Міністерство освіти і науки України
Київський університет імені Бориса Грінченка

А.Ю. Нашинець-Наумова

ІНФОРМАЦІЙНА БЕЗПЕКА: ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ

Монографія

Київ
2017

УДК 342.95:004.056
ББК 67.301.1
Н 37

Рекомендовано до друку Вченою радою
Факультету права та міжнародних відносин
Київського університету імені Бориса Грінченка
(протокол №2 від 8 листопада 2016 р.)

Рецензенти:

***П.В. Діхтієвський**, доктор юридичних наук, професор, професор кафедри адміністративного права Юридичного факультету Київського національного університету імені Т.Г. Шевченка.*

***В.К. Колпаков**, доктор юридичних наук, професор, завідувач кафедри адміністративного та господарського права Запорізького національного університету.*

Нашинець-Наумова А.Ю.

Н 37 Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. – Київ: Видавничий дім «Гельветика», 2017. – 168 с.

ISBN 978-966-916-176-5

У монографії розглядаються загальнонаукові категорії інформаційної безпеки в Україні та в світі. Авторка акцентує увагу на особливостях функціонування системи інформаційної безпеки. Окремо досліджуються питання захисту інсайдерської інформації суб'єктів господарювання.

Розраховано на викладачів, аспірантів та студентів.

УДК 342.95:004.056
ББК 67.301.1

ISBN 978-966-916-176-5

ЗМІСТ

ВСТУП

Інформаційна безпека – це правове поняття. Їм позначається стан захищеності національних інтересів України в інформаційній сфері, що визначається сукупністю збалансованих інтересів особистості, суспільства і держави. Забезпечення інформаційної безпеки – сфера державного, політичного управління, вища форма свідомого регулювання процесами функціонування самої державної системи. Інформаційна безпека здатна до розвитку і саморозвитку, тому будь-яке наукове знання про неї набуває актуального значення.

Проблемний характер функціонування політичної влади в Україні, необхідність налагодження механізму поділу державної влади, перетворення її з поля боротьби різних політичних сил в силу, консолідуючу суспільство, дефіцит суспільної згоди щодо цілей і змісту реформування самої держави і суспільства – все це робить науковий аналіз сучасної практики державного забезпечення інформаційної безпеки в різних сферах суспільно-політичного життя, особливо в сферах захисту цілісності та незалежності самої держави, виключно необхідним з точки зору нового бачення перспектив розвитку, вдосконалення держави як політико-вольового центру країни. Характеризуючи сучасний політичний стан нашої країни, Президент України П. Порошенко зазначив: «Ми всі розуміємо, що сьогодні йде війна за нашу незалежність. І якщо в умовах миру головне – забезпечення принципів демократії, свободи слова, закріплення європейських цінностей, то сьогодні на перший план вийшли питання інформаційної безпеки» [1].

Ефективність здійснення влади в будь-якій державі, в тому числі і в Україні, в чималому залежить від його інформаційного забезпечення. Без інформації неможливо уявити позитивно функціонуючу політичну структуру, розвиток масової політичної свідомості, взаємодію суб'єкта та об'єкта політики. В процесі інформаційно-комунікативного впливу у свідомості народу формується образ державної влади, його політичних інститутів та лідерів, а керуючі функції держави здійснюються з найбільшим потенціалом і найменшими енергетичними

затратами лише тоді, коли досить добре розвинена система інформаційних зв'язків між державою, громадянським суспільством і особистістю. У сучасному суспільстві інформаційні технології є однією з найважливіших рушійних сил соціальних змін. У вітчизняній науці зростає інтерес до вивчення перспектив формування інформаційного суспільства в Україні. Широке коло проблемних явищ пов'язаний з інформаційною безпекою особистості, суспільства, держави.

Дослідження інформаційного суспільства як науковий напрям сформувалося порівняно недавно і гуманітарні науки перебувають лише на підступах до його пізнання. Відзначимо, що всі провідні країни світу сформулювали свою політику і стратегію його побудови та розвитку. У всіх прийнятих програмах в якості окремих глав ставляться питання правового регулювання питань інформаційної безпеки. Це об'єктивно актуалізує теоретичну і практичну роботу, спрямовану на вирішення наукових задач, пов'язаних безпосереднім чином з формуванням інформаційного суспільства в Україні.

Інформаційна безпека – міждисциплінарна проблема. Як науковий напрямок, вона має кілька аспектів, зокрема, правовий, управлінський, економічний, психологічний, культурологічний, організаційно-технічний та інші. Однак за останній час, коли в геополітичному просторі світу інформаційні технології та інформація в цілому отримали визначальне значення, правовий аспект вивчення інформаційної безпеки особистості, суспільства і держави виходить на перший план. Характер і зміст політичних процесів, структура політичних, економічних, правових, інформаційних та інших відносин в суспільстві, що реформується, становить на сьогоднішній день складний конгломерат взаємодій і взаємовпливів різних сил, які вимагають пильного вивчення і осмислення. Головним регулятором цих взаємодій є Конституція України, яка містить основні стандарти сучасної демократії, її цінності. Цей документ став основним політичним джерелом сучасного українського права, в ньому викладені магістральні напрями становлення і розвитку України як правової держави. Конституція України містить норми, що стали основою будівництва нової державності. Закладаючи основи демократизації усього життя українського суспільства, вона відкриває тим самим для України широкі перспективи

міжнародної правосуб'єктності як у світовому, так і континентальному масштабі. Україна приєдналася до основоположних конвенцій Ради Європи, є повноправним членом ОБСЄ і готова до широкого співробітництва з багатьох політичних, економічних питань, а також з питань безпеки. Проблема безпеки країн і народів продовжує залишатися злободенною і диктує необхідність серйозної перегрупування сил.

Військова агресія Росії, спрямована на насильницьке протиправне відторгнення Кримської автономії та Севастополя від України та їх приєднання до Російської Федерації на правах суб'єкта Російської Федерації, що було здійснено протягом березня 2014 року, військове вторгнення Росії на Донбас, падіння літака «Боїнг-777» Малайзійських авіаліній та багато інших подій подібного роду, що відбулися в нашій країні, розкрили очевидну неспроможність колишньої структури національної безпеки, що створювалася для нейтралізації загроз, характерних для «холодної війни».

Виникли нові виклики і загрози, що ставлять світ на межу катастрофи: міжнародний тероризм; організована злочинність; незаконний обіг наркотиків і зброї; расова нетерпимість; релігійний фанатизм; політичний екстремізм; агресивний сепаратизм. Виникають загрози і в такій важливій сфері міжнародного співробітництва, інтеграції всього світового співтовариства, як інформаційна. Інформація має пряме відношення до політичних процесів в сучасному світі. Результати розвитку інформаційних технологій дозволяють сподіватися на створення динамічної світової інформаційної моделі. Всі останні роки неймовірно зростала інтенсивність споживання інформації в усіх сферах життєдіяльності людини і суспільства – соціальній, науково-технічній, технологічній, статистичній, економічній та ін. Процеси збору, накопичення, переробки та розповсюдження інформації стають необхідною умовою існуючих структур політичного та іншого управління, здійснення ефективних політичних впливів, вирішення масштабних економічних задач.

Однак інформація – це не тільки сила, що створює. На жаль, вона володіє дестабілізуючим потенціалом для суспільства, якщо її практично необмежені можливості впливу на людину і суспільство використовуються в інтересах коаліційних

співтовариств, окремих держав, політичних угруповань чи окремих осіб. Досвід новітньої історії світу визначив очевидність: інформація може стати джерелом політичної та соціальної загроз. Цим викликана необхідність державно-правового та громадського регулювання інформаційними потоками, зокрема, діяльністю засобів масової інформації. Саме з цього приводу президент України П. Порошенко провів зустріч з членами Національної Ради з питань телебачення та радіомовлення, де наголосив, що Нацрада має зайняти жорстку позицію у галузі інформаційної безпеки, оскільки проти України постала «надзвичайно добре розроблена пропагандистська машина». «Населення Донбасу потребує правдивої інформації про Україну», – підкреслив Президент.

Розділ 1
КОНЦЕПТУАЛЬНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Інформаційна безпека як загальнонаукова категорія

Сьогодні незадовільність стану українського інформаційного законодавства та необхідність термінових заходів щодо його удосконалення є очевидними. Однак єдності у шляхах якісної трансформації інформаційного законодавства України серед дослідників цієї проблематики не існує, що є логічним, зважаючи на складність, динаміку та масштабність сучасних інформаційних процесів, які відбуваються в умовах становлення національної правової системи [2, с. 252].

Не можна не погодитися з думкою В. Горбуліна та М. Биченка про те, що однією з основних причин невідповідності інформаційного законодавства України вимогам сучасності є несформованість у суспільній і науковій думці цілісного уявлення про інформаційну безпеку з позиції права та юридичної науки. Тому системний підхід до формування права й нормотворчості є актуальним завданням, зумовленим відсутністю належної систематизації чинного інформаційного законодавства. За відсутності методологічних засад інформаційного нормотворення виникають труднощі об'єктивного і суб'єктивного характеру при формуванні системи нормативно-правового регулювання інформаційної безпеки [3, с. 89]. Важливим підґрунтям удосконалення інформаційного законодавства є адекватне сучасним умовам відображення у свідомості нормотворців інформаційної безпеки у всій повноті аспектів, зокрема психологічному, технічному та правовому.

Очевидно, що інформаційна безпека не є явищем найвищого порядку і може розглядатися тільки ґрунтуючись на парадигмі соціальної безпеки, використовуючи її методологічний потенціал. Тому доцільним є з'ясування поняття «безпека» як базової категорії для дослідження інформаційної безпеки. Оскільки безпека за своєю сутністю є соціальним явищем, то

серед усього розмаїття поглядів необхідно звернути увагу на філософсько-соціологічне розуміння, яке має стати фундаментальною частиною системного підходу до розуміння явища безпеки, що дозволить на науковому (доктринальному) рівні уникнути використання у визначеннях таких неоднозначних і суперечливих понять, як «захищеність», «інтереси», «потреби» та «загрози», відобразивши при цьому синергетичний бік явища безпеки [2, с. 253]. Підґрунтя такого підходу окреслене Г. Іващенком. Наголошуючи на недосконалості загальнопоширеного визначення безпеки через стан захищеності життєво важливих інтересів особи, суспільства і держави від внутрішніх та зовнішніх загроз, він зазначає, що основою усвідомлення його повинен стати діяльнісний підхід, напрацьований соціальною філософією та теоретичною соціологією. Однак це не означає, що безпеку можна формально розуміти як вид діяльності у відриві від її результатів, умов, у яких вона здійснюється, та можливостей функціонування суб'єкта в цих умовах. З цієї позиції безпеку пропонується розглядати як «сукупність умов існування суб'єкта, якими він оволодів (осягнув, засвоїв, створив) у процесі самореалізації, і які він, таким чином, здатний контролювати» [4, с. 58]. Тут слід наголосити, що в синергетичному аспекті простежується певна взаємозалежність умов існування суб'єкта та здатностей або можливостей їх контролю. Умови існування можуть виступати стимулом розвитку здатностей та підвищення спроможності суб'єкта, що, у свою чергу, надає йому можливість впливати на умови свого існування з метою їх покращання. До таких умов можна віднести і потенційні загрози, рівень яких не дестабілізує діяльності суб'єктів, а навпаки спонукає до саморозвитку. Тоді завданням «мінімум» для держави стає створення загальних мінімальних умов, що забезпечать саморозвиток і самореалізацію індивідів [2, с. 253].

Розглянутий підхід можна прийняти за основу, але з урахуванням напрацювань теорії соціальних систем та управління ними. Квінтесенцією сучасного розуміння безпеки соціальної системи є стабільність її оптимального функціонування й розвитку. Саме за таких умов гарантується достатня захищеність системи. В Україні ідея взаємозв'язку

безпеки і стабільного розвитку вже набула закріплення на рівні чинного законодавства. Так, Закон України «Про основи національної безпеки України» визначає національну безпеку як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечується сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам [5].

Щодо визначення поняття «інформаційна безпека» на сьогодні відсутній цілісний підхід і єдиної думки щодо її визначення серед дослідників не існує. Тому в межах окресленого підходу інформаційну безпеку України можна інтерпретувати як сукупність життєво важливих умов функціонування суб'єктів (особи, суспільства, держави) в інформаційній сфері та суб'єктивних (правових, політичних, інформаційних, наукових, оперативно-розшукових) можливостей їх усвідомлення й контролю.

При цьому слід зауважити, що інформаційна безпека в такому контексті розгляду набуває об'єктивно-суб'єктивного характеру. Відображенням об'єктивного її боку є сукупність умов, які концептуально повинні забезпечувати оптимальне функціонування і розвиток суб'єктів, що надає цим умовам відносного та узагальненого характеру і вираження у вигляді стандартів безпеки. Суб'єктивний бік інформаційної безпеки знаходить свій вияв у можливостях суб'єктів усвідомлювати та контролювати умови, в яких вони функціонують. Такі можливості залежать безпосередньо від індивідуальних характеристик суб'єктів: рівня інтелектуального розвитку, свідомості, освіти, культури тощо [2, с. 253].

Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства. Вона орієнтована на захист значимих або вже згаданих суб'єктів інформаційних ресурсів, законних інтересів. Зміст поняття «інформаційна безпека» розкривається у практичній діяльності, наукових дослідженнях, а також нормативно-правових документах.

Так, в розділі XV «Інформаційна безпека як складова частина національної безпеки України» запропонованого проекту Інформаційного кодексу зазначається, що інформаційна

безпека – це стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації [6]. Слід зазначити, що 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. Відтак постає необхідність в угрупуванні напрямів визначення аналізованого поняття [7, с. 76]. Сьогодні також відсутня норма, яка б містила дефініцію поняття «інформаційна безпека», враховуючи різницю між інформаційною безпекою та безпекою інформації. Так, наприклад, Ю.А. Фісун, характеризує інформаційну безпеку як «стан захищеності інформаційного середовища, який відповідає інтересам держави, за якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх інформаційних загроз» [8, с. 89]. Такої ж позиції притримуються і розробники концепції інформаційної безпеки центру Разумкова, а також деякі українські дослідники, які вважають за необхідне визначати інформаційну безпеку як стан захищеності. Так наприклад, В.К. Гасеський, В.А. Авраменко [9, с. 123]. визначають інформаційну безпеку як стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації, у той час як О.Г. Додонов визначає інформаційну безпеку як стан захищеності інформаційного простору, який забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави [10, с. 65]. Аналогічного погляду дотримується і інший російський дослідник І.М. Панарін, роблячи більший акцент на ролі політичної еліти, яка може протистояти інформаційному впливу. На його думку, інформаційна безпека – стан інформаційного

середовища суспільства і політичної еліти, який забезпечує її формування і розвиток в інтересах керівництва країни, громадян і суспільства [11, с. 87]. Дещо в іншому ракурсі трактує інформаційну безпеку А.А. Тер-Акопов, який репрезентує позицію другого напряму. Під інформаційною безпекою він розуміє стан захищеності інформації, яка забезпечує життєво важливі інтереси людини [12, с. 9]. У рамках даного напряму існує визначення інформаційної безпеки як стану, тенденції розвитку, умови життєдіяльності соціуму, його структур, інститутів і установ, при яких забезпечується збереження їх якісної з об'єктивними обумовленими інноваціями в ній, і вільне, відповідне власній природі і її функціонування. Ряд представників цього напряму розглядають інформаційну безпеку як стан, який характеризується відсутністю небезпеки, тобто чинників і умов, які загрожують безпосередньо індивіду, спільноті, державі з боку інформаційно-комунікаційного середовища [7, с. 178]. Прибічники такого підходу розглядають інформаційну безпеку як стан і процес захищеності особи, суспільства, держави від реальних або потенційних загроз. Водночас, на нашу думку, розглядати безпеку лише як стан є не зовсім точним, і не відображає динамізму як самої безпеки, так і тої системи, для якої безпека виступає як функція її подальшого розвитку та існування [7, с. 180].

Такі науковці як Н.Р. Нижник, Г.Л. Ситник, В.Т. Білоус під інформаційною безпекою розуміють стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни [2, с. 240].

Зацікавленість викликає робота таких дослідників як О.Г. Данільян, О.П. Дзьобань, М.І. Панов, які у своєму навчальному посібнику «Національна безпека України: сутність, структура та напрямки реалізації» [4, с. 86], визначають інформаційну безпеку як безпеку об'єкта від інформаційних загроз або негативних впливів, пов'язаних з інформацією та нерозголошення даних про той чи інший об'єкт, що є державною таємницею. Вони також акцентують увагу на проблемі інформаційних війн, оскільки на сьогодні вона становить собою ефективний і цивілізований шлях колонізації однієї країни іншою та виділяють крім цього такі загрози

інформаційній безпеці як розголошення інформації, яка становить державну таємницю, вплив засобів масової інформації на свідомість людини та суспільства, забезпечення державних організацій повною, достовірною і своєчасною інформацією, що необхідна для прийняття рішень, неінтегрованість України до світового інформаційного поля, недостатня кваліфікованість та активність українських інформаційних служб, використання інформаційних технологій, кримінал тощо. О.В. Литвиненко під інформаційної безпекою розуміє єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності [13, с. 177]. Цікавим та водночас дискусійним є визначення Б.А Кормича, який зазначає, що інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави [14, с. 267].

Російський вчений В.М. Лопатін визначає інформаційну безпеку як стан захищеності національних інтересів країни (життєво важливих інтересів особи, суспільства та держави на збалансованій основі) в інформаційній сфері від внутрішніх та зовнішніх загроз, що віддзеркалює норму права Закону РФ «О безопасности», згідно з яким «Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз» [15, с. 354].

Використовує категорію національних інтересів і О.П. Баранов відповідно визначаючи інформаційну безпеку як стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації й несанкціоноване її поширення та використання, а також через негативний інформаційний вплив та негативні наслідки функціонування інформаційних технологій [16, с. 60-62]. Акцент на такій складовій інформаційної безпеки як безпека інформації, знаходить свій вираз також у визначеннях інших дослідників цієї проблематики, наприклад, інформаційна безпека – це стан захищеності інформаційного простору, що

забезпечує його формування та розвиток в інтересах громадян, організацій та держави, стан інфраструктури системи (об'єкта, держави), при якому інформація використовується суворо за призначенням та не завдає негативного впливу на систему (об'єкт, державу) при її використанні; стан інформації, за якого виключається чи суттєво ускладнюється порушення таких її властивостей як таємність, цілісність та доступність [7, с. 345].

Неординарністю та інноваційністю відрізняється також й визначення В.І. Гурковського відповідно до якого національна інформаційна безпека України – це суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутворюючої нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів [17, с. 9-18].

Відповідно до точки зору В. Петрика, інформаційна безпека – це стан захищеності особи, суспільства і держави, при якому досягається інформаційний розвиток, технічний, інтелектуальний, соціально-політичний, морально-етичний, за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди [18, с. 49-52].

На думку В.І. Ярочкіна та Т.А. Шевцової інформаційна безпека – це проведення правових, організаційних та інженерно-технічних заходів при формуванні та використанні інформаційних технологій, інфраструктури та інформаційних ресурсів, захисті інформації високого значення й прав суб'єктів, що беруть участь в інформаційній діяльності. У даному визначенні інформаційна безпека зводиться до захисту інформації, що не зовсім відбиває її сутність [19, с. 24].

Л.С. Харченко, Н.А. Ліпкан, О.В. Логінов визначили, що інформаційна безпека – це складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України [20, с. 75].

Проте, якщо проаналізувати зміст та напрямки досліджень поняття інформаційної безпеки, можна виокремити декілька підходів окреслення сутності цього феномену, а саме розуміння інформаційної безпеки в якості: – стану захищеності інформаційного простору; – процесу управління загрозами та небезпеками, що забезпечує інформаційний суверенітет України; – стану захищеності національних інтересів України в інформаційному середовищі; – захищеності встановлених законом правил, за якими відбуваються інформаційні процеси в державі; – стану захищеності національних інтересів країни в інформаційній сфері; – до суспільних відносин, пов'язаних із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі; – важливої функції держави; – невід'ємної частини політичної, економічної, оборонної та інших складових національної безпеки.

