

## РОЗДІЛ 7

### АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 342.6:342.922(477)

DOI <https://doi.org/10.32782/2524-0374/2022-6/51>

#### СУБ'ЄКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

#### SUBJECTS OF INFORMATION SECURITY IN UKRAINE

Баран М.В., здобувачка кафедри адміністративно-правових дисциплін

*Львівський державний університет внутрішніх справ*

Стаття присвячена висвітленню однієї з актуальних теоретичних проблем інформаційного права щодо класифікації суб'єктів забезпечення інформаційної безпеки України. При дослідженні суб'єктів забезпечення інформаційної безпеки застосовано факторний аналіз з використанням системного та діяльничого підходу, що дало можливість в умовах розвитку інформаційного суспільства, впровадження новітніх інформаційно-комунікаційних технологій дати характеристику новим суб'єктам забезпечення інформаційної безпеки. Метою дослідження є систематизація суб'єктів забезпечення інформаційної безпеки у контексті характеристика їх сутності та створення класифікації на підставі чинного інформаційного законодавства у зазначеній сфері діяльності. Проаналізовано теоретичні підходи до визначення сутності поняття класифікація суб'єктів забезпечення інформаційної безпеки. Акцентовано увагу на міждисциплінарності дослідження проблем визначення суб'єктів інформаційної безпеки, що сприяє багатоаспектному розумінню та дозволяє спрямувати зусилля на створення належного правового та нормативного підґрунтя класифікації досліджуваного феномену. Визначено коло суб'єктів забезпечення інформаційної безпеки України та розглянуті адміністративно-правові засади діяльності щодо різних підходів при класифікації суб'єктів, які досліджуються. Зазначено, що для забезпечення інформаційної безпеки як суб'єктно-комунікативної системи характерний свій особливий спосіб взаємодії. Вказано, що розвиток правового регулювання діяльності суб'єктів забезпечення інформаційної безпеки повинен базуватися на широкому підході до класифікації суб'єктів. Це дасть можливість уніфікувати теоретичні погляди щодо суб'єктів, які досліджуються та можливості усунення прогалів у правовому регулюванні діяльності щодо забезпечення інформаційної безпеки в умовах розвитку цифрової економіки та інтеграції в інформаційний простір Європейського Союзу.

**Ключові слова:** безпека, інформаційне право, органи публічної влади, класифікація суб'єктів, правосуб'єктність.

The article is devoted to the coverage of one of the current theoretical problems of information law regarding the classification of subjects of information security of Ukraine. In the study of the subjects of information security applied factor analysis using a systematic and operational approach, which allowed in the development of the information society, the introduction of new information and communication technologies to characterize the new subjects of information security. The purpose of the study is to systematize the subjects of information security in the context of the characteristics of their essence and to create a classification based on current information legislation in this area. Theoretical approaches to defining the essence of the concept of classification of information security entities are analyzed. Emphasis is placed on the interdisciplinary study of the problems of identifying the subjects of information security, which promotes multifaceted understanding and allows focusing efforts on creating an appropriate legal and regulatory basis for the classification of the phenomenon under study. The range of subjects of information security of Ukraine is determined and the administrative and legal bases of activity concerning various approaches at classification of the subjects, which are investigated, are considered. It is noted that to ensure information security as a subject-communicative system is characterized by its own special way of interaction. It is stated that the development of legal regulation of the activities of information security entities should be based on a broad approach to the classification of entities. This will provide an opportunity to unify theoretical views on the subjects under study and the possibility of eliminating gaps in the legal regulation of information security in the digital economy and integration into the information space of the European Union.

