the protection, defense, prevention and overcoming of natural and sociogenic threats.

In the legislative field of Ukraine, unfortunately, there is no framework law on information security of the state, the absence of information security is defined in the Law of Ukraine "On the basic principles of information society development in Ukraine for 2007–2015".

Today, the task of developing the theoretical foundations of information security of Ukraine remains unsolved. However, there are no definitions of many interrelated concepts in the information sphere: "state information policy", "information resource", "information security", "cyber security" etc. There is a need to improve the current legislation of Ukraine, in particular, the basic terminological provisions for defining the concept of "information security". One of the options for solving the above problems is the development of the Information Code of Ukraine, in addition, many scholars have already substantiated a wide range of terms used in the context of information security.

Key words: information, information security, theoretical foundations, legal support, information space, cyber security.