Строкатість поглядів на визначення поняття «інформаційна безпека» є зрозумілою, оскільки, як вірно зазначають Н.Р. Нижник, Г.Л. Ситник, В.Т. Білоусов до цього часу бракує єдиної думки в трактуванні базових понять національної безпеки, що дає теорія, яка передбачає [2, с. 158]: по-перше, формування базових понять (створення відповідного понятійно-категоріального апарату); по-друге, встановлення їх структурно-функціональних зв'язків; по-третє, вибір підходу (підходів) до формалізації процесів, що аналізуються (вивчаються), та розробка на цій основі методів дослідження, які б забезпечили поглиблене вивчення та виявлення відповідних (властивих даному об'єкту досліджень) закономірностей.

О.Г. Данільян, О.П. Дзьобань, М.І. Панов, стверджують, що це пов'язано як з певним суб'єктивізмом дослідника, який використовує вироблені наукою та філософією сукупність понять і категорій, інтерпретуючи їх у властивий для себе спосіб, так і з взагалі з переглядом багатьох традиційних положень, формуванням принципово нових концепцій, введенням в науковий обіг нових понять і категорій [4, с. 188].

Отже, конструктивним шляхом щодо визначення поняття інформаційна безпека, є виокремлення його базових ознак, яке є

похідним від поняття національна безпека, і має враховувати його сутнісні ознаки.

Даний підхід більш детально розписаний у монографії В.А. Ліпкана «Теоретико-методологічні засади управління у сфері національної безпеки України» [21, с. 122]. Методологічні ж проблеми, які спіткають дослідників феномену національної безпеки і її проявів в різних сферах життєдіяльності, викладені у монографії В.А. Ліпкана «Теоретичні основи та елементи національної безпеки України», в якій робиться спроба щодо формування теорії національної безпеки – націобезпекознавства. За задумом автора воно має виступати теорієстворюючим гносеологічним елементом загальної будови системи знань про національну безпеку взагалі та інформаційну зокрема [7, с. 343].

Запропоноване широке розуміння інформаційної безпеки дає змогу визначити будь-який з її аспектів, зокрема і правовий. Правовим відображенням інформаційної безпеки є сукупність правових умов, що забезпечують оптимальне функціонування і розвиток суб'єктів в інформаційному середовищі. Таке визначення по суті дозволяє говорити про інформаційно-правову безпеку й ототожнює її з режимом законності в інформаційній сфері.

Необхідно наголосити, що сама законність є досить складним і дискусійним у наукових колах явищем. У запропонованому контексті розгляду інформаційної безпеки законність має сприйматися спираючись на філософсько-правове розуміння закону, яке дає змогу розглядати її як загальноправове явище, що не залежить від особливостей правових систем та напрямів праворозуміння.

Н.М. Оніщенко, абстрагуючись від приватних, пов'язаних з типом праворозуміння розбіжностей у численних дефініціях, зазначає, що законність розуміють як фундаментальну юридичну категорію, яка є критерієм правового життя суспільства і громадян [22, с. 134]. Законність – це «комплексне політико-правове явище, що відображає правовий характер організації суспільного життя, органічний зв'язок права і влади, права і держави» [23, с. 274]. Законність також розуміють як специфічний режим суспільно-політичного життя, втілений у системі нормативних, політико-юридичних вимог (неухильного

дотримання правових актів усіма суб'єктами, верховенства права, рівності всіх перед законом, належного й ефективного застосування права, послідовної боротьби з правопорушеннями) [24, с. 194]. Законність в юридичному розумінні – це правовий режим у державі, за якого діяльність усіх державних органів, юридичних і фізичних осіб здійснюється відповідно до вимог закону [25, с. 214].

Таким чином, саме законність є необхідним організаційно-ідеологічним фундаментом, на якому можливе досягнення таких високих цілей, як розвиток громадянського суспільства та розбудова правової держави. Законність в інформаційній сфері життя суспільства і держави, у свою чергу, активно сприятиме цим процесам та забезпечуватиме стабільний інформаційний розвиток суспільства, ефективну взаємодію держави і громадян та громадян між собою, що, по суті, є досягненням високого рівня інформаційної безпеки.

Реалізація режиму законності у державі базується на системі гарантій, дієвість яких покликана зробити законність реальною [26, с. 210]. Слід зазначити, що гарантії законності мають досить широкий комплексний характер, а також як юридичну, так і загальносоціальну природу.

До загальносоціальних гарантій законності в інформаційній сфері належить уся сукупність умов існування суспільства (економічних, політичних, соціальних, ідеологічних тощо), які позитивно впливають на формування суспільної свідомості й, зокрема, її інформаційної складової. У сучасній Україні ці умови знаходяться в зародковому стані, що гальмує загальний розвиток суспільства й створює складні перешкоди на шляху реалізації законності й досягнення правопорядку. Тому практичне значення має аналіз загальносоціальних факторів як позитивного, так і негативного характеру, які є реальними умовами здійснення правового регулювання, становлення громадянського й інформаційного суспільства, розбудови правової держави, забезпечення національної та інформаційної безпеки з метою вироблення ефективних моделей державного управління та адекватних форм і методів здійснення державної влади.

Сучасний етап розвитку нашої держави характеризується великою кількістю проблем у багатьох сферах суспільного життя. Задекларована на конституційному рівні модель України

як незалежної, соціальної, демократичної, правової держави, незважаючи на окремі позитивні зрушення, залишається поки що далекою перспективою. Аналізуючи шляхи розбудови правової держави і громадянського суспільства в Україні, А. Колодій зазначає, що навіть загального погляду на сучасну соціально-економічну ситуацію достатньо, щоб переконатися у відсутності в ній ознак соціального громадянського суспільства. Навпаки, у сучасній Україні відсутня послідовна та виважена державна програма (концепція) соціального розвитку, соціальної політики, довгострокова та незалежна від будь-якої влади, політичних сил, що нею володіють [27, с. 21]. Наведена думка свідчить про можливість дискусії щодо синергетичного характеру розвитку українського суспільства лише на теоретичному рівні, оскільки існуючий загальний рівень свідомості та самоорганізаційних можливостей індивідів є занадто низьким.

Тому сьогодення України можна назвати початковим етапом становлення національної свідомості та етапом зародження національної інформаційної свідомості, що надає особливого значення відповідному існуючим умовам правовому регулюванню сфери інформаційних відносин. Одним із головних завдань держави на такому етапі розвитку є визначення напрямів правового регулювання та створення правових гарантій, необхідних для самореалізації суб'єктів в інформаційній сфері. Виконання цього завдання ускладнюється рядом об'єктивних факторів, які виступають передумовами становлення інформаційного права України. Більшість із цих факторів є загальними чинниками (джерелами) процесу утворення національного права і тому дозволяють розглядати процеси розвитку інформаційного права України в контексті проблем становлення правової системи України в цілому [28, с. 254]. Відповідно, розвиток науки, тобто отримання нового знання, є складним творчим процесом, який має певну логічну послідовність в діяльності дослідника. У цілому він відповідає поступальному характеру розвитку форм наукового знання. Підтримуємо автора курсу лекцій «Методологія системного підходу та наукових досліджень» О.В. Кустовську у тому, що наукове дослідження обумовлюється об'єктивними та суб'єктивними факторами [29, с. 90]. Вважаємо цілком

вивіреною таку позицію вченої щодо логіки наукового процесу і, беручи її за основу, вважаємо за доцільне проаналізувати об'єктивні та суб'єктивні фактори в контексті інформаційного розвитку суспільства та забезпечення інформаційної безпеки.

1. Інтелектуальний (психологічний) фактор. До нього можна віднести такі характеристики української суспільної свідомості та явища негативного характеру, що у сукупності гальмують процеси інформаційного розвитку суспільства та забезпечення інформаційної безпеки: – ірраціональність, консерватизм та апатичність суспільної свідомості; – відсутність сформованості в загальносуспільній свідомості інформаційних потреб; – відсутність усвідомленості інформаційних загроз; – низький рівень правової свідомості громадян; – падіння рівня загальної освіти і культури громадян; – загальна поширеність правового нігілізму.

2. Динамічність інформаційної сфери. Ускладнює процеси утворення інформаційного права на всіх його етапах: і на етапі формування, і на етапі формулювання, і на етапі реалізації права. Цей фактор призводить до недосконалості законодавства, що регламентує інформаційну сферу суспільних відносин, та неефективної його реалізації. Основними чинниками динамічності перетворень в інформаційній сфері є: стрімкий розвиток інформаційної сфери; стрімкий розвиток інформаційно-комунікаційних технологій; підвищена складність і різноманітність суспільних відносин в інформаційній сфері; новизна інформаційних відносин та відсутність досвіду їх правового регулювання; відсутність загальноприйнятих варіантів поведінки в інформаційній сфері, вироблених суспільством.

3. Підвищення соціального значення інформаційних процесів. Визначає пріоритетність організаційно-забезпечувальної діяльності держави в інформаційній сфері як основи подальшого розвитку суспільства, що підтверджується такими чинниками: всепроникливість інформаційних процесів; створення широких інформаційно-комунікативних можливостей; виникнення додаткових можливостей саморозвитку суб'єктів; виникнення нових особливо небезпечних загроз суспільній безпеці; безпрецедентне підвищення загальносоціального значення всіх складових інформаційної безпеки.

4. Економічний фактор. Створює економічне підґрунтя інформаційного розвитку суспільства і держави та матеріально-технічні можливості впровадження інформаційно-комунікаційних технологій. Узагальнені чинники економічного характеру, що визначають результативність процесу забезпечення інформаційної безпеки: відсутність стабільного зростання економіки; низький рівень забезпеченості широких верств населення всіма необхідними для розвитку матеріально-технічними засобами; низький рівень забезпеченості апарату держави сучасними інформаційно-комунікаційними засобами; недостатність фінансування сфери освіти та науки.

5. Технічний фактор. Складові цього фактору характеризують технічну досконалість і сучасність засобів обробки інформації, що визначає рівень технічної готовності до розгортання інформаційних процесів. Основними з них є: нерозвиненість мережі швидкісного Інтернету; недосконалість інформаційних ресурсів; застарілість автоматизованих систем обробки інформації.

6. Політико-ідеологічний фактор. Визначає рівень усвідомленості соціально сильними групами індивідів необхідності вирішення соціальних проблем та проблем інформаційної сфери. До нього можна віднести: відсутність сталої, незалежної від політичних персон, стратегії становлення України на світовій арені; відсутність реальної, послідовної та виваженої державної програми соціального розвитку; неправовий характер діяльності державної влади; пріоритетність політичної доцільності над правовою; бюрократичність апарату держави; нерозвиненість громадянського суспільства; нерозвиненість інформаційних зв'язків між державою і суспільством тощо.

Названі фактори зумовлюють особливу важливість та пріоритетність різнопланової високопрофесійної державно-владної діяльності в інформаційній сфері, юридичного її забезпечення, а також виваженого вибору методів правового регулювання [2, с. 254]. Юридичною основою створення сприятливих правових умов в інформаційній сфері можна вважати систему спеціально-юридичних та організаційних гарантій законності, яка складається з сукупності закріплених законодавством засобів та організаційно-правової діяльності

щодо їх застосування, спрямованих на забезпечення інформаційної безпеки, а також заходів організаційного характеру, що забезпечують підвищення рівня інформаційної безпеки, боротьбу з правопорушеннями в інформаційній сфері, захист прав суб'єктів інформаційних відносин [2, с. 254].

Запропоноване розуміння правового аспекту інформаційної безпеки надає йому системності (поєднання під правовим кутом зору економічних, ідеологічних, спеціально-юридичних, організаційних важелів забезпечення), що об'єктивно зумовлено міждисциплінарним характером інформаційної безпеки та правовим характером діяльності сучасної держави. Підтвердженням цієї позиції є і популяризація останнім часом сучасними українськими спеціалістами з проблем національної безпеки виключно комплексного вирішення проблем інформаційної безпеки України, незважаючи на їх неосяжність. Так, наприклад, В. Горбулін, М. Биченок, П. Копка серед актуальних проблем системного забезпечення інформаційної безпеки України виокремлюють такі напрями: нормативно-правове забезпечення, фінансово-економічні важелі, адміністративно-організаційні заходи, морально-етичне виховання та науково-технічне забезпечення [30, с. 79].

Системність підходу до забезпечення інформаційної безпеки зумовлює й необхідність широкого погляду на спеціально-юридичні гарантії законності в інформаційній сфері та дає змогу інтерпретувати їх як наявність дієвого, ефективного, виваженого інформаційного законодавства і, що особливо актуально для України, відображає інтеграційне спрямування держави та об'єктивні умови її існування. Сучасне трактування ефективності законодавства пов'язують із середовищем дії права, під яким розуміють взаємодію багатьох складових – стану економіки, політичного режиму, якості законодавства, ефективності роботи правових установ. Якщо ці фактори плідно взаємодіють, то формується певне правове середовище, що визначає правомірність дій суспільства, держави та індивіда [31, с. 86]. Однак в узагальненому вигляді потенційну ефективність та дієвість інформаційного законодавства України можна відобразити за допомогою низки вимог, які визначають і проблематику наукових досліджень юридичного характеру у сфері забезпечення інформаційної безпеки: забезпеченість на

рівні концепцій, принципів, дефініцій, що відображають багатоаспектність інформаційної безпеки; високий рівень законодавчої техніки та термінологічний комплекс, що відповідає всім вимогам до мови закону та юридичної термінології; адекватне відображення в інформаційному законодавстві реальних умов життя; напрямів розвитку суспільства; балансу інтересів держави, суспільства та особистості; міжнародних стандартів; зручність інформаційного законодавства; передбаченість ефективних механізмів реалізації; розвиненість та виваженість інституту юридичної відповідальності за різні правопорушення в інформаційній сфері [2, с. 254]. Виконання означених вимог – складне завдання, що потребує системного підходу. Особливо важливим і першочерговим кроком на цьому шляху є напрацювання універсального понятійно-категоріального апарату через безпосереднє закріплення у відповідній науці, а також надання відповідних знань практичним працівникам (в першу чергу через формування навчальної дисципліни, присвяченої інформаційній безпеці).

Щодо першого аспекту, то інформаційну безпеку, на наш погляд, необхідно розуміти, як відокремлений інститут інформаційного права. Цей інститут розглядає не тільки захист інформації, але й організаційні, політичні, правові та інші заходи, спрямовані на забезпечення стійкого, стабільного розвитку суспільства й держави.

Другий аспект (надання відповідних знань практичним працівникам), на наш погляд, можна реалізувати, запровадивши навчальний курс «Інформаційне право» та «Правова інформатика». Предметом навчального курсу «Інформаційне право» є правове регулювання суспільних інформаційних відносин. В свою чергу, предметом навчального курсу «Правова інформатика» є суспільні відносини, що виникають при реалізації інформаційних процесів, тобто створення, збирання, обробки, накопичення, зберігання, пошуку, розповсюдження та споживання інформації, а також процесів створення та застосування інформаційних систем і мереж, інформаційних технологій, засобів інформаційної безпеки на базі використання комп’ютерної техніки та засобів зв’язку і телекомунікації.

Дані дисципліни є спеціальними навчальними курсами, складовою частиною циклу фундаментальних дисциплін навчального плану підготовки фахівців і вивчаються в циклі спеціальних дисциплін як самостійні предмети. Основна мета навчальної дисципліни «Інформаційне право» полягає в тому, щоб допомогти студентам зорієнтуватися в методах, способах, засобах регулювання, охорони, захисту діяльності у сфері інформації, що знайшли відображення у нормативно-правових актах, науці, практиці. Головне призначення даної дисципліни зводиться до того, щоб сформувати у студентів комплексні знання, навички щодо застосування норм інформаційного права у майбутній практичній діяльності. Метою навчальної дисципліни «Правова інформатика» є формування у студентів розуміння загальних основ правової інформатики як науки, принципів організації та правових засад функціонування державних правових інформаційних систем, отримання навичок проведення робіт з пошуку нормативних правових актів та судової практики в конкретній сфері діяльності. При вивченні даної дисципліни вирішуються такі основні завдання: освоєння студентами особливостей створення та застосування автоматизованих інформаційних систем у правовій сфері; освоєння методології і придбання навичок використання сучасних інформаційних технологій при зборі, обробці, зберіганні, передачі і пошуку необхідної правової інформації.

Таким чином, подальша розробка загальнонаукових та правових категорій (зважаючи на суттєве теоретичне та практичне значення) є актуальним напрямком наукових досліджень в першу чергу в контексті інформаційної безпеки.

Загалом дослідження генезису наукової думки та правової практики в сфері забезпечення інформаційної безпеки України дозволило виділити три основні етапи їх становлення [32].

Перший етап (1991–1996 рр.). Відсутні ґрунтовні наукові дослідження інформаційної складової національної безпеки. Здебільшого наукові роботи присвячені національній безпеці, в контексті чого автори лише поверхнево зазначають про необхідність виокремлення її інформаційної складової, при чому не надаючи пріоритету серед інших складових. Інформаційна безпека здебільшого ототожнюється з безпекою інформації. Автори виділяють ряд основних загроз та

пріоритетів інформаційної безпеки України, що, як правило, мають внутрішній характер та пов'язані, насамперед, із відсутністю кваліфікованого кадрового забезпечення та політичною нестабільністю в країні.

Другий етап (1996–2000 рр.). Розгляд інформаційної безпеки виходить на пріоритетне місце в системі національної безпеки, про що свідчить конституційна закріпленість інформаційної безпеки як важливої функції держави. В той же час здебільшого в наукових розробках інформаційна складова розглядається через висвітлення проблем інформаційної безпеки держави, залишаючи осторонь інші важливі об'єкти – людини і громадянина, а також суспільство. Ще однією особливістю досліджень цього періоду є те, що в них акцентується увага на необхідності превентивної діяльності щодо захисту з метою забезпечення інформаційної безпеки України. З'являються перші ґрунтовні дисертаційні дослідження політологічного та юридичного спрямування, предметом розгляду яких є інформаційна безпека. Необхідно відзначити, що у багатьох роботах вчених – правників інформаційна безпека ототожнюється з комп'ютерною, внаслідок чого тенденційним є бурхливий сплеск розробок саме кримінального спрямування. У чисельних наукових розвідках зазначається про появу нового виду тероризму – інформаційного, та загалом про кіберзлочинність як різновид злочинності, а також про таку новітню загрозу інформаційній безпеці України як маніпулювання свідомістю людини, громадянина та загалом суспільства.

Третій етап (2001–2013 рр.). Враховуючи те, що інформаційна проблематика має транснаціональний характер та потребує узгоджених дій всього світового співтовариства, характерною рисою даного етапу є інтенсифікація наукових розвідок міжнародних засад інформаційної безпеки. Крім того, проголошений зовнішньополітичний курс України на інтеграцію до Європейського Союзу обумовив появу наукових робіт, присвячених саме досвіду забезпечення інформаційної безпеки євроспільнотою, проблемам, перспективам, напрямам узгодження (адаптації) вітчизняного інформаційного законодавства до європейського. Зважаючи на специфіку термінології, що використовується при репрезентації окремих

аспектів інформаційної безпеки, наступною віхою для вітчизняної науки в цій сфері стала поява чисельних словників, глосаріїв тощо. Необхідно відзначити, що для даного періоду також достатньо характерним є інтенсифікація наукових розвідок, що присвячені ролі, місця, завдань тощо окремих органів влади у сфері забезпечення інформаційної безпеки України та загалом ґрунтовна деталізація окремих її засад.