**Key words:** security, information law, public authorities, classification of subjects, legal personality.

Економічний розвиток України детермінує ряд процесів у галузі науки, культури, освіти, формує цілісну систему соціального організму держави. Стійкий розвиток та функціонування цифрової економіки в умовах європейської інтеграції вимагає єдиного підходу до вирішення багатьох питань забезпечення інформаційної безпеки у сферах державного, економічного, соціально-культурного будівництва та правового регулювання. Це зумовлює необхідність забезпечення єдності суб'єктів інформаційної безпеки, їх ефективну взаємодію у вигляді цілого комплексу юридичних інструментів – правового статусу, правоздатності та дієздатності, суб'єктивних прав і юридичних обов'язків, юридичної відповідальності.

Системність, логічність, встановлення у законодавстві правового становища суб'єктів інформаційної безпеки свідчить про рівень правової культури у суспільстві, виступають важливою гарантією проти правозастосовного волонтаризму і бюрократичного свавілля. Оскільки законодавство є підсумковим продуктом законотворчої діяльності, досягнення такого якісного рівня передбачає вдосконалення законотворчої діяль-

ності, оновлення правових норм, які закріплюють статус суб'єктів права, їхню правоздатність та дієздатність, а також юридичну відповідальність. Розвиток наукових досліджень щодо суб'єктів інформаційної безпеки за умов трансформації права є важливим для розвитку теорії права та для галузевого законодавства, зокрема інформаційного права.

Досліджень питань правового статусу суб'єктів інформаційного права, у тому числі суб'єктів інформаційної безпеки здійснювали: В. Б. Авер'янов, І. В. Арістова, О. О. Баранов, Н. П. Бортник, К. В. Бондаренко, В. М. Брижко, В. М. Гарашук, Т. О. Гаврилюк, Р. А. Каложний, Л. П. Коваленко, Б. А. Кормич, В. С. Цимбалюк, В. О. Шамрай, Ю. С. Шемшученко та інші вчені.

В юридичній науці проблема суб'єкта права розглядається у рамках загальної теорії держави і права та на рівні галузевих наук. Теоретичні розробки не вичерпали аналізованої проблеми. Необхідність теоретичного аналізу суб'єктів забезпечення інформаційної безпеки викликана відсутністю ясною та послідовною класифікацією видів даних суб'єктів, їх організаційно-правових форм, єдності

у поглядах щодо правоздатності та дієздатності індивідуальних і колективних суб'єктів.

**Метою статті** є дослідження суб'єктів правового забезпечення інформаційної безпеки в Україні.

Інформаційна безпека – це сукупність заходів організаційного, технічного та правового характеру внутрішнього і зовнішнього напрямів. Внутрішній напрям пов'язаний із забезпеченням інформаційної безпеки у процесі реалізації фізичними та юридичними особами інформаційної діяльності. Зовнішній напрям полягає у забезпеченні інформаційної безпеки особи, суспільства та держави, що досягається шляхом підвищення ефективності використання інформаційної інфраструктури на користь соціально-економічного розвитку суспільства та держави і задоволення законних інформаційних інтересів особи.

Перспективним методом вивчення суб'єктів забезпечення інформаційної безпеки є факторний аналіз на підставі системного підходу. Система суб'єктів вказаного виду діяльності сприймається як єдина цілісна сукупність суб'єктів різних категорій (фізичних і юридичних осіб, приватноправових і публічно-правових), що перебувають у стані структурно-функціональних зв'язків з метою забезпечення оптимальної діяльності у межах правових відносин.

Кожна організаційно-правова форма юридичної особи структурно та функціонально доповнює інші форми, суб'єкти приватного права реалізують юридичні можливості при безпосередній взаємодії з публічно-правовими утвореннями у сфері забезпечення інформаційної безпеки, індивідуальні суб'єкти, поєднуючи зусилля, утворюють складні, багатоскладові суб'єкти права.

Встановлення системи суб'єктів забезпечення інформаційної безпеки забезпечується відповідною системною правовою регламентацією у законодавстві, яке постійно розвивається, доповнюючи існуючу систему новими суб'єктами.

Суб'єкт забезпечення інформаційної безпеки це фізична чи юридична особа, яка за своїми особливостями фактично є носієм суб'єктивних юридичних прав і обов'язків через юридичні норми, а також потенційно здатна сама або через своїх представників брати участь у правовідносинах.