Отже, перші роботи, в яких була зроблена спроба наукового узагальнення досвіду та формування основ інформаційної безпеки, з'явилися на початку 90-х років минулого століття. Визнання інформаційної безпеки як важливої функції держави, зі своїми цілями і завданнями, складною структурою, властивою тільки їй специфікою, викликала необхідність більш детального вивчення питання кодифікації інформаційного законодавства, яка підтримується багатьма науковцями-юристами та дослідниками національного інформаційного простору. Дослідження загальнонаукової та правової категорії інформаційної безпеки проводили такі вчені, як Н.Р. Нижник, Г.П. Ситник, Д.Г. Данільян, В.А. Ліпкан, О.В. Олійник, Б.А. Кормич, М.М. Галамба, В.П. Горбулін, О.В. Бойченко та інші.

Так, В.С. Цимбалюк у монографії «Інформаційне право:концептуальні положення до кодифікації інформаційного законодавства» з позиції системного підходу розглянув методологічні положення до кодифікації інформаційного законодавства, як складової теорії та практики інформаційного права [33, с. 107]. Окремо зазначимо, що в межах суміжних юридичних наук, зокрема в адміністративному та цивільному праві, здійснено достатньо значну кількість досліджень з питань інформаційної безпеки, отримано вагомі наукові результати. І хоча можливості їх використання в межах цієї роботи обмежені відомою специфікою предмета й методу адміністративно-правового регулювання, аналіз висловлених пропозицій щодо сутності інформаційної безпеки та загальних засад її правового забезпечення є необхідним.

Значної уваги кодифікації інформаційного законодавства приділяли В. Горобцов, М. Швець, В. Брижко. У своїх роботах вони підкреслювали, що необхідність обговорення проблем кодифікації інформаційного законодавства зумовлена сукупністю значної кількості неузгоджених правових норм у сфері інформаційних

відносин. Зважаючи на відсутність системності у підходах до кодифікації інформаційного законодавства, однією з важливих проблем є підготовка та прийняття Інформаційного кодексу України, який би відповідав рівню розвитку інформаційних відносин та адекватно врегульовував питання функціонування інформаційної сфери [34, с. 122].

Узагальнивши зазначені праці, можна підсумувати, що: по-перше, достатньо стрімкий розвиток наукових досліджень в сфері забезпечення інформаційної безпеки у 90-х роках минулого століття змінився науковою байдужістю до цього питання, адже жодних концептуальних документів по інформаційній безпеці досі не прийнято; по-друге, аналіз наукових праць з питання інформаційної безпеки показує, що в цілому дана проблема досліджена неповно. Більшість наукових розробок представлена у вигляді лекцій, практичних посібників, монографій тощо. Це обумовлено такими причинами:

- інформаційна безпека згадується в сотнях нормативних актів, безпосередньо її захисту вже 15 років присвячуються десятки документів, серед яких Доктрина інформації безпеки, укази президентів, декілька рішень РНБО, міжнародні документи про співробітництво в межах СНД. Але в жодному з них немає визначення цього поняття, і що, власне, захищається, можна намагатися зрозуміти з переліку численних загроз та заходів щодо їх подолання.
- актуальним залишається встановлення сутнісних характеристик інформаційної безпеки шляхом дослідження підходів до визначення цього поняття.
- при дослідженні питання інформаційної безпеки спостерігається однобічність та поверховість (зокрема, взагалі не досліджувалась змістовна складова, яка виражається в захисті суспільства від поширення недостовірної або маніпулятивної інформації).
- тривалий час безпека інформації залишалася закритою, що не дозволяло повною мірою вивчати питання інформаційної безпеки як всередині, так і ззовні неї. Такий стан призвів до того, що наукові дослідження та обґрунтування здійснювалися обмеженим колом вчених, що призвело до однобічності і суб'єктивізму сформованих наукових положень та висновків.

1.2. Система забезпечення інформаційної безпеки держави

Очевидно, що запорукою створення надійної системи охорони інформації сьогодні може бути тільки зміцнення самої української держави та її державних органів, відповідальних за забезпечення інформаційної безпеки в країні. У зв'язку з цим стоять масштабні завдання, пов'язані з виробленням системи забезпечення інформаційної безпеки, пошуку принципово нових, нестандартних форм організації, взаємодії, координації діяльності, удосконалення всіх засобів, спрямованих на забезпечення процесу управління загрозами та небезпеками.

Для комплексного визначення системи забезпечення інформаційної безпеки проаналізуємо теоретичні положення, які передбачають наявність відповідних структур і певно регламентованого процесу прийняття і реалізації управлінських рішень у сфері управління інформаційною безпекою. Підтвердженням актуальності даного дослідження є те, що 1 травня 2014 року виконуючий обов'язки Президента України, голова Верховної Ради України Олександр Турчинов підписав Указ № 449/2014 про рішення РНБО від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [35]. Виходячи з необхідності вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз інформаційній безпеці, Рада національної безпеки і оборони України доручила Кабінету Міністрів України у місячний строк розробити і внести на розгляд Верховної Ради України законопроекти про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав.

Отже, важливим моментом має стати те, що Україна повинна сформувати таку систему забезпечення інформаційної безпеки, яка дозволить гарантовано забезпечити національні інтереси за будь-яких умов.

У даний час проблематика інформаційної безпеки держави досліджується в роботах багатьох українських учених, таких як: І.В. Арістової, В.К. Гіжевського, І.П. Голосніченко, Ю.В. Іщенко, Р.А. Калюжного, В.А. Ліпкана, В.С. Цимбалюка, М.Я. Швеця та ін.

Проте зазначені дослідження та наукові праці стосувалися лише національної безпеки в інформаційній сфері. На цей час залишаються недостатньо вивченими концептуальні засади системи забезпечення інформаційної безпеки держави.

Необхідність забезпечення інформаційної безпеки держави є очевидною. Потреба у захисті рівною мірою стосується як інформації, що міститься у всіх інформаційних системах і передається мережею, так і тієї, що перебуває «поза кадром». Різноманіття інформації величезне – від матеріалів обговорень у залах сесійних засідань та кабінетах комітетів і комісій – в тому числі таких, що відбуваються за закритими дверима, – до особистого листування, даних відділу кадрів та іншої делікатної інформації, тому гарантування безпеки є завжди актуальною темою. Щодня з'являються нові повідомлення про зловживання та зломи. Разом зі складнішими проблемами, пов'язаними з соціотехнікою, проблеми захисту інформації вимагають від її власників постійно бути насторожі. Вторгнення, атаки, спрямовані на зрив обслуговування користувачів, незаконне розголошення інформації – «одвічні» загрози, протистояти яким мають ретельно продумані програми захисту даних для всіх аспектів діяльності законодавчого органу. Йдеться як про внутрішні системи й процедури, так і про ті, що висвітлюються в Інтернеті. З означених щойно причин, більшість державних органів дотримуються базових принципів гарантування інформаційної безпеки: використання інформації у відповідності з законодавством та виключно з тією метою, з якою вона надається; зведення обсягів інформації до необхідного мінімуму; повага до прав громадян або організацій, яких стосується інформація, що використовується; своєчасне оновлення, забезпечення актуальності і достовірності інформації; зберігання інформації лише доти, доки вона потрібна; підтримка безпеки інформаційного середовища; надання інформації іншим організаціям лише після надходження відповідних запитів та здійснення захисних заходів.

Таким чином, визначення даного поняття має не лише суто теоретичний, а й практичний інтерес, пов'язаний із необхідністю формування системи органів державного управління інформаційною безпекою держави.

Аналіз наукової літератури засвідчує, що питання системи забезпечення інформаційної безпеки недостатньо досліджені. В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський розглядають систему забезпечення інформаційної безпеки як систему інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об'єктів інформаційної безпеки, а також інфраструктури її забезпечення [36, с. 158]. Як бачимо, автори у громіздкому визначенні поєднують суб'єктивний та нормативний підходи, не вказавши елементів системи. Інший підхід демонструє А.А. Стрельцов і до системи інформаційної безпеки включає такі елементи: суб'єкти інформаційних процесів, інформація, призначена для використання суб'єктами інформаційного суспільства, інформаційна інфраструктура, суспільні відносини, які складаються у зв'язку зі створенням, зберіганням, передачею та розповсюдженням інформації [37, с. 15-21]. Але вчений, на наш погляд, розглядає механізм забезпечення інформаційної безпеки, а не її систему. Очевидним є те, що система забезпечення інформаційної безпеки є сукупністю окремих елементів, якими, зазвичай, є об'єкт, суб'єкти та види. У той же час окремими її складовими є основні характеристики, рівні інформаційної безпеки та перелік загроз.

Таким чином, система забезпечення інформаційної безпеки – це внутрішня структура, систематизована сукупність, єдність, взаємозв'язок і диференціація окремих її елементів (об'єкт, суб'єкти, основні характеристики, рівні інформаційної безпеки та перелік загроз).

У питанні про об'єкт інформаційної безпеки звертаємо увагу, що законодавець подає перелік об'єктів національної безпеки: людина і громадянин – їхні конституційні права і свободи; суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності; інформаційне та навколишнє природнє середовище і природні ресурси; держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканість [5]. Як уточнюють автори підручника «Курс адміністративного права України», основними об'єктами безпеки є: особа – її права і свободи; суспільство – матеріальні і духовні цінності; держава – конституційний лад,

суверенітет і територіальна цілісність [38, с. 345]. Отже, очевидним є необхідність доповнення цього переліку (на прикладі інформаційної безпеки) таким об'єктом, як: інформація, інформаційна діяльність.

Законодавство не містить чіткого переліку суб'єктів інформаційної безпеки, а в Законі України «Про основи національної безпеки України» подано лише систему суб'єктів забезпечення національної безпеки. Про те в Законі України «Про інформацію» [39] суб'єктами визначені: фізичні особи, юридичні особи, об'єднання громадян та суб'єкти владних повноважень. Інший перелік ми можемо переглянути в Законі України «Про доступ до публічної інформації», де суб'єктами визнано: запитувачів інформації (фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи, крім суб'єктів владних повноважень); розпорядників інформації; структурний підрозділ або відповідальну особу з питань запитів на інформацію розпорядників інформації. Необхідно уточнити, що до розпорядників інформації законодавець відніс чималий перелік, а саме: суб'єкти владних повноважень – (органи державної влади, інші державні органи, органи місцевого самоврядування, органи влади Автономної Республіки Крим, інші суб'єкти, що здійснюють владні управлінські функції відповідно до законодавства та рішення яких є обов'язковими для виконання); юридичні особи, що фінансуються з державного, місцевих бюджетів, бюджету Автономної Республіки Крим, – стосовно інформації щодо використання бюджетних коштів; особи, якщо вони виконують делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором, включаючи надання освітніх, оздоровчих, соціальних або інших державних послуг, – стосовно інформації, пов'язаної з виконанням їхніх обов'язків; суб'єкти господарювання, які займають домінуюче становище на ринку або наділені спеціальними чи виключними правами, або є природними монополіями, – стосовно інформації щодо умов постачання товарів, послуг та цін на них. Вважаємо, що зазначений перелік неповний, оскільки, на наше переконання, суб'єктом інформаційної безпеки є, з одного боку, Україна як держава в цілому, інші держави та міжнародні організації, а з іншого – юридичні та фізичні особи (споживачі інформації,

виробники інформації, експерти по кваліфікації та фахівці із сертифікації).

Насамперед у системі забезпечення інформаційної безпеки розглянемо її основні характеристики. Інформаційна безпека виступає як характеристика стабільного, стійкого стану системи, яка при впливі внутрішніх та зовнішніх загроз та небезпек зберігає суттєво важливі характеристики для власного існування. Так, Ю.А. Гатчин, В.В. Сухостат виокремлюють такі основні характеристики інформаційної безпеки: доступність, цілісність та конфіденційність [40, с. 34]. С.В. Кавун, В.В. Носов, О.В. Манжай основними характеристиками інформаційної безпеки називають критерії конфіденційності, критерії цілісності, критерії доступності, критерії спостережності [41, с. 16]. Авторський колектив під редакцією В.Г. Кононовича об'єднує основні характеристики інформаційної безпеки в діяльність власника інформації або уповноваженої ним особи з: забезпечення своїх прав на володіння, розпорядження і управління захищеною інформацією; запобігання витоку і втрати інформації; збереження повноти, вірогідності, цілісності захищеної інформації, її масивів і програм обробки; збереження конфіденційності або таємності захищеної інформації, відповідно до правил, установлених законодавчими й іншими нормативними актами [42, с. 9]. Але їх об'єднання за різними критеріями (суб'єкти та сфера інформаційної діяльності) є спірним. Увагу заслуговує думка, що інформаційна безпека держави має динамічний характер. У кожний конкретний відрізок часу стан захищеності може мати різний рівень, що визначається гостротою внутрішніх та зовнішніх загроз і характером реагування на них управлінського апарату відкритої соціальної системи [43].

Доречним, на нашу думку, віднести до характеристики інформаційної безпеки змістовні її показники, які проявляються по-особливому на кожному з рівнів державного управління, зокрема на: стратегічному – Кабінет Міністрів України; тактичному – центральні органи виконавчої влади; оперативному – місцеві органи виконавчої влади, провідне місце серед яких посідають місцеві державні адміністрації.

У системі забезпечення інформаційної безпеки основними елементами вважаємо перелік її рівнів. Аналіз джерел засвідчує,

що науковці пропонують розглядати такі рівні інформаційної безпеки: нормативно-правовий рівень – закони, нормативно-правові акти тощо; адміністративний рівень – дії загального характеру, які вживаються органами державного управління; процедурний рівень – конкретні процедури забезпечення інформаційної безпеки; програмно-технічний рівень – конкретні технічні заходи забезпечення інформаційної безпеки. Так, В.А. Ліпкан пропонує розглядати такі рівні інформаційної безпеки: стратегічний рівень – Рада національної безпеки і оборони України та Кабінет Міністрів України; тактичний рівень – центральні органи виконавчої влади; оперативний рівень – місцеві органи виконавчої влади [21, с. 147].

Проте в навчальному посібнику «Інформаційна безпека України в умовах євроінтеграції», В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський [36, с. 34]. знаходимо інший перелік рівнів інформаційної безпеки, зокрема: фізичний, програмно-технічний, управлінський, технологічний, рівень користувача, мережний, процедурний. Розглянемо дещо детальніше кожний з цих рівнів. На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються, і управлінських технологій. На програмно-технічному рівні здійснюється ідентифікації і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності. На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління з боку єдиної системи забезпечення інформаційної безпеки органів державного управління. На технологічному рівні здійснюється реалізації політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій. На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на суб'єктів державного управління, унеможливлення інформаційного впливу з боку соціального середовища. На рівні мережі дана політика реалізується у форматі координації дій органів державного управління, які пов'язані між собою однією метою. На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна

виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт. С.І. Макаренко для захисту інтересів суб'єктів інформаційних відносин пропонує поєднувати такі рівні забезпечення інформаційної безпеки: законодавчі; адміністративні (накази та інші дії керівництва, які пов'язані з захистом інформаційних систем); процедурні; програмно-технічні [44, с. 62].

Законодавчий рівень є найважливішим для забезпечення інформаційної безпеки. Більшість людей не здійснюють протиправних дій не тому, що це технічно неможливо, а тому, що це засуджується і / або карається суспільством, тому, що так чинити не прийнято.

На законодавчому рівні розрізняють дві групи заходів: – заходи, спрямовані на створення і підтримку в суспільстві негативного (у тому числі із застосуванням покарань) ставлення до порушень і порушників інформаційної безпеки (назвемо їх заходами обмежувальної спрямованості); – направляючі і координуючі заходи, що сприяють підвищенню освіченості суспільства в галузі інформаційної безпеки, що допомагають у розробці та поширенні засобів забезпечення інформаційної безпеки (заходи творчої спрямованості). Найважливіше (і, ймовірно, найважче) на законодавчому рівні – створити механізм, що дозволяє узгодити процес розробки законів з реаліями і прогресом інформаційних технологій. Закони не можуть випереджати життя, але важливо, щоб відставання не було занадто великим, так як на практиці, крім інших негативних моментів, це веде до зниження інформаційної безпеки.

До адміністративного рівня інформаційної безпеки відносяться дії загального характеру. Головна мета заходів адміністративного рівня – сформувати програму робіт в галузі інформаційної безпеки та забезпечити її виконання, виділяючи необхідні ресурси і контролюючи стан справ. Основою програми є політика безпеки, що відображає підхід організації до захисту своїх інформаційних активів. Керівництво кожної організації має усвідомити необхідність підтримки режиму безпеки і виділення на ці цілі значних ресурсів. Політика безпеки будується на основі аналізу ризиків, які

визнаються реальними для інформаційної системи організації. Коли ризики проаналізовані та стратегія захисту визначена, складається програма забезпечення інформаційної безпеки. «Політика безпеки» (є не зовсім точним перекладом англійського словосполучення «security policy»), має на увазі не окремі правила або їх набори, а стратегію організації в галузі інформаційної безпеки. Політика безпеки – сукупність документованих рішень, прийнятих керівництвом організації і спрямованих на захист інформації та асоційованих з нею ресурсів.

Процедурний рівень, орієнтований на людей, а не на технічні засоби. Саме люди формують режим інформаційної безпеки, і вони ж виявляються головною загрозою, тому «людський фактор» заслуговує особливої уваги. Слід усвідомити ту ступінь залежності від комп'ютерної обробки даних, в яку потрапило сучасне суспільство. Акцент слід робити не на військовому чи кримінальному боці справи, а на цивільних аспектах, пов'язаних з підтриманням нормального функціонування апаратного та програмного забезпечення, тобто концентруватися на питаннях доступності та цілісності даних.

Програмно-технічний рівень, тобто рівень, спрямований на контроль комп'ютерних сутностей – обладнання, програм та/або даних, утворюють останній і найважливіший рубіж інформаційної безпеки. Наголошуємо, що збиток наносять в основному дії легальних користувачів, по відношенню до яких процедурні регулятори малоефективні. Головні вороги – некомпетентність і неакуратність при виконанні службових обов'язків, і тільки програмно-технічні заходи здатні їм протистояти.

Доречним є віднесення до рівнів забезпечення інформаційної безпеки ті, які пропонує розглядати В.С. Цимбалюк. За основу поділу він визначає такий критерій, як середовище, в якому знаходиться інформація: а) соціальне середовище (окрема людина, спільноти людей, держава); б) інженерно-технологічне (машинне, апаратно-програмне, автоматичне, телекомунікаційне) середовище; в) соціотехнічне (людино-машинне) середовище. Кожен зазначений рівень щодо середовища об'єктивно доповнює і взаємообумовлює інші рівні, в основі

утворюючи триєдину гіперсистему – систему забезпечення інформаційної безпеки [45, с. 32].

Отже, перераховані рівні забезпечення інформаційної безпеки підкреслюють важливість комплексного підходу до їх впровадження.

Серед складових частин системи інформаційної безпеки важливе місце займає перелік її загроз. Так, вже в згаданому Законі України «Про основи національної безпеки» всі види безпеки, в тому числі й інформаційна, пов'язуються зі станом захищеності життєво важливих інтересів її об'єктів.

Аналіз джерел засвідчує, що деякі вчені ставлять знак рівності між поняттями «загрози інформаційній безпеці» та «загрози національній безпеці та національним інтересам», з чим ми не погоджуємося, бо має місце загальне явище та окреме. Інші науковці розуміють загрози як сукупність умов, процесів та чинників, які перешкоджають реалізації національних інтересів або створюють ім. небезпеку [7, с. 32]. Є думки, що загрози – це конкретні і безпосередні форми небезпеки або сукупність негативних чинників чи умов [46, с. 132]; сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства й держави в інформаційній сфері [47, с. 156]; явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію національних інтересів в інформаційній сфері та створюють небезпеку для системи державного управління, життєзабезпечення її системостворюючих елементів [36, с. 75]; Слід погодитися з тими дослідниками, які вважають загрози сукупністю негативних чинників чи умов. У визначенні їх ролі прийнятою є думка Г.В. Ємел'янова та А.А. Стрельцова: одним з джерел загроз інтересам суспільства в інформаційній сфері є безперервне ускладнення інформаційних систем і мереж зв'язку критично важливих інфраструктур забезпечення життя суспільства [48, с. 15-17].

Отже, загрози інформаційної безпеки є сукупністю дій або подій, які можуть привести до порушення достовірності, цілісності, конфіденційності інформації, яка зберігається, передається або оброблюється.

У питанні про класифікацію зазначених загроз вчені демонструють різні підходи. Окремі з них не подають саму

класифікацію, а лише наголошують на малопродуктивності ізольованого, не комплексного виявлення загроз безпеці та пропонують їх розглядати в комплексі [49, с. 266]. Інша група науковців [50] дає перелік загроз без поділу на групи, виділяючи серед них: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Деякі вчені визначають як загрози інформаційній безпеці узагальнений чинник – криміналізацію інформаційних відносин та зростання кіберзлочинності [51, 52, с. 15], а інші – окремі види правопорушень. Так, Г.М. Лінник [52, с. 15] наголошує, що для кожної країни характерно різне змістовне наповнення та визначення складових національної безпеки, що залежить від інтенсивності, кількості, специфіки потенційних чи реальних загроз у чітко визначений часовий період та соціально-економічного, політичного, культурного тощо потенціалу, а також геополітичних і геостратегічних амбіцій. В.Ю. Триняк [53, с. 11] серед загроз називає небезпеку виникнення нових видів нерівності в суспільстві, що призводить, у свою чергу, до реальної загрози цифрової нерівності та потенційної загрози формування переважно інформаційної еліти суспільства. Небезпека використання результатів процесу інформатизації може викликати реальну загрозу комп'ютерної злочинності. До загроз інформаційній безпеці О.В. Логінов [54, с. 9] відносить інформаційну війну, інформаційне протиборство та інформаційну боротьбу.

Представники третьої групи без критеріїв поділу виокремлюють прямі, непрямі, зовнішні та внутрішні загрози. Інші дослідники формулюють критерії поділу, лише окремих загроз. Зокрема, Л.О. Євдоченко [50, с. 10] виділяє зовнішні і внутрішні загрози національним інтересам України в

інформаційній сфері. О.Л. Морозов [55] крім внутрішніх та зовнішніх, розмежовує існуючі загрози за своєю загальною спрямованістю, а саме на: загрози конституційним правам і свободам людини і громадянина у сфері духовного життя й інформаційної діяльності, індивідуальній, груповій і суспільній свідомості, духовному відродженню України; загрози інформаційному забезпеченню державної політики України; загрози розвиткові вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікацій і зв'язку; загрози безпеці інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються. Але аналізовані підходи, як уявляється, є недосконалими. Найбільш ґрунтовну систему загроз інформаційної безпеки запропонували В.А. Ліпкан, Б.А. Кормич, В.С. Цимбалюк, Г.П. Ситник. Критично оцінивши зазначені думки, вважаємо, що критерій поділу загроз інформаційної безпеки на внутрішні та зовнішні доцільно називати «за напрямами впливу на інформаційну діяльність», на реальні та потенційні – «за ймовірністю дій», а на загальнонаціональні, локальні, індивідуальні – «за масштабом дії». Водночас за критерієм «сфера інформаційної діяльності» пропонуємо взяти за основу Указ Президента України «Про Доктрину інформаційної безпеки України» і виокремити загрози інформаційної безпеки у зовнішньополітичній сфері; у воєнній сфері; у внутрішньополітичній сфері; в економічній сфері; у соціальній та гуманітарній сферах; у науково-технологічній сфері; в екологічній сфері [56]. Звертаємо увагу на те, що в переліку загроз Доктрини подана «сфера державної безпеки», що повністю суперечить науковому підходу, адже «сфера державної безпеки» – це елемент іншої класифікації – за об'єктом загроз, де іншими елементами є безпека суспільства і безпека людини.

Автор пропонує таку систему загроз інформаційній безпеці:

– за ступенем небезпеки – особливо небезпечні, небезпечні;
– за можливістю дії – реальні, потенційні;
– за масштабами дії – національні, локальні, індивідуальні;
– за тривалістю дії – тимчасові, постійні;
– за характером впливу – прямі, безпосередні, опосередковані;

– за терміном дії – довгострокові, середньострокові, короткострокові, поточні;

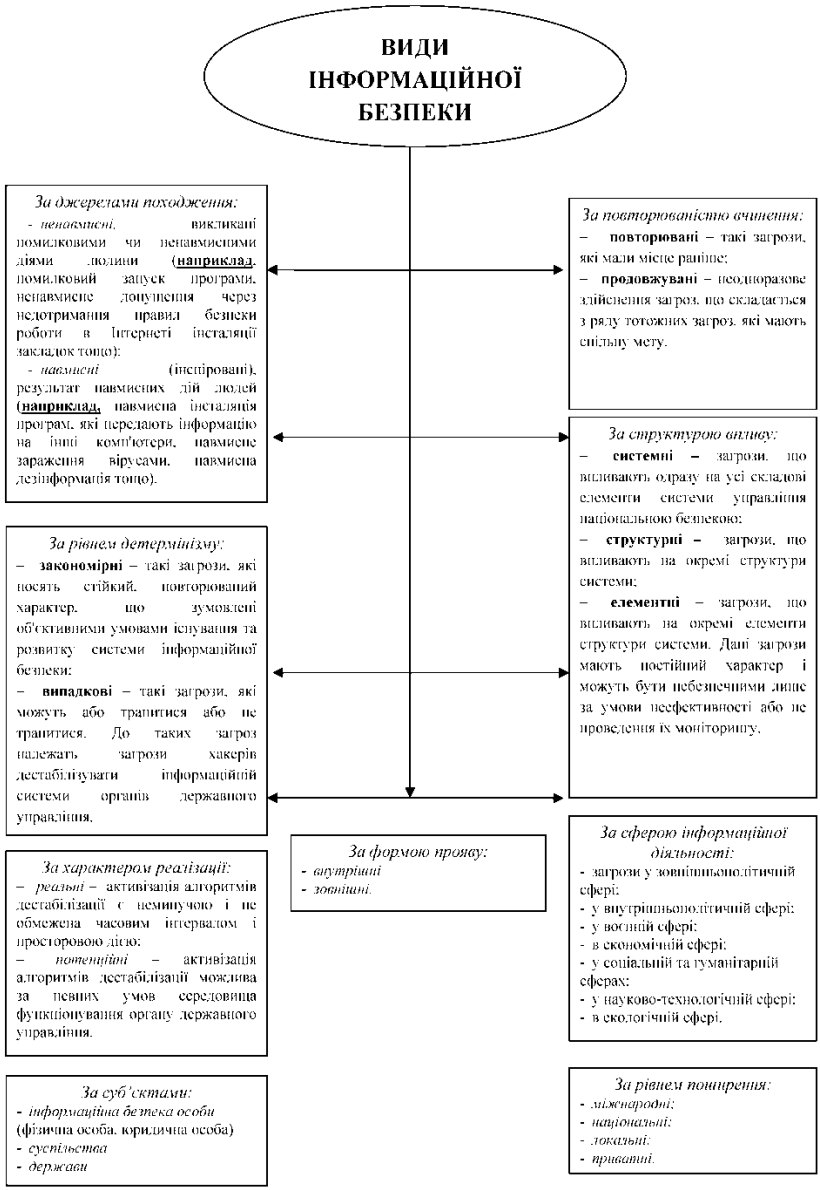
– за сферою інформаційної діяльності – загрози у зовнішньополітичній сфері; у воєнній сфері; у внутрішньополітичній сфері; в економічній сфері; у соціальній та гуманітарній сферах; у науково-технологічній сфері; в екологічній сфері.

Учені одностайні, що існують різні види інформаційної безпеки, а саме: за джерелами походження; за ступенем гіпотетичної шкоди; за повторюваністю вчинення; за сферами походження; за ймовірністю реалізації; за рівнем детермінізму. Вони вважають, що її видами є безпека особи, суспільства, держави [49, с. 278]. Але зазначені підходи свідчать про класифікацію інформаційної безпеки лише за критерієм «суб'єкт». Окремі науковці вказують на критерії об'єднання видів інформаційної безпеки в певні групи. Б.А. Кормич використовує для класифікації загроз різні критерії. Ґрунтуючись на критерії рівня загроз, або простору і масштабами можливих негативних наслідків, виділяє міжнародні (які, в свою чергу поділяються на глобальні та регіональні, в сенсі регіонів світу), національні, локальні (або регіональні у значенні регіонів країни) і приватні (небезпеки фірмам або особистостям) загрози [49, с. 278]. Але назви критеріїв запропонованої системи потребують уточнення.

Автор пропонує залежно від характеру загроз класифікацію інформаційної безпеки за такими критеріями (рис. 1.1).

Більш детально проаналізуємо види інформаційної безпеки за сферою інформаційної діяльності та систему загроз для них.

На сучасному етапі основними реальними та потенційними загрозами інформаційній безпеці України у зовнішньо-політичній сфері є: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; прояви комп'ютерної злочинності, комп'ютерного тероризму, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем; зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет.


ВИДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
За джерелами походження:
- ненавмисні, викликані помилковими чи ненавмисними діями людини (наприклад, помилковий запуск програми, ненавмисне допущення через недотримання правил безпеки роботи в Інтернеті інсталяції закладок тощо);
- навмисні (інспіровані), результат навмисних дій людей (наприклад, навмисна інсталяція програм, які передають інформацію на інші комп'ютери, навмисне зараження вірусами, навмисна дезінформація тощо).
За повторюваністю вчинення:
– повторювані – такі загрози, які мали місце раніше;
– продовжувані – неодноразове здійснення загроз, що складається з ряду тотожних загроз, які мають спільну мету.
За структурою впливу:
– системні – загрози, що впливають одразу на усі складові елементи системи управління національною безпекою;
– структурні – загрози, що впливають на окремі структури системи;
– елементні – загрози, що впливають на окремі елементи структури системи. Дані загрози мають постійний характер і можуть бути небезпечними лише за умови неефективності або не проведення їх моніторингу.
За рівнем детермінізму:
– закономірні – такі загрози, які носять стійкий, повторюваний характер, що зумовлені об'єктивними умовами існування та розвитку системи інформаційної безпеки;
– випадкові – такі загрози, які можуть або трапитися або не трапитися. До таких загроз належать загрози хакерів дестабілізувати інформаційній системі органів державного управління.
За формою прояву:
- внутрішні
- зовнішні.
За сферою інформаційної діяльності:
- загрози у зовнішньополітичній сфері;
- у внутрішньополітичній сфері;
- у воєнній сфері;
- в економічній сфері;
- у соціальній та гуманітарній сферах;
- у науково-технологічній сфері;
- в екологічній сфері.
За характером реалізації:
– реальні – активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом і просторовою дією;
– потенційні – активізація алгоритмів дестабілізації можлива за певних умов середовища функціонування органу державного управління.
За суб'єктами:
- інформаційна безпека особи (фізична особа, юридична особа)
- суспільства
- держави
За рівнем поширення:
- міжнародні;
- національні;
- локальні;
- приватні.

Державній безпеці загрожують: «негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України» та «використання засобів масової інформації, а також мережі Інтернет для пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками». Проте вищеперераховані чинники можуть знаходити своє відображення і в внутрішньополітичному середовищі – на сьогодні відсутня чітка межа між двома зазначеними видами загроз у сфері інформаційної діяльності. Використовуючи такий підхід, ми спостерігаємо вплив різних компонентів інформаційної впливової дії на внутрішню структуру (структуру інтересів – життєвих цінностей, соціальних пріоритетів, внутрішніх настанов), на соціальні об'єкти (соціальні групи, зокрема особистість), а отже, і на зовнішню структуру [57]. У цьому контексті, на наш погляд, очевидним є те, що саме залежність між зовнішньополітичними та внутрішньо-політичними структурами обумовлює причини соціальних конфліктів у суспільстві. Таким чином, наявність можливості (і вміння) здійснювати цілеспрямований інформаційний вплив на зазначені структури суспільства визначає можливість вирішення цих конфліктів політичними засобами. Що, у кінцевому підсумку, характеризує рівень інформаційної і національної безпеки держави.

До найбільш важливих об'єктів забезпечення інформаційної безпеки України у зовнішньополітичній сфері належать: інформаційні ресурси органів виконавчої влади, що реалізують зовнішню політику України, українські представництва та організації за кордоном, представництва України при міжнародних організаціях; блокування діяльності українських засобів масової інформації з роз'яснення зарубіжній аудиторії цілей і основних напрямів державної політики України, її думки з соціально значимих подій українського і міжнародного життя.

Із зовнішніх загроз інформаційної безпеки України у зовнішньополітичній сфері найбільшу небезпеку становлять: інформаційний вплив іноземних політичних, економічних, військових та інформаційних структур на розробку та реалізацію стратегії зовнішньої політики України; поширення за кордоном дезінформації про зовнішню політику України;

порушення прав українських громадян і юридичних осіб в інформаційній сфері за кордоном; спроби несанкціонованого доступу до інформації та впливу на інформаційні ресурси, інформаційну інфраструктуру органів виконавчої влади, що реалізують зовнішню політику України, українських представництв та організацій за кордоном, представництв України при міжнародних організаціях.

Із внутрішніх загроз інформаційної безпеки України у зовнішньополітичній сфері найбільшу небезпеку становлять: порушення встановленого порядку збирання, обробки, зберігання та передачі інформації в органах виконавчої влади, що реалізують зовнішню політику України; інформаційно-пропагандистська діяльність політичних сил, громадських об'єднань, засобів масової інформації та окремих осіб, що спотворює стратегію і тактику зовнішньополітичної діяльності України; недостатня інформованість населення про зовнішньополітичну діяльність України.

Основними заходами щодо забезпечення інформаційної безпеки України у зовнішньополітичній сфері є: розробка основних напрямів державної політики в галузі вдосконалення інформаційного забезпечення зовнішньополітичного курсу України; розробка та реалізація комплексу заходів щодо посилення інформаційної безпеки інформаційної інфраструктури органів виконавчої влади, що реалізують зовнішню політику України, українських представництв та організацій за кордоном, представництв України при міжнародних організаціях; створення українськими представництвами та організаціями за кордоном умов для роботи з нейтралізації поширюваної там дезінформації про зовнішню політику України; вдосконалення інформаційного забезпечення роботи з протидії порушенням прав і свобод українських громадян і юридичних осіб за кордоном; вдосконалення інформаційного забезпечення суб'єктів України з питань зовнішньополітичної діяльності, які входять до їхньої компетенції.

Розглядаючи інформаційну безпеку України у воєнній сфері, необхідно зазначити, що основними реальними та потенційними загрозами в цій галузі є: порушення встановленого регламенту збирання, обробки, зберігання і передачі інформації з обмеженим

доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України; несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони; реалізація програмно-математичних заходів з метою порушення функціонування інформаційних систем у сфері оборони України; перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв'язку та управління; інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби.

Останнім часом безпосередньо в військовій справі рівень інформаційного потенціалу все більшою мірою обумовлює оперативність прийняття рішень, структуру і якість озброєнь, оцінку рівня їх достатності, дієвість пропаганди, ефективність дій союзників і власних збройних сил і, в підсумку, результат збройного протистояння [58].

Значущість інформаційної безпеки як складової воєнної безпеки України пояснюється залежністю реалізації найбільш важливих інтересів України у воєнній сфері від інформаційних загроз. З аналізу найбільш небезпечних загроз важливим національним інтересам України у воєнній сфері [59, с. 3-6]. випливає, що реалізаційною основою більшості цих загроз є інформаційна.

Наведемо найбільш показові приклади. Зокрема, з-поміж інших загроз стабілізації воєнно-політичного стану в Центральній Європі та недопущення збройних конфліктів наведено такі [59, с. 3-6]: висунення територіальних претензій до України; втручання у внутрішні справи України; нестабільність воєнно-політичного стану навколо України; активізація сепаратистських сил і підтримання їх ззовні; заяви та акції, що дискредитують внутрішню і зовнішню політику України; войовничість політичного керівництва сусідніх країн; загострення міжетнічних і міжконфесійних суперечностей; нестабільність соціально-політичного стану в деяких країнах Центральної Європи. Не виникає сумніву те, що всі ці загрози тією чи іншою мірою реалізуються на інформаційному рівні, причому їх інформаційна складова досить вагома. Слід

зазначити, що йдеться не про абсолютизацію інформаційних факторів у реалізації наведених загроз, а про те, що вони, поряд з економічними, політичними, соціальними та іншими факторами, є домінуючими [60, с. 38-45].

Проблема інформаційної безпеки базується на вже сформованій залежності всіх сфер життєдіяльності суспільства і держави – економіки, політики, науки, культури, забезпечення національної та міжнародної безпеки – від нормального обміну інформацією, надійного функціонування інформаційних і телекомунікаційних систем. Тим самим для розвинених країн створюється спокуса використовувати наявні у них переваги (електронно-цифровий розрив) в інформаційних технологіях і засобах маніпулювання суспільною свідомістю для експансії в вищевказаних сферах життєдіяльності, використовуючи поки не обмежений ніякими положеннями міжнародного права абсолютно новий вид зброї – інформаційної [61, с. 143-147].

У сучасних умовах застосування інформаційної зброї як засобу ведення війн може викликати наслідки, цілком порівнянні за силою своєї дії з «традиційною» зброєю масового знищення. Дана теза аж ніяк не випадкова. Аналіз використання сучасних технологій іншими державами вимагає здійснення системи спеціальних заходів щодо забезпечення інформаційної безпеки, в т.ч. міжнародної [62, с. 65-66].

Останнім часом ми спостерігаємо, як Російська Федерація поширює недостовірну, неповну, упереджену інформацію про Україну, через що намагається маніпулювати суспільною свідомістю в Україні та за її межами, що призводить до необхідності вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері. Тому ефективність своєчасного виявлення та нейтралізації розглянутих загроз національній безпеці в воєнній сфері істотно залежить від виваженості й активності заходів щодо забезпечення воєнної безпеки на інформаційному рівні [63, с. 23-25].

Розглядаючи інформаційну безпеку України в економічній сфері, необхідно зазначити, що основними реальними та потенційними загрозами в цій галузі є: відставання вітчизняних наукоємних і високотехнологічних виробництв, особливо у сфері телекомунікаційних засобів і технологій; недостатній

рівень інформатизації економічної сфери, зокрема кредитно-фінансової системи, промисловості, сільського господарства, сфери державних закупівель; несанкціонований доступ, порушення встановленого порядку роботи з інформаційними ресурсами в галузях національної економіки, викривлення інформації в таких ресурсах; використання неліцензованого і несертифікованого програмного забезпечення, засобів і комплексів обробки інформації; недостатній рівень розвитку національної інформаційної інфраструктури. Одним з найважливіших ресурсів будь-якого підприємства є інформація, роль якої зростає по мірі розвитку бізнесу та посилення конкуренції. Володіння інформацією необхідного обсягу, в потрібний час і в потрібному місці, є запорукою успіху в будь-якому виді господарської діяльності. Інформаційна безпека в економічній сфері, захист її від несанкціонованого використання, знищення або зміни, набуває в умовах ринкової конкуренції першочергове значення. Забезпечення безпеки економічних інформаційних систем – це комплекс заходів, спрямованих на захист конфіденційних відомостей у виробничо-господарській, управлінській, науково-технічній та фінансовій сферах. Інформаційна безпека в економічній сфері являє собою комплексну проблему, що охоплює всі стадії обробки і зберігання важливої документації, включаючи бухгалтерську звітність, договори з партнерами, персональні дані клієнтів та іншу фінансово-економічну інформацію, витік якої може привести до серйозних фінансових збитків і необоротних наслідків [64, с. 34-37].