Категорії, які характеризують суб'єкта забезпечення інформаційної безпеки, «суб'єкт права», «правосуб'єктність» та «правовий статус» – самостійні діалектично взаємопов'язані категорії. Суть правосуб'єктності у тому, що вона визначає ті юридично значимі показники, володіння якими створює реальне персонально індивідуалізоване визначення власника правового становища. Правосуб'єктність слід представляти як своєрідну правову конструкцію між реальною особою і статусом суб'єкта права. Ця правова конструкція відбиває склад юридичних фактів, наявність яких дозволяє конкретній фізичній або юридичній особі виступити як володар відповідного правового становища.

Класифікація суб'єктів інформаційного права, як зазначає юридична наука характеризується різноманітністю, проте основною точкою зору у науці залишається уявлення про необхідність виділення загально-правових суб'єктів.

Відповідно при класифікації суб'єктів забезпечення інформаційної безпеки необхідно враховувати вид здійснюваної інформаційної діяльності (функціонально-діяльнісний критерій), правова природа якого залежить від об'єкта, з приводу якого формується інформаційна взаємодія (об'єктний критерій). Головна особливість інформаційної діяльності полягає в тому, що вона носить комплексний характер, так як пронизує всі зрізи простору суспільних відносин – приватні та публічні, матеріальні та процесуальні, внутрішньодержавні та міжнародні.

Усі види інформаційної діяльності здійснюються приватними особами, державою, органами місцевого

самоврядування. Інформаційна діяльність складається з публічної інформаційної діяльності та інформаційної діяльності приватних суб'єктів.

В умовах розвитку цифрової економіки та необхідності забезпечення інформаційної безпеки доцільно говорити про широке коло нових суб'єктів інформаційних правовідносин. При класифікації суб'єктів інформаційних правовідносин у сфері інформаційної безпеки потрібен аналіз нормативно-правових актів, які регулюють інформаційну сферу, а також відповідних доктринальних положень і концепцій, у першу чергу Стратегії інформаційної безпеки України, Стратегії кібербезпеки України, Закону України «Про національну безпеку України» [1–3].

В Україні політика у сфері забезпечення інформаційної безпеки на рівні держави формується та реалізується центральними та регіональними органами, спеціалізованими організаціями та підприємствами. Законодавством України визначено організаційну основу системи забезпечення інформаційної безпеки, принципи, механізми, напрями діяльності [4].

До суб'єктів належать: державні органи, державні установи, юридичні особи та фізичні особи-підприємці, яким на праві власності, оренди або на іншій законній підставі належать інформаційні системи, інформаційно-комунікаційні мережі, автоматизовані системи управління, що функціонують у сфері охорони здоров'я, науки, транспорту, зв'язку, банківській сфері та інших сферах фінансового ринку, енергетичного комплексу, в галузі атомної енергії, оборонної, космічної, металургійної та хімічної промисловості, юридичні особи та фізичні особи-підприємці, які забезпечують взаємодію зазначених систем чи мереж.

У даний час сформувалася певна ієрархічна система суб'єктів, пов'язаних із забезпеченням безпеки в інформаційній сфері, яку очолює Президент України (відповідно до п. 17 статті 106 Конституції України). Ряд функцій щодо інформаційної безпеки покладено на Раду національної безпеки і оборони України, як конституційного дорадчого органу, закріплено у Законі України «Про Раду національної безпеки і оборони України» [5; 6].

До компетенції Ради національної безпеки і оборони віднесено розгляд питань забезпечення національної безпеки, проведення стратегічної оцінки на основі аналізу інформації про стан інформаційної безпеки України та розвиток інформаційного суспільства в Україні.