Перехід до ринкових відносин в економіці викликав появу на внутрішньому українському ринку товарів і послуг безліч вітчизняних і зарубіжних комерційних структур, у тому числі виробників і споживачів інформації, засобів інформатизації та захисту інформації. Безконтрольна діяльність цих структур по створенню і захисту систем збору, обробки, зберігання та передачі статистичної, фінансової, біржової, податкової, митної інформації створює реальну загрозу безпеці України в економічній сфері. Аналогічні загрози виникають при безконтрольному залученні іноземних фірм до створення подібних систем, оскільки при цьому складаються сприятливі умови для несанкціонованого доступу до конфіденційної економічної інформації і для контролю за

процесами її передачі та обробки з боку іноземних спецслужб. Широке використання імпортних засобів інформатизації, телекомунікації, зв'язку та захисту інформації створює загрозу виникнення технологічної залежності України в цій сфері від іноземних держав [65, с. 118-120].

Недостатність нормативної правової бази, що визначає відповідальність господарюючих суб'єктів за недостовірність чи приховування відомостей про їх комерційної діяльності, про споживчі властивості вироблених ними товарів і послуг, про результати їх господарської діяльності, про інвестиції і т. п. перешкоджає нормальному функціонуванню економіки країни в цілому.

З іншого боку, істотний економічний збиток господарюючим суб'єктам може бути завдано внаслідок розголошення інформації, яка містить комерційну таємницю. У системах збору, обробки, зберігання та передачі фінансової, податкової, митної інформації найбільш небезпечними є протиправне копіювання інформації або її спотворення внаслідок навмисних порушень технології роботи з інформацією та несанкціонованого доступу до неї. Це стосується і органів виконавчої влади, зайнятих формуванням і поширенням інформації про зовнішньо-економічну діяльність України. Основними заходами щодо забезпечення інформаційної безпеки України у сфері економіки є: організація та здійснення державного контролю за створенням, розвитком і захистом систем і засобів збору, обробки, зберігання та передачі статистичної, фінансової, біржової, податкової, митної інформації; корінна перебудова системи державної статистичної звітності з метою забезпечення достовірності, повноти та захищеності інформації, що здійснюється шляхом введення суворої юридичної відповідальності посадових осіб за підготовку первинної інформації, організацію контролю за діяльністю цих осіб та служб обробки та аналізу статистичної інформації, а також шляхом обмеження комерціалізації такої інформації; розробка національних сертифікованих засобів захисту інформації та впровадження їх у системи та засоби збору, обробки, зберігання та передачі статистичної, фінансової, біржової, податкової, митної інформації; розробка і впровадження національних захищених систем електронних платежів на базі

інтелектуальних карт, систем електронних грошей та електронної торгівлі, стандартизація цих систем, а також розробка нормативної правової бази, що регламентує їх використання; вдосконалення нормативної правової бази, що регулює інформаційні відносини в сфері економіки; вдосконалення методів відбору та підготовки персоналу для роботи в системах збору, обробки, зберігання та передачі економічної інформації.

Розглядаючи інформаційну безпеку України у соціальній та гуманітарній сферах, необхідно зазначити, що основними реальними та потенційними загрозами в цій галузі є: відставання України від розвинутих держав за рівнем інформатизації соціальної та гуманітарної сфер, насамперед освіти, охорони здоров'я, соціального забезпечення, культури; недодержання прав людини і громадянина на одержання інформації, необхідної для захисту їх соціально-економічних прав; поширення в засобах масової інформації невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської і національної гідності; тенденція до витіснення з інформаційного простору та молодіжної культури українських мистецьких творів, народних традицій і форм дозвілля; послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства; відставання рівня розвитку українського кінематографу, книговидання, книго розповсюдження та бібліотечної справи від рівня розвинутих держав.

Першочерговими завданнями держави щодо забезпечення інформаційної безпеки у соціальній та гуманітарній сферах є неухильне забезпечення конституційного права кожного на одержання, використання, поширення та зберігання інформації, на вільне вираження своїх поглядів на основі ефективного використання новітніх засобів обміну інформацією; вироблення та просування на світовому рівні власного інформаційного продукту [66].

На тлі стрімкої глобалізації у світі, де панують новітні технології та інформаційна уніфікованість, досі не подолане відставання у сфері комунікаційних технологій – особливо важливій в епоху інформаційних суспільств. Це загрожує національній безпеці України, бо вже призвело до значної

інформаційної та технологічної залежності від іноземних держав та міжнародних медіа-структур.

Для подолання цих явищ необхідне:

– прискорення реформування національної медійної та комунікаційної систем, модернізація їх стандартів, створення системи суспільного мовлення;

– забезпечення незалежності та плюралізму засобів масової інформації та їх залучення до інтеграції України у глобальний інформаційний простір;

– впровадження та поширення сучасних інформаційних технологій;

– недопущення монополізації інформаційного ринку України;

– забезпечення вигідного для українських виробників місця у світовому поділі праці у сфері інформаційних послуг;

– забезпечення захисту громадян від інформаційної продукції, що негативно впливає на фізичний, психічний, інтелектуальний та моральний розвиток людини;

– удосконалення національного інформаційного законодавства щодо забезпечення отримання громадянами суспільно значущої інформації і чітке визначення процедури доступу до інформації;

– удосконалення організаційних та правових засад національного інформаційного ринку;

– розвиток електронних інформаційних технологій у системі управлінських структур;

– активізація державної політики шляхом розробки законодавства у сфері захисту вітчизняного Інтернет-простору та розвитку Інтернет-послуг, у тому числі для безпеки вітчизняних Інтернет-ресурсів і нейтралізації несанкціонованих втручань у користування інформаційними послугами.

Розглядаючи загрози інформаційної діяльності, нам також необхідно розглянути проблеми, які виникають з цього приводу в науково-технологічній сфері. Ці загрози, в першу чергу, стосуються витоку за кордон наукових кадрів та суб'єктів права інтелектуальної власності; низька конкурентоспроможність вітчизняної інформаційної продукції на світовому ринку; недостатній захист від несанкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій та техніки.

Сьогодні українська наука перебуває у вкрай критичному стані, який не тільки не відповідає потребам сучасної якісної освіти, а й створює реальну загрозу безпеці держави взагалі та інформаційній зокрема [67, с. 48-50].

З точки зору інформаційної безпеки науково-технічної сфери можна говорити про те, що, по-перше, в широкому сенсі її безпека залежатиме від внутрішніх інформаційних зв'язків між усіма складовими даної системи (внутрішній аспект) та зовнішніх зв'язків зі світовим інформаційним простором, в якому знаходиться науково-технічна інформація (зовнішній аспект). У вузькому сенсі вона залежатиме від ефективності системи захисту інформації, що охороняється з обов'язковим забезпеченням можливості доступу до цієї інформації, іншими суб'єктами. Ґрунтуючись на обліку всіх складових інформаційної безпеки в науково-технічній сфері, можна оцінити її стан, в якому вирішальну роль відіграє оцінка реальних і потенційних загроз. Доцільно їх умовно розділити за такими основними параметрами: на загальні та спеціальні загрози.

До загальних загроз ми відносимо: 1) розрив потоків інформації між: а) наукової та науково-технічної сферами; б) науково-технічної та економічної сферами; 2) односторонній характер зовнішніх зв'язків з акцентом на надання науково-технічної інформації зовнішньому споживачеві; 3) обмеженість доступу до світових інформаційних ресурсів; 4) неясність державної науково-технічної політики; 5) догляд науково-технічних кадрів – носіїв інформації в інші сфери діяльності.

До загроз спеціального характеру відносимо: 1) проникнення зовнішніх суб'єктів до частини науково-технічної інформації, що захищається через: а. агентурне проникнення; б. технічне проникнення; 2) витік науково-технічних кадрів за кордон («витік мізків»); 3) інформаційний вплив зовнішніх суб'єктів (дезінформування і т. п.).

Даний перелік може бути уточнений і розширений. Однак, як видається, він відповідає основному завданню – можливості принципової оцінки основних загроз для інформаційної безпеки науково-технічної сфери.

Розглядаючи інформаційну безпеку України в екологічній сфері, необхідно зазначити, що основними реальними та

потенційними загрозами в цій галузі є: приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації чи надзвичайні ситуації техногенного та природного характеру; недостатня надійність інформаційно-телекомунікаційних систем збирання, обробки та передачі інформації в умовах надзвичайних ситуацій; низький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпечних об'єктів і територій, завчасного прогнозування та реагування на надзвичайні ситуації.

В умовах деградації навколишнього природного середовища, погіршення екологічних умов існування людини, виснаження природних ресурсів та порушення екологічного балансу особливого значення набувають саме правові засоби забезпечення законності в екологічній сфері. Складний стан довкілля віддзеркалює негативні, не завжди прогнозовані наслідки науково-технічного прогресу. Ускладнює ситуацію недостатня поінформованість громадян про свої права в екологічній сфері та можливості їх реалізації, а також досить часта відсутність доступу до екологічної інформації, яка б дала можливість об'єктивно оцінити ситуацію.

Одним з головних пріоритетів розвитку України є побудова соціально-орієнтованого, відкритого, демократичного суспільства, в якому кожен міг би створювати, накопичувати, поширювати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, реалізуючи тим самим свій потенціал, можливості соціального зростання. Для забезпечення становлення інформаційного суспільства в Україні держава повинна впливати не лише на інформаційну сферу, а й на інші сфери суспільних відносин. Таким чином, побудова інформаційного суспільства, як якісно нового цивілізаційного етапу його розвитку, повинна сприйматися як загальна стратегічна мета діяльності держави в цілому, що полягає у трансформації всього комплексу суспільних відносин, з акцентом на розвиток інформаційних та інформаційно-інфраструктурних відносин. Однією зі сфер, яка потребує належного інформаційного забезпечення у цьому контексті, є екологічна сфера [68, с. 3]. Охорона життя і здоров'я людини від

несприятливого впливу довкілля тривалий час була предметом розгляду в межах загального захисту екологічних інтересів суспільства. Закріплення у ст. 50 Конституції України права фізичних осіб на безпечне для життя і здоров'я довкілля зумовило подальшу розробку належного механізму його реалізації та захисту на галузевому рівні. Нині особливу роль у сфері забезпечення та захисту права особи на безпечне для життя і здоров'я довкілля, інших конституційних екологічних прав відіграють інформаційно-правові засоби.

Для розгляду інформаційної безпеки держави необхідно розкрити зміст понять «забезпечення інформаційної безпеки», «система забезпечення інформаційної безпеки», «механізм забезпечення інформаційної безпеки», «Стратегія забезпечення інформаційної безпеки». Ці питання частково розглядаються розглядали В.А. Ліпкан, О.С. Ліпкан, О.І. Пастернак-Таранушенко, Г.М. Лінник та інші. Однак потребують дослідження такі елементи системи забезпечення, як наукове, політичне забезпечення та зміст правового забезпечення інформаційної безпеки.

Під забезпеченням безпеки взагалі і інформаційної зокрема фахівці розуміють: діяльність держави і всього суспільства, спрямовану на захист національних інформаційних інтересів [55]; реалізацію (захист) національних інтересів [69, с. 132-137]. Існує думка, що забезпечення безпеки включає кадрове, матеріально-технічне, науково-методичне, інформаційне забезпечення [70, с. 212-219.]. На нашу думку, пропоновані визначення слід уточнити з урахуванням змісту поняття «інформаційна безпека» і, відповідно, забезпечення інформаційної безпеки визначити як діяльність, спрямовану на захист інформаційних інтересів особи, суспільства, держави, її адміністративно-територіальних утворень з метою гарантування інформаційної незалежності України та захисту її інформаційної системи від внутрішніх і зовнішніх загроз. На нашу думку, слід розрізняти поняття «система забезпечення інформаційної безпеки», «механізм забезпечення інформаційної безпеки»; систему забезпечення інформаційної безпеки розглядати як сукупність елементів, з яких така система складається (у вузькому розумінні), а механізм та стратегію забезпечення (у широкому розумінні). Колектив авторів

навчального посібника «Основи інформаційного права України» [71, с. 114] під категорією «інформаційна система» розуміють організаційно упорядковану та оформлену множину людей, даних (документів), інформаційних потоків, каналів зв'язку, технічних і технологічних засобів, що забезпечують взаємозв'язок між складовими системи соціального управління з метою її ефективного функціонування і розвитку. Дещо по-іншому систему забезпечення інформаційної безпеки розглядає В.А. Ліпкан, а саме як сукупність інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об'єктів інформаційної безпеки, а також інфраструктури її забезпечення [7, с. 133]. Схожу позицію демонструють й ті дослідники, які систему забезпечення безпеки розглядають як сукупність організаційно об'єднаних органів управління, сил та засобів, призначених для розв'язання завдань щодо забезпечення безпеки [7, с. 208].

На сьогодні зміст окремих елементів системи забезпечення інформаційної безпеки не визначені ні у нормативних актах, ні вченими. Зокрема, дослідники, вказуючи на існування інформаційного забезпечення як елемента такої системи, не розглядають його зміст та особливості. На наш погляд, інформаційне забезпечення – це комплекс організаційних, технічних, технологічних заходів, засобів та методів щодо локалізації потенційних загроз інформаційної безпеки.

Окремою складовою вважаємо політичне забезпечення інформаційної безпеки, сутністю якої, на наш погляд, є утвердження демократичних форм і інститутів. Чітке розмежування компетенції органів законодавчої, виконавчої та судової влади у сфері інформаційної безпеки. Так, основним завданням органів законодавчої влади є встановлення найважливіших правил поведінки у сфері інформаційної діяльності, виконавчої влади – здійснення державної політики щодо забезпечення інформаційної безпеки, судової – у твердження верховенства права шляхом захисту гарантованих Конституцією і законами України інформаційних інтересів держави, суспільства, фізичних та юридичних осіб.

Важливим елементом є кадрове забезпечення. Оскільки склад кадрів впливає на вирішення відповідними органами завдань і функцій у сфері забезпечення інформаційної безпеки. З іншого боку, недостатній професіоналізм, рівень матеріального забезпечення та соціальні гарантії, плинність кадрів можуть бути причинами вчинення ними неправомірних діянь у інформаційній сфері, а тому, враховуючи результати проведеного нами анкетування, визначаємо такі напрями кадрового забезпечення: вдосконалення системи добору, підготовки, соціального захисту кадрів; запровадження підготовки юристів із спеціалізації «Інформаційне право», «Забезпечення інформаційної безпеки держави», «Інформація з обмеженим доступом».

Основним напрямом наукового забезпечення – є здійснення науково-аналітичної та прогнозної діяльності науково-дослідними установами, з метою прогнозування та оцінки можливих внутрішніх і зовнішніх загроз, інформування державних органів про них, проведення наукових досліджень, видання наукових праць у зазначеній сфері.

Забезпечення інформаційної безпеки неможливо без оперативно-розшукового забезпечення – сукупності оперативно-розшукових засобів, спрямованих на отримання та обмін необхідною оперативно-розшуковою інформацією щодо фактів правопорушень у сфері інформаційної діяльності. Така інформація може свідчити про поширення певних інформаційних правопорушень, використовуватися для інформування відповідних державних органів як привід і підстава для порушення кримінальної справи, для упередження та припинення злочинів і розшуку злочинців, причетних до їх вчинення [72, с. 51] та застосовуватися у досудових та судових стадіях [73, с. 349]. Окремими напрямами оперативного забезпечення дослідники вважають діяльність спільних оперативних груп, взаємодію оперативних та контролюючих органів шляхом швидкого інформування останніми про виявлені порушення [74, с. 108]. На нашу думку, оперативне забезпечення займає важливе місце у системі забезпечення інформаційної безпеки через змогу специфічними засобами своєчасно реагувати на скоєні правопорушення суб'єктів інформаційного права. З огляду на те, що стан інформаційної

безпеки багато в чому визначається рівнем правового регулювання, а причиною правопорушень є недосконаліть законодавства [75, с. 23], вважаємо найважливішим елементом системи забезпечення інформаційної безпеки її правове забезпечення.

Адміністративно-правовою наукою питання правового забезпечення інформаційної безпеки не досліджено. На нашу думку, сутністю правового забезпечення інформаційної безпеки є здійснюване державою за допомогою системи правових засобів упорядкування суспільних відносин у цій сфері, їх юридичне закріплення та охорона, а його механізмом – система таких правових засобів. Відповідно, завданням правового забезпечення інформаційної безпеки вважаємо створення досконалої правової бази та системи контролю за інформаційною діяльністю з метою забезпечення стабільності інформаційної системи, попередження, виявлення та припинення правопорушень суб'єктами інформаційного права.

Правову основу у сфері інформаційної безпеки держави складають Декларація про державних суверенітет України від 16 липня 1990 р. [76], Конституція України [77], кодифіковані законодавчі акти, які містять норми про відповідальність за правопорушення у сфері інформаційної діяльності [78; 79; 80], Основи національної безпеки України від 19 червня 2003 р. [81]. Значна кількість правовідносин у сфері забезпечення інформаційної безпеки регулюється нормами заковів України, указів та розпоряджень Президента України. В умовах інтеграційних процесів зростає роль норм міжнародно-правових актів у захисті інформаційної системи.

З огляду на викладене вище, система забезпечення інформаційної безпеки у широкому розумінні також включає механізм та стратегію її забезпечення.

Поняття механізму забезпечення інформаційної безпеки ні законодавцями, ні науковцями не визначено. На нашу думку, механізм забезпечення інформаційної безпеки є системою різних засобів (політичних, кадрових, оперативно-розшукових, інформаційних, правових), за допомогою яких забезпечується захист інформаційних інтересів держави, суспільства, особи від внутрішніх і зовнішніх загроз.

У аналізованій системі окремим елементом є стратегія забезпечення інформаційної безпеки, яку вчені вважають наукою і мистецтвом ефективного використання національної могутності для досягнення бажаного рівня реалізації національних інтересів і досягнення національних цілей [82, с. 222], планом (програмою) дій [83, с. 35]. Як бачимо, дослідники досить стисло формулюють її зміст (у другому визначенні) та мету (у першому визначенні).

Заслуговують уваги думки О.І. Барановського про стратегію, як систему конкретних заходів, спрямованих на реалізацію намічених цілей [84, с. 24] та Г.І. Пастернак-Таранушенко про включення до неї не лише результатів і заходів, а й засобів та методів, що мають бути використані [85, с. 13]. Підтримуємо розуміння стратегії як прийнятої у державі системи поглядів на характер сучасних загроз і небезпек, на цілі й завдання, форми і способи захисту та реалізації національних інтересів [82, с. 222]. Разом із тим уточнюємо, що це документ, який включає перелік основних загроз інформаційній безпеці України за сферою інформаційної діяльності (загрози у зовнішньополітичній сфері; у внутрішньополітичній сфері; у воєнній сфері; в економічній сфері; у соціальній та гуманітарній сферах; у науково-технологічній сфері; в екологічній сфері) та визначає напрями запобігання їм.

Розділ 2
ПРАВОВІ АСПЕКТИ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАЦІЙ

2.1. Теоретичні аспекти функціонування системи інформаційної безпеки корпорацій

У сучасних економічній та юридичній науках корпорація є одним з найголовніших об'єктів дослідження. Така ситуація виникла не випадково, оскільки корпорації за останні півтори століття стрімко розвивались, активно і постійно трансформувались, розповсюджувались у всьому світі. Вони завоювали панівне становище в світовій ринковій економічній системі, швидко завойовують його в економіках навіть слаборозвинутих країн.

Сутність поняття «корпорація» науковці трактують по-різному. У найзагальнішому вигляді корпорація – це організаційна структура, яка об'єднує необхідні ресурси для виробництва товарів та надання послуг населенню. Ця форма організації досить поширена в усіх країнах, оскільки вона: а) обмежує фінансовий ризик акціонерів унаслідок виключення за чинним законодавством їхньої відповідальності перед кредиторами товариства за межами капіталу, що розміщений в акціях; б) робить можливим залучення капіталу за рахунок випуску додаткової кількості акцій та емісії інших цінних паперів; в) продовжує діяльність навіть після зміни складу акціонерів; г) сприяє отриманню інвестицій на вигідних умовах; д) дає змогу власникам корпорацій успішно реалізовувати стратегічні плани на засадах колективних інтересів; е) пропонує працівникам участь у розподілі прибутків та капіталу; ж) створює механізм повернення вкладених у статутний капітал коштів шляхом продажу акцій; з) забезпечує контроль за діяльністю управлінського апарату тощо [86, с. 116].

Приведемо визначення сутності поняття «корпорація» окремими вченими. Так, Г.Б. Кочетков, В.Б. Супян доводять, що: «корпорация – это важнейший институт современной экономики. В промышленности развитых стран она является неотъемлемым атрибутом» [87, с. 23]. С.А. Румянцев надає корпораціям наступне визначення: «Корпорація – це система виборних та призначених органів, які здійснюють управління діяльністю відкритих акціонерних товариств, що відображає баланс інтересів власників і спрямована на збереження максимально можливого прибутку від усіх видів діяльності товариства згідно з нормами чинного законодавства.» [88, с. 13]. Розглядаючи поняття корпорації, І.Б. Гурков зауважує, що вони демонструють приголомшливі темпи розвитку, «при цьому не стільки у кількісному виразі (об'єми продаж, географічний розмах операцій, кількість зайнятих), скільки в якісному виразі – за складністю і відповідальністю завдань, які слід вирішувати» [89, с. 7].

Такі вчені, як Н.В. Мочерний, О.А. Устенко, С.І. Чеботар, визначають поняття корпорації як найдосконалішу форму організації підприємств, що існує переважно у вигляді акціонерного товариства, засновники якого формують акціонерний капітал шляхом об'єднання власних ресурсів через механізм випуску і продажу цінних паперів (передусім акцій), а співвласники несуть обмежену відповідальність [90, с. 108]. З.С. Варналій розглядає корпорації як договірні об'єднання, створені на основі поєднання виробничих, наукових та комерційних інтересів, з делегуванням окремих повноважень централізованого регулювання діяльності кожного з учасників [91, с. 69]. Досить вдало, на наш погляд, визначають сутність поняття та ознаки корпорації С.Ф. Покропивний та В.М. Колот, а саме: а) корпорація є найефективнішою формою організації підприємницької діяльності з огляду на реальну можливість залучення необхідних інвестицій. Саме через ринок цінних паперів вона може об'єднувати різні за розмірами капітали великої кількості фізичних і юридичних осіб для фінансування сучасних напрямків науково-технічного й організаційного прогресу, нарощування виробничого потенціалу; б) потужній корпорації значно простіше постійно збільшувати обсяги виробництва або послуг. Це дає добру можливість отримувати

постійно зростаючий прибуток; в) кожний акціонер, як співвласник корпорації, несе лише обмежену відповідальність (за банкрутства фірми він втрачає тільки вартість своїх акцій). Важливо й те, що окрема особа може зменшити свій власний фінансовий ризик, якщо купуватиме акції кількох корпорацій. Кредитори можуть пред'явити претензії лише корпорації як юридичній особі, а не окремим акціонерам як фізичним особам; г) корпорація – це організаційно-правове утворення, яке може функціонувати дуже тривалий період (постійно), що створює необмежені можливості для перспективного розвитку [92, с. 22].

Погодимось із твердженням Н.С. Глусь, яка визначає поняття корпорації як акціонерного товариства чи товариства з обмеженою відповідальністю або товариства з додатковою відповідальністю, управління яким здійснюється через складну централізовану систему органів, учасники якої відносно неї здійснюють інвестиційну діяльність з метою отримання дивідендів [93, с. 3].

У розумінні К. Майєра корпоративна форма бізнесу – корпорація – це група осіб, які надали певній своїй частині юридично визнане право бути самостійним утворенням з власними правами, привілеями та обов'язками (на відміну від тих, що властиві всім членам товариства) [94, с. 25].

Вичерпне визначення поняття корпорації подає Д.М. Розенберг, а саме: «Корпорація – це організація, що поставила перед собою визначені цілі, діє для суспільного блага, має певні права, є юридичною особою, діє на постійній основі та несе обмежену відповідальність» [95, с. 105].

Джеймс Уорті та Роберт Нейшел визначають корпорацію як суму зобов'язань, виділяючи серед проблем корпорацій законність корпоративної влади, корпоративну підзвітність, перед ким і за що корпорація має відповідальність, хто і за якими нормами повинен нею управляти [96, с. 36].

У довідкових виданнях та юридичній літературі існує декілька підходів до визначення сутності поняття «корпорація»: а) поняття «корпорація» походить від латинського слова «corporation», що означає об'єднання, товариство [97, с. 356]; б) група осіб, об'єднаних вузько фаховими, становими та іншими інтересами [98, с. 245]; в) корпорація – це об'єднання [99, с. 5]; г) це об'єднана група, коло осіб однієї професії, одного

стану; одна із форм монополістичного об'єднання [100, с. 298]; д) договірне об'єднання, створене на основі поєднання виробничих, наукових і комерційних інтересів підприємств, що об'єдналися [101, с. 63]; е) товариство, сукупність осіб, об'єднаних на основі комерційних та інших інтересів [102, с. 294]; є) корпорація – це акціонерна компанія [103, с. 172].

З урахуванням вищезазначеного вважаємо за доцільне дати наступне визначення поняття корпорації: це акціонерне товариство, яке діє на підставі статуту, забезпечує постійну оптимізацію доходів акціонерів та забезпечує діяльність товариства завдяки ефективному управлінню та врахуванню інтересів зацікавлених осіб.

Законодавче регулювання процесів створення і діяльності корпорацій в Україні почало формуватися на початку 90-х років після здобуття нею політичної та економічної незалежності. Загалом, розвиток корпорації і корпоративного законодавства в Україні можна поділити на кілька етапів.

У 1991 р. приймається низка законодавчих актів з правового регулювання підприємницької діяльності: закони України «Про підприємництво» [104], «Про власність» [105] та «Про цінні папери і фондову біржу» [106]. Ухвалення цих нормативних актів заклало правові засади для розвитку в Україні ринкових відносин, вперше було визначено учасників таких відносин – це підприємці різних організаційно-правових форм, включаючи товариства. Правовий статус господарських товариств як корпоративних суб'єктів підприємницької діяльності був закріплений у спеціальному законодавчому акті – Законі України «Про господарські товариства» від 19 вересня 1991 р. [107], що складається з 83 статей, присвячених питанням створення, функціонування і припинення діяльності господарських товариств. У цьому нормативному акті вирізняються вже п'ять форм господарських товариств: акціонерне, з обмеженою відповідальністю, з додатковою відповідальністю, повне і командитне.

У 1992 р. було прийнято низку приватизаційних законів, зокрема це закони України: «Про приватизацію державного майна» [108], «Про приватизацію невеликих державних підприємств (малу приватизацію)» [109] та «Про приватизаційні папери» [110]. Ці законодавчі акти поклали

початок процесам приватизації державної власності та створення акціонерних товариств і товариств з обмеженою відповідальністю на базі майна колишніх державних підприємств. У подальші роки корпоративні структури розвивалися під впливом процесів приватизації та корпоратизації, діяльності інвестиційних посередників, таких, як довірчі та страхові товариства, інвестиційні фонди і компанії. Упродовж 1996-2002 рр. було істотно переглянуто норми корпоративного законодавства, зокрема:

– внесено значні зміни до законів України «Про господарські товариства», «Про підприємництво»;

– суттєво вдосконалено законодавство про цінні папери і фондовий ринок (прийнято закони України «Про державне регулювання ринку цінних паперів в Україні» від 30 жовтня 1996 р., «Про національну депозитарну систему та особливості електронного обігу цінних паперів в Україні» від 10 грудня 1997 р.);

– прийнято низку законодавчих актів, що регулюють діяльність інститутів спільного інвестування (корпоративних та пайових інвестиційних фондів), а також діяльність на ринках фінансових послуг (закон України «Про інститути спільного інвестування (пайові та корпоративні інвестиційні фонди)» від 15 березня 2001 р. та «Про фінансові послуги та державне регулювання ринків фінансових послуг» від 12 липня 2001 р.).

Разом з тим формується система недержавного регулювання діяльності господарських товариств – емітентів цінних паперів (переважно акціонерних товариств) і професійних учасників фондового ринку – через систему організацій, провідними серед яких є Українська фондова біржа, Перша Фондова торговельна система, Професійна асоціація реєстраторів та депозитаріїв.

На наш погляд, важливо наголосити, що створення дедалі більшої кількості корпорацій в Україні, залучення великих інвесторів (фізичних та юридичних осіб, включаючи іноземців) у корпоративні відносини, активізація фондового ринку супроводжується недостатньою ефективністю та недосконалістю чинного законодавства в цій сфері правового регулювання, що найчастіше призводить до порушення прав учасників корпорацій. Постає проблема негайного і належного

врегулювання на законодавчому рівні процесів ефективної діяльності цих об'єднань.

До прийняття нового Закону України «Про акціонерні товариства» та нового Цивільного кодексу України окремі питання вирішувалися на підзаконному рівні. Відповідно до указів Президента України «Про додаткові заходи щодо розвитку фондового ринку України» від 26 березня 2001 р., «Про заходи щодо розвитку корпоративного управління в акціонерних товариствах» від 21 березня 2002 року Державною комісією з цінних паперів та фондового ринку України було узгоджено Рекомендації з найкращої практики корпоративного управління для акціонерних товариств України (протокол від 2 червня 2002 р. № 8). Прийняття Закону України «Про акціонерні товариства» зумовлено вступом у дію з 1 січня 2004 р. Цивільного кодексу України, який прямо передбачає існування в законодавстві України спеціального «акціонерного» закону. Кодекс істотно змінює усталені норми, що регулюють діяльність акціонерних товариств, але детально не описує порядку їхнього застосування й містить посилання на спеціальний закон, яким мають конкретизуватися ті чи інші норми. Як бачимо, прийняття окремого закону про акціонерні товариства набуло обов'язкового характеру.

Останнім етапом розвитку на шляху створення необхідної правової бази щодо регулювання діяльності вітчизняних корпорації можна вважати прийняття 17 вересня 2008 року Верховною Радою України Закону України «Про акціонерні товариства» [111].

Враховуючи історичний та сучасний досвід розвитку корпорацій в Україні, необхідно зробити акцент на адміністративно-правовому аспекті функціонування системи інформаційної безпеки в корпораціях. Визначальним елементом цієї системи є її мета. Забезпечення інформаційної безпеки корпорацій досягається у процесі свідомої цілеспрямованої діяльності керівних органів корпорації щодо запобігання можливого порушення її звичайного функціонування в результаті дії загроз та небезпек.

Метою забезпечення інформаційної безпеки корпорацій є створення реальних умов діяльності самої корпорації, а також проведення моніторингу стану інформаційної безпеки для

розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки.

Виходячи з наведеного, метою функціонування системи забезпечення інформаційної безпеки корпорацій є організація управління системою інформаційної безпеки через ефективне функціонування самої системи її забезпечення. У більш загальному плані мета полягає у створенні необхідних економічних та правових механізмів формування розвитку і забезпечення ефективного використання інформаційних ресурсів корпорації.

Ефективність системи управління інформаційними ресурсами корпорації та її захистом значною мірою визначає загальний рівень національної безпеки, а будь-які недоліки в структурі й функціонуванні корпорації призводить до непоправних збитків в самій корпорації. Необхідно враховувати, що побудова системи інформаційної безпеки в корпорації неминуче наштовхується на різні протистояння, які необхідно врегульовувати в установленому в корпорації порядку з урахуванням норм чинного законодавства. Існують типові алгоритми локалізації загроз і етапи формування системи інформаційної безпеки, які застосовуються при створенні будь-якої системи безпеки [112, с. 95-99]. Так, наприклад, цілісна система інформаційної безпеки повинна передбачати як профілактичну, так і внутрішню оперативну роботу. Профілактична робота допускає використання технічних методів і способів контролю, однак можливість їх проведення стосовно співробітників повинна бути, в обов'язково порядку, закріплена письмовою згодою самого працівника. Внутрішня оперативна робота – це процес виявлення інформації небезпечного характеру. До основних етапів формування системи інформаційної безпеки корпорацій можна віднести наступні: ідентифікація джерел загроз і ризиків для бізнесу; оцінка ступеня серйозності загрози; вибір та застосування оптимального алгоритму локалізації загроз (побудова системи захисту) з урахуванням виділеного на це бюджету. Необхідно зазначити, що повсякденна практика недержавних об'єктів свідчить про їх підвищену порівняно з державними структурами уразливість від протиправних та інших посягань з боку різного роду кримінальних структур, а також окремих осіб. Власність тепер зобов'язує корпорації займатись

діяльністю, яка раніше була виключно прерогативою спеціальних державних органів. Забезпечення безпеки приватної діяльності стає важливою необхідністю, є підґрунтям функціонування недержавних об'єктів. Отже, охорона корпорацій і забезпечення інформаційної безпеки корпоративної діяльності є стрижневою проблемою, що обіймає комплекс організаційно-правових, техніко-технологічних, інформаційних, адміністративних, виховних, фінансових і спеціальних заходів, спрямованих на виявлення, попередження і припинення загроз і зазіхань на стабільність функціонування і розвитку корпорацій. Цей процес містить у собі безпеку інформації, охорону приватної власності корпорацій і фізичний захист його персоналу. При цьому до власності відносять, по-перше, основне матеріальне майно: приміщення, земельна ділянка, парк техніки, сировина й інвентар, а також допоміжне устаткування, призначене для збереження, переробки і перевезення вантажів. По-друге, сюди ж варто віднести інтелектуальну власність, що складає інформацію, яка є активом компанії про власність власника, а також знання і досвід співробітників корпорацій, їхні професійні секрети і винаходи. Корпорації, які прагнуть мати власну службу безпеки, не повинні розглядати витрати на її створення, як необґрунтовано високі, оскільки життя та репутація цінується набагато вище. Нещастям корпорацій є те, що, заробивши великі гроші, вони не хочуть усвідомлювати, що багатство неминуче переводить їх у «групу ризику». Як показує сумний досвід, наші корпорації починають здійснювати суттєві кроки із забезпечення власної безпеки, безпеки інформації лише після того, як у них починаються неприємності [113, с. 817-821].

Таким чином зрозуміло, що без конкретних завдань щодо забезпечення інформаційної безпеки корпорацій не можливо уявити майбутнє цього сектору економіки. Отже, головним завданням системи забезпечення інформаційної безпеки корпорацій є створення умов для організації управління системою інформаційної безпеки.

До основних завдань системи забезпечення інформаційної безпеки корпорацій можна віднести наступні:

– забезпечення інформаційної безпеки корпорацій на всіх рівнях;

– моніторинг (спостереження, оцінка і прогноз) стану інформаційної безпеки корпорацій у зв'язку із впливом загроз та небезпек як зсередини, так і ззовні;

– протидія технічному проникненню до інформаційної системи корпорацій з метою вчинення злочинів;

– забезпечення збереження комерційної таємниці.

З огляду на завдання, які постають перед системою забезпечення інформаційної безпеки корпорацій, доцільно визначити її функції.

Під такими ми розуміємо здійснення керівними органами організаційної діяльності зі створення умов для оптимального управління системи інформаційної безпеки корпорацій.

До основних функцій системи забезпечення інформаційної безпеки корпорацій слід віднести:

І. Створення та забезпечення діяльності елементів системи забезпечення інформаційної безпеки корпорацій, що включає:

– розроблення адміністративно-правових засад для побудови та функціонування системи інформаційної безпеки корпорацій;

– системне забезпечення діяльності елементів системи: аналітичне, інформаційне, адміністративно-правове, матеріально-технічне, кадрове, ресурсне забезпечення;

– розробка й прийняття управлінських рішень щодо забезпечення системи управління інформаційними ресурсами корпорацій та удосконалення механізмів реалізації правових норм щодо них.

ІІ. Управління системою інформаційної безпеки корпорацій – здійснення свідомого цілеспрямованого впливу корпорацій на загрози та небезпеки, внутрішні та зовнішні чинники, що впливають на стан інформаційної безпеки:

– розроблення на підставі концепції інформаційної безпеки корпорацій конкретних планів та технологій забезпечення інформаційної безпеки відповідно до потреб кожного підрозділу корпорацій;

– здійснення прогнозування, планування, організації, регулювання та контролю усією системою інформаційної безпеки та окремими її елементами;

– оцінка результативності дій, витрат на проведення заходів щодо забезпечення інформаційної безпеки корпорацій;

– оптимізація внутрішніх документів корпорацій щодо забезпечення науково-технічних, виробничо-технологічних, організаційно-економічних умов створення та застосування інформаційних технологій, інших елементів інформаційної інфраструктури для формування розвитку та ефективного використання інформаційних ресурсів корпорації.

III. Здійснення планової та оперативної діяльності щодо забезпечення інформаційної безпеки корпорацій:

– визначення інтересів кожного підрозділу корпорацій в інформаційній сфері та їх пріоритетності відповідно до цілей корпорації;

– діагнозування загроз та небезпек, виявлення джерел їх виникнення, а також прогнозування можливих наслідків;

– визначення і здійснення повноважень корпорацій щодо оперативного управління (володіння, розпорядження, користування) інформаційними ресурсами;

– забезпечення функціонування ефективно діючої комплексної системи захисту інформаційних ресурсів корпорації.

IV. Здійснення організаційних та матеріально-технічних заходів забезпечення інформаційної безпеки корпорацій:

– розробка і реалізація фінансово-економічних засад регулювання процесів формування та використання інформаційних ресурсів корпорації;

– забезпечення повноти створення первинних і похідних інформаційних ресурсів на засадах використання інформації, що виникає (створюється) у процесів діяльності корпорацій;

– введення технологічно та методологічно єдиних засад формування інформаційних ресурсів за результатами діяльності корпорації;

забезпечення захисту системи корпорацій від хибної, спотвореної та недостовірної інформації;

– інформаційно-аналітичне забезпечення прийняття управлінських рішень у сфері управління інформаційними ресурсами корпорації;

– кадрове забезпечення;

– забезпечення розробки та застосування організаційних та економічних механізмів стосовно форм та засобів обігу інформаційних ресурсів корпорації (інформаційних технологій,

засобів обробки інформації та інформаційних послуг) [114, с. 117-120].

V. Здійснення контрольно-наглядової діяльності щодо забезпечення інформаційної безпеки корпорації:

– забезпечення ефективного використання інформаційних ресурсів в корпорації;

– контроль за встановленим порядком і правилами формування, розвитку і використання інформаційних ресурсів корпорації;

– нагляд за додержанням законодавства в сфері формування, розвитку, використання інформаційних ресурсів корпорації.

Враховуючи викладені вище думки щодо поняття системи забезпечення інформаційної безпеки корпорацій, основ її формування та функціонування, захисту та призначення, мети, завдань та функцій, а також з урахуванням напрацювань з даних та інших споріднених питань, структура даної системи повинна мати наступний вигляд:

Стратегічний рівень.

Верховна Рада України:

- визначає засади зовнішньої та внутрішньої політики держави в інформаційній сфері;
- здійснює законодавче регулювання політики національної безпеки України в інформаційній сфері (нормативно закріплює права і свободи людини і громадянина в інформаційній сфері, гарантії цих прав і свобод; основні обов'язки громадянина; закріплює основи національної безпеки, засади цивільно-правової відповідальності; визначає діяння, які є злочинами, адміністративними або дисциплінарними правопорушеннями, та відповідальність за них);
- створює правові засади функціонування системи забезпечення національної безпеки в інформаційній сфері;
- затверджує загальнодержавні програми в цій сфері та контролює хід їх виконання;
- затверджує бюджетні асигнування для фінансування діяльності із забезпечення національної безпеки в інформаційній сфері;
- визначає порядок створення та повноваження Ради національної безпеки і оборони України;

- призначає за поданням Президента України, Прем'єр-міністра України, Міністра оборони України, Міністра закордонних справ України, Голови Служби безпеки України;
- призначає на посади та звільняє половини складу Національної ради України з питань телебачення і радіомовлення.