Серед суб'єктів зазначеної системи слід зазначити Верховну Раду України, яка безпосередньо займається законодавчою діяльністю; органи судової влади; органи виконавчої влади центрального рівня; органи, які здійснюють контроль та нагляд за виконанням законодавства іншими органами виконавчої влади повноважень та законів; державні та міжвідомчі комісії; місцеві органи представницької та виконавчої влади; органи місцевого самоврядування; громадяни та громадські об'єднання, які беруть участь у цій роботі відповідно до законодавства.

До суб'єктів забезпечення інформаційної безпеки відпасає Кабінет Міністрів відповідно до Закону України «Про Кабінет Міністрів України» [7].

У системі суб'єктів забезпечення інформаційної безпеки слід особливо відзначити такі центральні органи виконавчої влади, як Міністерство економіки України та Міністерство цифрової трансформації України, які мають завдання та функції у сфері розвитку електронних комунікацій, цифровізації та розвитку цифрової економіки.

Міністерство цифрової трансформації може виступати як орган у сферах електронних довірчих послуг, електронної ідентифікації, інвестицій в ІТ-індустрію та орган виконавчої влади, що здійснює функції з вироблення та реалізації державної політики, нормативно-правового регулювання у сфері інформаційних технологій.

Особливий статус щодо забезпечення інформаційної безпеки закріплюється за центрами надання адміністративних послуг.

Служба безпеки України здійснює повноваження щодо забезпечення інформаційної безпеки, безпосередньо реалізує основні напрями діяльності органів безпеки (наприклад, криптографії та захисту інформації, критичної інформаційної інфраструктури).

Державна служба України спеціального зв'язку та захисту інформації та підпорядковані регіональні органи мають повноваження у галузі технічного захисту інформації, здійснюють планові та позапланові перевірки об'єктів критичної інформаційної інфраструктури, організації спеціального зв'язку та захисту інформації в органах публічної влади.

Національний банк України має повноваження щодо забезпечення інформаційної безпеки у фінансово-кредитній сфері.

Діяльність уповноважених органів виконавчої влади, як суб'єктів забезпечення інформаційної безпеки полягає у здійсненні функцій контролю та нагляду в інформаційному просторі. Діяльність спрямована на зміст інформації, що розповсюджується або на техніко-технологічний ресурс.

Закон України «Про стимулювання розвитку цифрової економіки в Україні» визначає організаційні, правові та фінансові засади функціонування правового режиму Дія Сіті, що запроваджується з метою стимулювання розвитку цифрової економіки в Україні шляхом створення сприятливих умов для ведення інноваційного бізнесу, розбудови цифрової інфраструктури, залучення інвестицій, а також талановитих спеціалістів [8]. Нормативний акт вводить нових суб'єктів в інформаційне права, у тому числі у сфері забезпечення інформаційної безпеки.

Стаття 4 Закону України «Про інформацію» зазначає, що суб'єктами інформаційних відносин є: фізичні особи; юридичні особи; об'єднання громадян; суб'єкти владних повноважень.

У понятійному апараті Закону України «Про захист інформації в інформаційно-комунікаційних системах» закріплено визначення ряду суб'єктів у мережі Інтернет: власника сайту, власника інформації та ін. [9].

Відповідно до Закону України «Про доступ до публічної інформації» суб'єктами інформаційних правовідносин є органи, які мають публічну інформацію, до яких можна віднести Україну, органи державної влади, місцеві органи влади та органи місцевого самоврядування. Зазначені вище суб'єкти інформаційних правовідносин безпосередньо мають відношення до забезпечення інформаційної безпеки [10].

У даному випадку доцільно розглядати багаторівневу класифікацію суб'єктів забезпечення інформаційної безпеки.

Законодавець виділяє такі категорії суб'єктів як фізичні особи та юридичні особи. У рамках кримінально-правових відносин існує певна класифікація суб'єктів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, які зазначені у розділі 16 Кримінального кодексу України [11].

В. В. Філатов зазначає, що необхідно узагальнення уявлень про систему суб'єктів забезпечення інформаційної безпеки, зокрема тих, які з'явилися останнім часом. Мова йде не тільки про їхню класифікацію, а й чітке розмежування обсягу та особливостей правового статусу. Потреба у такому узагальненні обумовлена науково-технічним прогресом [12, с. 55].