Президент України здійснює загальне керівництво у сфері інформаційної безпеки України, а саме:

- очолює Раду національної безпеки і оборони України;
- здійснює керівництво в інформаційній та інших сферах національної безпеки та оборони України;
- здійснює контроль і координацію діяльності державних органів у забезпеченні національної безпеки в інформаційній та інших сферах;
- вживає оперативні заходи з метою нейтралізації загроз національним інтересам України в межах компетенції, визначеної Конституцією;
- один раз на рік на сесії Верховної Ради звітує перед народом України про стан національної безпеки України;
- забезпечує взаємодію усіх гілок державної влади між собою, а також із недержавною складовою системи забезпечення національної безпеки в інформаційній сфері;
- видає нормативно-правові акти з питань забезпечення національної безпеки в інформаційній сфері;
- визначає реальні та потенційні загрози та небезпеки для національної безпеки в інформаційній сфері та вживає необхідних заходів з її забезпечення.

Кабінет Міністрів України у сфері забезпечення інформаційної безпеки:

- забезпечує інформаційний суверенітет України, здійснення внутрішньої і зовнішньої інформаційної політики держави, виконання Конституції і законів України, актів Президента України, що стосуються інформаційної безпеки;
- вживає заходів щодо забезпечення прав і свобод людини і громадянина в інформаційній сфері;
- забезпечує проведення державної політики інформаційної безпеки;

- спрямовує і координує роботу усієї системи органів державного управління з питань, що стосуються інформаційної безпеки;
- визначає потреби в витратах на забезпечення інформаційної безпеки, забезпечує виконання затвердженого Верховною Радою України Державного бюджету України щодо фінансування заходів у сфері інформаційної безпеки у визначених обсягах;
- організовує розроблення і виконання державних програм з розвитку інформаційної інфраструктури органів державного управління;
- здійснює передбачені законодавством заходи щодо формування, розміщення, фінансування та виконання державного оборонного замовлення на поставку (закупівлю) продукції, виконання робіт, надання послуг для потреб органів, що забезпечують інформаційну безпеку;
- встановлює порядок надання суб'єктам забезпечення інформаційної безпеки у користування державного майна, засобів зв'язку і радіочастотного ресурсу, комунікацій, інших об'єктів інфраструктури держави, навігаційної, топогеодезичної, метеорологічної, гідрографічної та іншої інформації;
- забезпечує комплектування особовим складом сили забезпечення інформаційної безпеки;
- утворює, реорганізовує, ліквідовує науково-дослідні установи, навчальні заклади та окремі кафедри (відділення, факультети) суб'єктів забезпечення інформаційної безпеки;
- забезпечує реалізацію права на соціально-економічний захист відповідно до законодавства України, що регламентує діяльність окремих суб'єктів забезпечення інформаційної безпеки;
- здійснює у визначених законом випадках регулювання господарської діяльності у суб'єктах забезпечення інформаційної безпеки;
- встановлює відповідно до закону порядок реалізації та утилізації об'єктів інформаційної інфраструктури, інформаційних ресурсів;
- забезпечує здійснення, передбачених законодавством заходів, щодо цивільної оборони України, надання військової

допомоги іншим державам, направлення підрозділів Збройних сил України до інших держав, допуску та умов перебування підрозділів збройних сил інших держав на території України та участі України в міжнародних миротворчих операціях;

- контролює виконання законів у сфері оборони, здійснює відповідно до законів інші заходи щодо забезпечення обороноздатності України, координує і контролює їх виконання та несе, в межах своїх повноважень, відповідальність за забезпечення.

Тактичний рівень.

Міністерства та інші центральні органи виконавчої влади в межах своїх повноважень:

- забезпечують реалізацію законів України, указів та розпоряджень Президента України, концепцій, доктрин, програм, постанов органів державного управління у сфері інформаційної безпеки;
- забезпечують створення, підтримку в готовності і застосування сил та засобів забезпечення інформаційної безпеки, а також управління їх діяльністю;
- у межах своєї компетенції розробляють нормативні правові акти в інформаційній сфері і представляють їх Президентові України та Кабінету Міністрів України;
- вносять в органи виконавчої влади пропозиції по удосконалення функціонування системи забезпечення інформаційної безпеки України;
- керують діяльністю підвідомчих організацій з планування і проведення заходів по забезпеченню інформаційної безпеки;
- забезпечують дотримання прав і законних інтересів громадян, організацій і держави, законів та інших нормативно-правових актів в інформаційній сфері;
- притягують до відповідальності посадових осіб, дії яких призводять до порушення національних інтересів в інформаційній сфері, створюють умови або безпосередню загрозу інформаційній безпеці України.

Органи місцевого самоврядування та місцеві державні адміністрації забезпечують вирішення питань у сфері інформаційної безпеки України у відповідних адміністративно-територіальних одиницях, а саме:

- забезпечують виконання Конституції та законів України, рішень Конституційного Суду України, актів Президента України, Кабінету Міністрів України, інших органів державної влади в сфері забезпечення інформаційної безпеки;
- забезпечують здійснення заходів щодо охорони громадської безпеки, громадського порядку, боротьби зі злочинністю в інформаційній сфері;
- здійснюють заходи щодо організації правового інформування та інформаційного виховання населення;
- проводять роботу, пов'язану з розробленням та здійсненням заходів щодо інформаційного забезпечення біженців, а також депортованих осіб, які добровільно повертаються в регіони їх колишнього проживання;
- забезпечують виконання законодавства щодо національних меншин і міграції, про свободу думки і слова, свободу світогляду і віросповідання;
- оголошують у разі стихійного лиха, аварій, катастроф, епідемій, енізоотій, пожеж, інших надзвичайних подій зони надзвичайної ситуації; здійснює передбачені законодавством заходи, пов'язані із забезпеченням інформаційної безпеки, захистом інформаційних прав особи;
- забезпечують своєчасне інформування населення про загрозу виникнення або виникнення надзвичайних ситуацій під час проведення потенційно небезпечних заходів в умовах присутності цивільного населення за участю особового складу Збройних сил України, інших військових формувань та правоохоронних органів з використанням озброєння і військової техніки.

Оперативний рівень.

Діяльність МВС України в інформаційній сфері держави здійснюється властивими їй формами та методами, передбаченими законами України «Про національну поліцію» [115], «Про оперативно-розшукову діяльність» [116], «Про боротьбу з тероризмом» [117], «Про запобігання корупції» [118], «Про організаційно-правові основи боротьби з організованою злочинністю» [119], «Про очищення влади» [120] у тісній взаємодії з іншими суб'єктами забезпечення національної безпеки та спрямована на нейтралізацію загроз національним інтересам і національній безпеці України.

Відповідно до п. 3 Указу Президента України «Про Положення про Міністерство внутрішніх справ України» [121] серед основних завдань МВС України є:

- організація і координація діяльності органів внутрішніх справ щодо захисту прав і свобод громадян, інтересів суспільства і держави в інформаційній сфері від протиправних посягань на них, охорони громадського порядку і забезпечення громадської безпеки в інформаційній сфері;
- участь у розробленні та реалізації державної політики щодо боротьби із кіберзлочинністю та кібертероризмом;
- забезпечення запобігання злочинам в інформаційній сфері, їх припинення, розкриття і розслідування, розшуку осіб, які вчинили злочини, вжиття заходів до усунення причин і умов, що сприяють вчиненню правопорушень;
- організація охорони та оборони внутрішніми військами особливо важливих державних об'єктів, зокрема об'єктів критичної інфраструктури держави тощо.

Діяльність Служби безпеки України в інформаційній сфері держави здійснюється властивими їй формами та методами, передбаченими законами України «Про Службу безпеки України» [122], «Про оперативно-розшукову діяльність» [116], «Про прокуратуру [123], «Про боротьбу з тероризмом» [117], «Про запобігання корупції» [118], «Про Раду національної безпеки і оборони України» [124] у тісній взаємодії з іншими суб'єктами забезпечення національної безпеки та спрямована на нейтралізацію загроз національним інтересам і національній безпеці України, визначеним у ст. 7 Закону України «Про основи національної безпеки України» [5]:

- постійний моніторинг впливу на національну безпеку процесів, що відбуваються, в першу чергу, в інформаційній, політичній, соціальній, економічній, екологічній, науково-технологічній, воєнній та інших сферах, релігійному середовищі, міжетнічних стосунках; прогнозування змін, що відбуваються в них, та потенційних загроз національній безпеці;
- систематичне спостереження за станом і проявами міжнародного та інших видів тероризму (зокрема й кібертероризму);

- прогнозування, виявлення, та оцінка можливих загроз, дестабілізуючих чинників і конфліктів, причин і умов їх виникнення та наслідків прояву;
- комплексне інформаційно-аналітичне забезпечення діяльності вищих органів державної влади та інших суб'єктів забезпечення національної безпеки України в інформаційній сфері;
- розроблення науково обґрунтованих пропозицій і рекомендацій щодо прийняття управлінських рішень з метою захисту національних інтересів України;
- запобігання та нейтралізація впливу загроз і дестабілізуючих чинників на національну безпеку та національні інтереси в інформаційній сфері;
- локалізація, деескалація та врегулювання конфліктів, ліквідація їх негативних наслідків або впливу дестабілізуючих чинників;
- оцінка результативності дій щодо забезпечення національної безпеки в інформаційній сфері та визначення витрат на ці цілі;
- участь у двосторонньому і багатосторонньому співробітництві в галузі інформаційної безпеки, якщо це відповідає національним інтересам України;
- спільне проведення планових та оперативних заходів з компетентними структурами іноземних держав у рамках міжнародних організацій та договорів у галузі безпеки.

Державна служба спеціального зв'язку та захисту інформації України забезпечує формування і реалізацію державної політики у сферах захисту державних інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, криптографічного та технічного захисту інформації, використання і захисту державних електронних інформаційних ресурсів, телекомунікацій, користування радіочастотним ресурсом України; приймає участь у формуванні і реалізації державної політики у сфері електронного документообігу органів державної влади та органів місцевого самоврядування, розробленні та впровадженні електронного цифрового підпису в органах державної влади та органах місцевого самоврядування; забезпечує в установленому порядку урядовим зв'язком Президента України, Голови Верховної Ради України, Прем'єр-

міністра України, інших посадових осіб органів державної влади, місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного та воєнного стану, а також у разі виникнення надзвичайної ситуації; забезпечує функціонування, безпеки та розвитку державної системи урядового зв'язку і Національної системи конфіденційного зв'язку; розробляє та здійснює заходи щодо розвитку телекомунікаційних мереж, поліпшення їх якості, забезпечення доступності і сталого функціонування; сприяє інтеграції сфер телекомунікацій, користування радіочастотним ресурсом України у світовий інформаційно-комунікаційний простір.

Суди загальної юрисдикції здійснюють судочинство у справах про злочини, що завдають шкоди інформаційній безпеці України.

Прокуратура України здійснює повноваження щодо забезпечення національної безпеки України в інформаційній сфері відповідно до Конституції України та Закону України «Про прокуратуру України» [123]. Прокуратура України становить єдину систему, на яку покладаються:

- підтримання державного обвинувачення в суді, зокрема за справами щодо посягань у сфері інформаційних правовідносин;
- представництво інтересів громадянина або держави в суді у випадках, визначених законом;
- нагляд за додержанням законів органами, які проводять оперативно-розшукову діяльність, дізнання» досудове слідство за справами щодо посягань у сфері інформаційних правовідносин;
- нагляд за додержанням законів під час виконання судових рішень у кримінальних справах щодо посягань у сфері інформаційних правовідносин, а також під час застосування інших заходів примусового характеру, пов'язаних з обмеженням особистої свободи громадян, зокрема в інформаційній сфері;
- нагляд за додержанням прав і свобод людини і громадянина в інформаційній сфері, додержанням законів з цих питань органами виконавчої влади, органами місцевого самоврядування, їх посадовими і службовими особами.

Правовий статус Ради національної безпеки і оборони України щодо забезпечення національної безпеки України в інформаційній сфері визначений у Конституції України, в законах України «Про основи національної безпеки України» [5] та «Про Раду національної безпеки і оборони України» [124]. Серед основних завдань є:

- внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики в інформаційній та інших сферах національної безпеки і оборони;
- координація та здійснення контролю за діяльністю органів виконавчої влади в інформаційній та інших сферах національної безпеки й оборони у мирний час;
- координація та здійснення контролю за діяльністю органів виконавчої влади в інформаційній та інших сферах національної безпеки й оборони в умовах воєнного або надзвичайного стану та під час виникнення кризових ситуацій, що загрожують національній безпеці України.

Основними завданнями Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки є:

- здійснення аналізу стану і можливих загроз національній безпеці України в інформаційній сфері та узагальнення міжнародного досвіду щодо формування та реалізації інформаційної політики;
- здійснення аналізу здійснення галузевих програм і виконання заходів, пов'язаних із реалізацією міністерствами та іншими центральними органами виконавчої влади державної політики в інформаційній сфері;
- розроблення і внесення Президентові України та РНБО України пропозицій щодо:

– визначення національних інтересів України в інформаційній сфері, концептуальних підходів до формування державної інформаційної політики та забезпечення інформаційної безпеки держави;

– здійснення системних заходів, спрямованих на вдосконалення інформаційної політики України, реалізацію державної стратегії розвитку і захисту національного інформаційного простору та входження України у світовий інформаційний простір;

– удосконалення системи правового та наукового забезпечення інформаційної безпеки України;

– розвиток інформаційної інфраструктури в державі, зокрема з питань модернізації її матеріально-технічної бази та належного фінансового забезпечення;

– організація та порядок міжвідомчої взаємодії міністерств, інших центральних органів виконавчої влади у сфері забезпечення інформаційної безпеки;

– удосконалення системи оперативного інформаційно-аналітичного забезпечення Президента України, зокрема альтернативною інформацією у сфері національної безпеки й оборони.

Основними завданнями Державного комітету телебачення і радіомовлення України з питань інформаційної політики та інформаційної безпеки є:

- участь у формуванні та забезпечення реалізації державної політики в інформаційній та видавничій сферах, державної політики у сфері захисту суспільної моралі;
- міжгалузева координація та функціональне регулювання з питань діяльності інформаційної та видавничої сфер;
- здійснення управління в інформаційній та видавничій сферах;
- сприяння реалізації конституційного права на свободу слова, забезпечення розвитку інформаційної сфери, розширення національного інформаційного простору.

Державне агентство з питань електронного урядування України є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України через Віце-прем'єр-міністра України – Міністра регіонального розвитку, будівництва та житлово-комунального господарства і який реалізує державну політику у сфері інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства.

Основними завданнями Агентства є:

- реалізація державної політики у сфері інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства;

- координує діяльність органів виконавчої влади, пов'язану із створенням та інтеграцією електронних інформаційних систем і ресурсів в Єдиний веб-портал органів виконавчої влади та наданням інформаційних та інших послуг через електронну інформаційну систему «Електронний Уряд»;
- створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів;
- розробляє і здійснює разом з іншими органами виконавчої влади та органами місцевого самоврядування заходи щодо розвитку інформаційного суспільства;
- координує адміністрування адресного простору українського сегмента Інтернету;
- визначає у межах повноважень, передбачених законом, особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом тощо.

Державний комітет телебачення і радіомовлення України є головним у системі центральних органів виконавчої влади з формування та реалізації державної політики у сфері телебачення і радіомовлення, в інформаційній та видавничій сферах.

Основними завданнями Держкомтелерадіо України є формування та реалізація державної політики у сфері телебачення і радіомовлення, інформаційній та видавничій сферах, поліграфії.

Держкомтелерадіо України відповідно до покладених на нього завдань:

- розробляє заходи щодо запобігання внутрішньому і зовнішньому інформаційному впливу, який загрожує інформаційній безпеці держави, суспільства, особи;
- бере участь у формуванні єдиного інформаційного простору, сприянні розвитку інформаційного суспільства;
- реалізує разом з іншими державними органами завдання щодо забезпечення інформаційної безпеки тощо.

Національна комісія з утвердження свободи слова та розвитку інформаційної галузі здійснює свою діяльність відповідно до Положення про Національну комісію з утвердження свободи слова та розвитку інформаційної галузі,

затвердженого Указом Президента України № 493/2006 від 6 червня 2006 р.

Основними завданнями Комісії є:

- підготовка пропозицій щодо виконання зобов'язань України, які випливають з її членства в Раді Європи, ОБОЄ, інших міжнародних організаціях, а також досягнення Україною відповідності політичній складовій Копенгагенських критеріїв 1993 року щодо набуття членства в ЄС в частині забезпечення стабільності та ефективності функціонування відповідних інститутів, які гарантують демократію, принципи свободи слова та розвиток засобів масової інформації та виконання відповідних положень Плану дій «Україна-ЄС»;
- проведення моніторингу ефективності реалізації законів та інших нормативно-правових актів щодо свободи слова та розвитку інформаційної галузі, їх відповідності стандартам Ради Європи, ОБСЄ, інших міжнародних організацій та вимогам політичної складової Копенгагенських критеріїв і відповідних положень Плану дій «Україна-ЄС» та підготовка проектів відповідних законодавчих, інших нормативно-правових актів;
- підготовка довідкових матеріалів з питань відповідності стандартам Ради Європи, ОБСЄ, інших міжнародних організацій, вимогам політичної складової Копенгагенських критеріїв, виконання відповідних положень Плану дій «Україна-ЄС», вжиття заходів до висвітлення цієї роботи в засобах масової інформації;
- опрацювання пропозицій щодо запровадження європейських стандартів в інформаційній галузі, зокрема щодо:

– реформування державних та комунальних засобів масової інформації;

– створення та розвитку системи суспільних (громадських) засобів масової інформації;

– впровадження цифрового телебачення та інших новітніх інформаційних технологій;

– розвитку українського сегменту мережі Інтернет;

– вдосконалення системи підготовки та перепідготовки працівників засобів масової інформації.

Особливість реальних функцій забезпечення інформаційної безпеки полягає у тому, що кожний орган держави здійснює власну діяльність на базі використання інформаційної

інфраструктури суспільства, виробляє і споживає інформаційні ресурси, має певні відносини з юридичними особами як власник інформаційних ресурсів, має вживати певні дії щодо забезпечення збереження ресурсів і безпеки функціонування інформації і телекомунікаційних систем управління.

Реалізація окремих положень щодо збереження інформації в корпораціях особливим чином відображено в Законі України «Про акціонерні товариства» на прикладі реалізації норм оприлюднення інформації в використанні. Забезпечення безпеки інформації в корпораціях закріплене в ст. ст. 9, 10 Закону України «Про інформацію» [39], ст. ст. 25, 26 Закону України «Про акціонерні товариства» (щодо права акціонера на інформацію про діяльність акціонерного товариства), ст. 77 Закону ПАТ (щодо інформації про товариство), а також ст. 78 надання акціонерним товариством інформації [111].

Надання інформаційних послуг корпораціями через мережу Інтернет повинно супроводжуватися постійним моніторингом загроз та небезпек, які можуть вплинути на безперебійне функціонування веб-сайтів. Одна з вимог вказаної норми полягає в тому, що інформація розміщена на веб-сайтах корпорацій, повинна мати захист від несанкціонованої модифікації.

Передбачається, що інформаційне наповнення, захист інформації від несанкціонованої модифікації та технічне забезпечення функціонування веб–сайтів корпорації здійснюють самостійно. У свою чергу, контроль за дотриманням вимог щодо захисту інформації, доступної через Веб-портал, здійснюється Департаментом спеціальної телекомунікаційної системи та захисту інформації СБУ.

2.2. Особливості реалізації адміністративно-правових форм та методів у сфері забезпечення інформаційної безпеки корпорацій

Забезпечення інформаційної безпеки корпорацій здійснюється за допомогою загальноприйнятих адміністративно-правових форм. Виокремимо ті з них, які відповідають меті нашого дослідження.

Під адміністративно-правовою формою забезпечення інформаційної безпеки корпорацій необхідно розуміти:

– характерну діяльність учасників корпорації по забезпеченню інформаційної безпеки, через яку відбувається реалізація їх функцій;

– конкретні, здійснювані в межах певних правових, організаційних рамок дії учасників корпорації та посадових осіб за допомогою яких реалізовується їх компетенція;

– здійснення передбачених нормативно-правовими актами видів дій учасниками корпорації, за допомогою яких реалізовується їх завдання по забезпеченню інформаційної безпеки корпорацій.