Вчений виділяє наступних суб'єктів: юридичні та фізичні особи, які виробляють та споживають інформацію; фізичні та юридичні особи, які розробляють і застосовують інформаційні системи, технології та засоби забезпечення, підприємства та установи органи державної

влади та місцевого самоврядування, юридичні особи, що формують інформаційні ресурси.

Т. С. Перун вважає, що для забезпечення інформаційної безпеки характерна багаторівнева система суб'єктів, заснована на принципі єдності та диференціації. Перший рівень – це три групи суб'єктів: фізичні і юридичні особи, публічно-правові утворення, складові підсистеми цих суб'єктів. Інші рівні (структурні елементи зазначених підсистем) це різного роду спеціальні суб'єкти адміністративного права, поділ яких обумовлено диференціацією предмета відповідного правового регулювання [13, с. 140–149].

На нашу думку не можна визнати наведену класифікацію вичерпною, оскільки до неї не включено низку суб'єктів інформаційних правовідносин – загальних (міжнародні організації та регіональні громадські об'єднання, органи місцевого самоврядування), та спеціальних (інформаційний посередник, центри надання адміністративних послуг тощо).

Автори статті «Розвиток цифрової економіки в контексті забезпечення інформаційної безпеки в Україні», досліджуючи відносини у сфері міжвідомчої електронної взаємодії, виділяє як суб'єктів забезпечення інформаційної безпеки: центральні органи виконавчої влади, державні позабюджетні фонди, місцеві виконавчі органи державної влади, органи місцевого самоврядування, державні та комунальні установи, центри надання адміністративних послуг, інші органи та організації [14, с. 2027].

Автори статті «Гарантії прав людини та громадянина при забезпеченні інформаційної безпеки» вказують, що на тенденцію появи раніше невідомих суб'єктів інформаційно-правових відносин, різноманітних посередників, яких можна розділити на два види: традиційних інформаційних посередників (наприклад, операторів пошукової системи, блогерів, інсайдерів, реєстраторів доменних імен) та торгових інформаційних посередників [15, с. 1011]. До останніх можна віднести великі мережеві майданчики, організаторів торгівлі. Зазначені суб'єкти забезпечують інформаційну безпеку у межах визначених чинним законодавством.

Важливою категорією суб'єктів забезпечення інформаційної безпеки є оператори – у законодавстві їх видів налічується понад сорок (наприклад, можна виділити наступні: оператори, що займають домінуюче становище у мережах загального користування; оператори зв'язку; оператори універсального обслуговування; оператори обов'язкових загальнодоступних телеканалів та (або) радіоканалів; оператори реєстру; оператори інформаційної системи, оператори пошукової системи; оператори персональних даних; оператори національної платіжної системи).

Спеціальним суб'єктом є оператор електронних комунікацій та постачальник електронних комунікаційних мереж або послуг. Відповідно до Закону України «Про електронні комунікації» оператор електронних комунікацій (оператор) – суб'єкт господарювання, який володіє, здійснює експлуатацію та управління електронними комунікаційними мережами та/або пов'язаними засобами; постачальник електронних комунікаційних послуг – суб'єкт господарювання, який фактично надає та/або має право надавати електронні комунікаційні послуги на власних мережах та/або на мережах інших постачальників електронних комунікаційних послуг [16].

Основна діяльність операторів пов'язана із забезпеченням доступу до комунікаційних мереж інших суб'єктів, вони мають технологічні можливості щодо припинення правопорушень в Інтернеті. Зазначені суб'єкти різняться за особливостями інформаційної сфери взаємодії з іншими учасниками інформаційного обміну, функціональним особливостям і правовим статусом, обсягом прав і обов'язків у сфері забезпечення інформаційної безпеки.

Можна назвати особливості правового статусу інших категорій суб'єктів. Наприклад, заслуговує на увагу такий суб'єкт, як адвокати, оскільки вони несуть відповідальність за адміністративне правопорушення як посадові особи. Правовий статус низки суб'єктів щодо критичної інформаційної інфраструктури визначено у Законі України «Про критичну інфраструктуру» [17].

Широкий підхід до класифікації суб'єктів забезпечення інформаційної безпеки необхідний для розвитку правового регулювання питань відповідальності, уніфікації теоретичних поглядів на суб'єктів, які досліджуються і можливості усунення прогалин правового регулювання. Класифікація суб'єктів забезпечення інформаційної безпеки не вичерпується вище зазначеними підходами.

**Висновки.** Різноманіття суб'єктів забезпечення інформаційної безпеки обумовлено значною кількістю критеріїв розрізнення особливих правових властивостей, функцій, мети діяльності, організації діяльності. Кожна класифіка-

ція має особливу цінність за умови, що застосовна у практиці правового регулювання та правозастосування, у теорії юриспруденції.

Необхідна розробка різних науково обґрунтованих класифікацій суб'єктів забезпечення інформаційної безпеки з більш широких підстав. Класифікація суб'єктів забезпечення інформаційної безпеки дозволить уникнути термінологічної невизначеності, не лише врахувати існуючих учасників інформаційної взаємодії, а й передбачити появу нових, органічно включити у інформаційно-правовий простір. В результаті буде забезпечено стійкість та актуальність нормативно-правових положень, що, у свою чергу, має гарантувати ефективність правового регулювання.

Перспективи дослідження цієї актуальної теми пов'язані з подальшою науковою розвідкою суб'єктів забезпечення інформаційної безпеки та виробленням рекомендацій, які б допомогли максимально повно реалізувати розроблені у документах стратегічного планування концепти на практиці.

#### ЛІТЕРАТУРА

1. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021>
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 р. № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021>
3. Про національну безпеку України: Закон України від 21.06.2021 р. № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/card/2469-19>
4. Малашко О. Є., Єсімов С. С. Зміст державної діяльності із забезпечення інформаційної безпеки. *Міжнародний науковий журнал «Інтернаука»*. 2020. № 15 (95). Т. 1. С. 46–54. URL: <https://www.inter-nauka.com/issues/2020/15/>
5. Конституції України: Закон України від 28.06.1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>
6. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 р. № 183/98-ВР. URL: <https://zakon.rada.gov.ua/laws/card/183/98-вр>
7. Про Кабінет Міністрів України: Закон України від 27.03.2014 р. № 794-VII. URL: <https://zakon.rada.gov.ua/laws/card/794-18>
8. Про стимулювання розвитку цифрової економіки в Україні: Закон України від 15.07.2021 р. № 1667-IX. URL: <https://zakon.rada.gov.ua/laws/show/1667-20#Text>
9. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/card/80/94-вр>
10. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
11. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. URL: <https://zakon.rada.gov.ua/laws/card/2341-14>
12. Філатов В. В. Доктрина інформаційних правовідносин в умовах державної політики перехідного періоду в Україні. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2021. № 1. С. 53–57.
13. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис. ... канд. юрид. наук: спец.: 12.00.07. Львів, 2019. 268 с.
14. Єсімов С., Ковалів М., Скриньковський Р., Сопільник Р. Гарантії прав людини та громадянина при забезпеченні інформаційної безпеки. *Traektoriâ Nauki = Path of Science*. 2018. Vol. 4. № 5. S. 1008–1016.
15. Сопільник Л., Ковалів М., Єсімов С., Скриньковський Р. і інші. Розвиток цифрової економіки в контексті забезпечення інформаційної безпеки в Україні. *Traektoriâ Nauki = Path of Science*. 2020. Vol. 6. № 5. S. 2023–2032.
16. Про електронні комунікації: Закон України від 16.12.2020 р. № 1089-IX. URL: <https://zakon.rada.gov.ua/laws/card/1089-20>
17. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>