Таким чином, під адміністративно-правовою формою забезпечення інформаційної безпеки корпорацій ми розуміємо здійснення передбаченими нормативно-правовими актами характерної діяльності учасників корпорації, за допомогою якої відбувається реалізація їх функцій по забезпеченню інформаційної безпеки.

Названі форми поділяються на правові та не правові. Зміст діяльності корпорацій, множинність суб'єктів управління нею, особливості їх правової структури, функціонального призначення дозволяють вести мову про наявність системи форм забезпечення інформаційної безпеки, а, відповідно, і про можливість її класифікації [125, с. 46-48]. Класифікація необхідна для найповнішого з'ясування сутності різновиду форми регулювання у сфері інформаційної безпеки. Можна обирати різні критерії для класифікаційного розподілу форм регулювання у сфері інформаційної безпеки корпорацій. В якості базового може виступити розподіл форм забезпечення інформаційної безпеки в залежності від характеру наслідків її застосування. А саме, за цим критерієм можна виділити:

1) правові форми забезпечення інформаційної безпеки корпорацій, що викликають чітко виражені зовнішні юридичні наслідки для всіх учасників корпоративних відносин. Така форма притаманна всім суб'єктам управління корпоративною діяльністю, оскільки вони всі є суб'єктами нормотворчої діяльності в сфері інформаційної безпеки. Інша справа, що є державні суб'єкти, що приймають загальнообов'язкові правила поведінки (наприклад, Державна комісія з цінних паперів та

фондового ринку щодо безпеки інформації про випуск цінних паперів, що пропонуються для відкритого продажу та порядок реєстрації випуску цінних паперів та інформації про їх випуск [125, с. 46-48]); Президент України в межах його компетенції (зокрема, шляхом прийняття Указу від 17 червня 1997 року «Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин»; Розпорядження Президента України від 26.04.2014 № 762/2014-рп «Про деякі заходи щодо забезпечення безпеки в інформаційній сфері»). Таким чином, правова форма забезпечення інформаційної безпеки корпорацій може знаходити прояв у наступних різновидах:

– прийнятті нормативно-правових актів: наприклад, Закон України Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки [126]; Розпорядження Кабінету Міністрів України 15 травня 2013 р. № 386-р «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» [127];

– прийняття індивідуальних актів: наприклад, Рішення Національної комісії з цінних паперів та фондового ринку від 03.12.2013 № 2826 «Про затвердження Положення про розкриття інформації емітентами цінних паперів» [128]; Рішення Національної комісії з цінних паперів та фондового ринку №1249 «Про затвердження Змін до Положення про порядок складання та розкриття інформації компаніями з управління активами та особами, що здійснюють управління активами недержавних пенсійних фондів, та подання відповідних документів» [129]; Рішення Національної комісії з цінних паперів та фондового ринку від 25.12.2012 №1857 «Про схвалення Концептуальних засад функціонування загальнодоступної інформаційної бази даних Національної комісії з цінних паперів та фондового ринку про ринок цінних паперів» [130]; Рішення Національної комісії з цінних паперів та фондового ринку від 03.06.2014 № 733 «Про затвердження Положення про формування інформаційної бази даних про ринок цінних паперів» [131].

– укладання адміністративних договорів: наприклад Національна комісія, що здійснює державне регулювання у

сфері ринків фінансових послуг уклала Угоду про інформаційне співробітництво з Національною комісією з цінних паперів та фондового ринку.

2) неправові форми забезпечення інформаційної безпеки корпорацій, які не спричиняють зовнішніх юридичних наслідків для суб'єктів корпорацій. Неправові форми забезпечення інформаційної безпеки корпорацій – це повсякденні та різноманітні види діяльності, необхідні для забезпечення чіткої та ефективної роботи всіх суб'єктів корпорацій в Україні в сфері безпеки інформації [125, с. 46-48]. Вони також досить різноманітні за зовнішніми проявами. До них можна віднести: організаційно-правові заходи: наприклад, Про схвалення проекту рішення Національної комісії з цінних паперів та фондового ринку «Про внесення Змін до Порядку складання та подання запитів на публічну інформацію, розпорядником якої є Національна комісія з цінних паперів та фондового ринку»; участь Національної комісії з цінних паперів та фондового ринку в обговоренні нагальних проблем кібербезпеки, виявлення спільних рішень, запобігання загроз, забезпечення ефективного захисту і безпеки активів в кіберпросторі під час проведення Міжнародної науково-практичної конференції «Кібербезпека-2013»; матеріально-технічні операції: наприклад, Про внесення змін до рішення Національної комісії з цінних паперів та фондового ринку від 08 травня 2012 року № 646 «Про затвердження Системи довідників та класифікаторів Національної комісії з цінних паперів та фондового ринку для використання учасниками фондового ринку України»; Про схвалення проекту рішення «Про затвердження Положення про формування інформаційної бази даних про ринок цінних паперів».

При здійсненні корпораціями своїх функцій щодо забезпечення інформаційної безпеки важливу роль відіграють засоби та прийоми, що застосовуються в межах вищезазначених адміністративно-правових форм з метою реалізації завдань і функцій.

Метод передбачає певну послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіювати в залежності від типу діяльності корпорації, в якій вони використовуються, а також сфери застосування. Як і форми, методи діяльності корпорацій класифікуються за

чисельними критеріями [132, с. 16-20; 133, с. 21-24]. Водночас, на наш погляд, ураховуючи той факт, що методи застосовуються в межах тих форм, які ми окреслили вище, зосередимо увагу на адекватних групах методів адміністративно-правових та організаційних.

Перш ніж досліджувати методи забезпечення інформаційної безпеки корпорацій зазначимо, що деякі автори характеризують методи управління, виходять з численних управлінських зв'язків, які виникають між суб'єктами та об'єктами управління [134, 135], інші – із взаємозв'язку учасників управління сил та засобів, які використовуються для впливу на об'єкти [136, с. 28]. Як одні, так і інші автори використовують єдиний інструментарій – відносини у сфері управління корпорацією (управлінські зв'язки), знаряддя та засоби (політика їх застосування), якими наділений вищезазначений суб'єкт [137, с. 177].

Під адміністративно-правовим методом розуміється сукупність прийомів впливу, що містяться в адміністративно-правових нормах за допомогою яких встановлюється юридично-владне становище сторін у правовідносинах [138, с. 36].

Сказане дозволяє зосередити увагу в цьому дослідженні на основних методах адміністративного права – переконанні та примусі.

Виходячи з мети та завдання дослідження, ми зосередимо свою увагу саме на особливостях застосування адміністративного примусу в сфері забезпечення інформаційної безпеки корпорацій.

Адміністративний примус – це застосування у передбачених законом формах і порядку уповноваженими на те органами або їх осадовими особами до окремих суб'єктів права примусових заходів морального, матеріального чи фізичного впливу з метою забезпечення громадського порядку та громадської безпеки, попередження та припинення правопорушень, а також покарання та виховання правопорушників [139, с. 98].

У своїй докторській дисертації «Адміністративно-правовий примус у механізмі забезпечення особистої безпеки» П.В. Діхтієвський стверджує, що адміністративний примус в системі механізмів громадської і державної безпеки являє собою особливого роду діяльність щодо застосування засобів,

прийомів правового впливу на фізичних і юридичних осіб, що створюють загрозу безпеці держави. Автор додає, що основним критерієм для класифікації заходів адміністративного примусу, відводиться безпосередня мета застосування тих чи інших заходів [140, с. 124].

Необхідно зазначити про погляди вчених–адміністративістів на підстави адміністративного примусу. Більшість вчених, таких як: Ю.П. Битяк, С.Т. Гончарук, Т.О. Коломоєць, Г.М. Остапович, В.О. Продаєвич та ін. пов'язують втілення в життя заходів адміністративного примусу з виявленням правопорушення та з настанням обставин, що містять у собі небезпеку завдання шкоди суспільним відносинам. Таким чином, адміністративний примус застосовується для: а) припинення протиправних дій; б) покарання правопорушників в адміністративному порядку; в) для забезпечення суспільної безпеки в умовах надзвичайного стану.

Таким чином, адміністративні методи становлять собою основні групу засобів охорони піднаглядних об'єктів від різного роду неправомірних посягань. Не завжди така діяльність закінчується застосуванням заходів стягнення. Значна частка примусового впливу керівних органів корпорацій на піднаглядні суб'єкти носить директивних характер і не пов'язана безпосередньо із застосуванням адміністративних санкцій [141, с. 133].

На сьогоднішній день існує велика кількість наукових робіт, присвячених особливостям заходів адміністративного примусу та їх класифікації, що говорить про підвищений інтерес з боку вчених до даної тематики. Однак, єдності думок щодо питання класифікації заходів адміністративного примусу не спостерігається.

Як зазначає Т.О. Коломоєць переважна більшість вчених-юристів дотримуються традиційної трьохчленної (рідко чотирьохчленної) класифікації заходів адміністративного примусу [142, с. 148]. Наприклад, З.С. Гладун виділяє заходи адміністративного попередження, заходи адміністративного припинення із деталізацією їх на загальні, спеціальні та процесуальні та адміністративні стягнення [143, с. 92]. І.П. Голосніченко погоджується з запропонованою тричленною класифікацією заходів і виділяє наступні: адміністративно-

попереджувальні заходи; заходи адміністративного припинення та забезпечення адміністративного провадження; адміністративні стягнення [144, с. 20].

В комплексі заходів адміністративного примусу щодо мети та характеру їх впливу С.Т. Гончарук виділяє теж три групи заходів: а) заходи адміністративного попередження (запобіжно-профілактичні); б) заходи адміністративного припинення; в) адміністративні стягнення. Також автор вбачає доцільність виділення серед вказаних заходів ще двох специфічних груп, зокрема: а) заходів забезпечення провадження в справах про адміністративні правопорушення; б) адміністративно-відновлювальні заходи [139, с. 74-75].

С. Мазурін, Л. Попов, Ю. Козлов пропонують виділяти заходи адміністративного попередження, адміністративного припинення, адміністративної відповідальності, адміністративно-процесуального забезпечення без внутрішньої класифікації [145, с. 151].

Найбільш обґрунтовано, на нашу думку, є класифікація заходів адміністративного примусу, яку запропонував С.О. Мосьондз, а саме: адміністративного попередження; адміністративного припинення з деталізацією на заходи припинення загального та спеціального призначення та заходи адміністративної відповідальності [146, с. 102]. Як можна помітити, майже усі автори виділяють серед заходів адміністративного примусу заходи припинення і стягнення. Щодо таких видів заходів як адміністративно-запобіжних та адміністративно-забезпечувальних у вчених-адміністративістів єдиної думки немає.

Перейдемо до втілення в життя адміністративно-запобіжних, адміністративно-забезпечувальних заходів, а також заходи відповідальності за порушення адміністративно-правових установлень.

Насамперед метою застосування адміністративно-запобіжних заходів є відвернення або зменшення шкідливих наслідків, які можуть настати внаслідок надзвичайних обставин та/або інших причин, не пов’язаних з вчиненням правопорушення. Завдяки цьому відмежування адміністративно-запобіжних заходів від інших заходів адміністративного примусу, на нашу думку, може відображатися через такі

елементи: а) відсутність зв'язку з неправомірною поведінкою учасника; б) вище зазначена мета застосування таких заходів.

Таким ознакам відповідають такі примусові заходи:

– Національна комісія з цінних паперів та фондового ринку має право звертатися до суду з позовом (заявою) про припинення акціонерного товариства внаслідок:

✓ допущення при його створенні порушень, які неможливо усунути;

✓ неподання акціонерним товариством НКЦПФР протягом двох років поспіль інформації, передбаченої законом (Стаття 8 Закону «Про державне регулювання ринку цінних паперів» доповнено п. 311);

✓ Частини 2 ст. 38 Закону «Про державну реєстрацію юридичних осіб та фізичних осіб – підприємців», що визначає підстави для постановлення судового рішення щодо припинення юридичної особи, що не пов'язане з банкрутством юридичної особи, доповнено такими підставами:

✓ неподання акціонерним товариством НКЦПФР протягом двох років поспіль інформації, передбаченої законом.

Слід зазначити, що до внесення цих змін у НКЦПФР не було повноважень звертатися до судів із позовом про припинення акціонерних товариств, що не здійснюють діяльність. Це одна з причин існування на фондовому ринку України великої кількості акціонерних товариств, які не здійснюють господарську діяльність і цінні папери яких (так звані сміттєві акції) використовуються в операціях з відмивання «брудних» коштів.

– Відповідно до ч. 10 ст. 17 та ч. 3 ст. 23 Закону України «Про цінні папери» торговці цінними паперами та фондові біржі зобов'язані подавати до загальнодоступної інформаційної бази даних НКЦПФР про ринок цінних паперів для подальшого розміщення таку інформацію про всі вчинені за їхньої участі правочини щодо емісійних цінних паперів:

✓ найменування емітента цінних паперів та його ідентифікаційний код згідно з ЄДРПОУ;

✓ вид, тип, клас, форму існування та форму випуску цінних паперів;

✓ міжнародний ідентифікаційний номер цінних паперів;

✓ кількість цінних паперів за кожним правочином;

- ✓ ціну цінних паперів;
- ✓ дату вчинення правочину;
- ✓ інші відомості, визначені НКЦПФР.

До зазначеної інформації не включаються відомості про сторони правочинів. Порядок та строки подання торговцем цінними паперами зазначеної інформації, а також порядок її подальшого розміщення встановлюються НКЦПФР.

– Відповідно до ч. 5 ст. 27 Закону України «Про цінні папери» юридична особа, яка має істотну участь у професійному учаснику фондового ринку, зобов'язана повідомляти НКЦПФР про всі зміни структури її власності, а також подавати інформацію про ділову репутацію новопризначених керівників у місячний строк із дня настання відповідних змін в установленому Комісією порядку.

Фізична особа, яка має істотну участь у професійному учаснику фондового ринку, зобов'язана повідомляти НКЦПФР про всі зміни у відомостях про своїх асоційованих осіб, а також подавати інформацію про свою ділову репутацію в порядку та у строк, які установлені Комісією.

Адміністративно-запобіжні заходи мають превентивний характер, тобто запобігають вчиненню нових правопорушень. Проте, для заходів припинення, попередження правопорушення не є основною, а переважно додатковою ознакою. Також, не всі заходи адміністративного припинення однаковою мірою сприяють запобіганню правопорушенням.

Так, заходи адміністративного припинення застосовуються, зокрема, Національною комісією з цінних паперів та фондового ринку і спрямовані на: припинення порушень правових норм (об'єктивно протиправних діянь); створення умов для подальшого притягнення винних до відповідальності; усунення шкідливих наслідків правопорушення; запобігання вчиненню нових правопорушень; відновлення попереднього, правомірного стану.

Адміністративно-забезпечувальні заходи дозволяють забезпечити: а) виконання рішення про накладання стягнення на порушника; б) провадження справ про правопорушення як в самій корпорації, так і на всьому ринку цінних паперів; в) формування доказової бази для притягнення порушників до відповідальності.

Таким ознакам відповідають такі примусові заходи:

– НКЦПФР може зупинити дію ліцензії профучасника фондового ринку на підставі рішення «Про затвердження Змін до Порядку зупинення дії та анулювання ліцензії на окремі види професійної діяльності на фондовому ринку». Прийнятий документ також уточнює причини, за якими НКЦПФР може зупинити дію ліцензії на строк, встановлений таким рішенням.

Зазначене може відбутись у разі:

– проведення перевірки щодо ознак маніпулювання на фондовій біржі;

– незаконного поширення інсайдерської інформації та її використання у власних корисних цілях або корисних цілях інших осіб;

– наявності правопорушення на ринку цінних паперів, за яким триває перевірка і яке може призвести до нехтування правами інвесторів.

– Змінами до Порядку визначено, у разі зупинення/відновлення дії ліцензії НКЦПФР протягом п'яти робочих днів із дати прийняття відповідного рішення має опублікувати інформацію про це на сайті та в офіційному виданні, проте, якщо це стосується діяльності депозитарної установи, також надіслати копію такого рішення Центральному депозитарію цінних паперів та Національному банку України.

– Територіальні органи Національної комісії з цінних паперів та фондового ринку відповідно до делегованих повноважень: здійснюють зупинення обігу, відновлення обігу, скасування реєстрації випусків акцій і анулювання свідоцтв про реєстрацію випусків акцій акціонерних товариств за їх місцезнаходженням згідно з даними Єдиного державного реєстру юридичних осіб та фізичних осіб – підприємців у разі прийняття рішення про припинення шляхом ліквідації або перетворення, якщо розмір статутного капіталу таких товариств не перевищує 30 000 000 грн. на дату прийняття рішення про їх припинення;

– Відповідно до пункту 30 статті 8 Закону України «Про державне регулювання ринку цінних паперів в Україні», у зв'язку із виявленням Національною комісією з цінних паперів та фондового ринку порушення емітентами цінних паперів вимог ч. 2 ст. 20 Закону України «Про акціонерні товариства» та ч. 3 ст. 6 Закону України «Про цінні папери та фондовий ринок»

в частині забезпечення існування акцій виключно в бездокументарній формі, п. 5 розділу XVII «Прикінцеві та перехідні положення» Закону України «Про акціонерні товариства» в частині неприведення статуту та внутрішніх положень у відповідність до норм цього Закону, з метою захисту інтересів інвесторів у цінні папери Національна комісія з цінних паперів та фондового може зупинити з 18.11.2014 внесення змін до системи депозитарного обліку щодо цінних паперів Товариств на строк до усунення порушення.

Раніше ніж перейти до розгляду питання адміністративної відповідальності в сфері забезпечення інформаційної безпеки корпорацій нами було з'ясовано, що серед теоретичних розробок, які присвячені цій проблемі визначається повна одностайність думок науковців.

Так, на думку авторів підручника з академічного курсу адміністративного права України, адміністративна відповідальність – це різновид юридичної відповідальності, що являє собою сукупність адміністративних правовідносин, які виникають у зв'язку із застосуванням уповноваженими органами (посадовими особами) до осіб, що вчинили адміністративний проступок, передбачених нормами адміністративного права особливих санкцій – адміністративних стягнень [147, с. 430].

В.К. Колпаков стверджує, що адміністративна відповідальність – це специфічне реагування держави на адміністративне правопорушення, що полягає в застосуванні уповноваженим органом або посадовою особою передбаченого законом стягнення до суб'єкта правопорушення [148, с. 289].

С.Т. Гончарук визначає адміністративну відповідальність як різновид юридичної відповідальності, що передбачає застосування адміністративних стягнень до осіб, які вчинили адміністративні проступки [139, с. 16].

На думку Ю.П. Битяка під адміністративною відповідальністю слід розуміти накладення на правопорушників загальнообов'язкових правил, які діють у державному управлінні, адміністративних стягнень, що тягнуть за собою для цих осіб обтяжливі наслідки матеріального чи морального характеру [149, с. 140].

Найбільш повним, на нашу думку, буде визначення зроблене Д.Н. Бахрахом, на основі наступних ознак, які зазначають що

адміністративна відповідальність: а) застосовується за правопорушення, встановлені законодавчими актами про адміністративну відповідальність; б) застосовується широким колом органів адміністративної юрисдикції та інших, уповноважених законом; в) реалізується в адміністративному провадженні, що має власні процесуальні особливості; г) являє собою реалізацію адміністративних стягнень по відношенню до частково (функціонально) підлеглих суб'єктів; д) може застосовуватись до колективних та індивідуальних суб'єктів [150, с. 26].

Таким чином зрозуміло, що до третьої групи адміністративно-правових методів найчастіше включають лише адміністративні стягнення.

Адміністративне законодавство України передбачає санкції за порушення встановлених правил у сфері забезпечення інформаційної безпеки корпорацій. Вони передбачають такі заходи відповідальності:

– Накладання стягнень на юридичних осіб за порушення нормативно-правових положень;

– Застосування заходів адміністративного впливу по відношенню до юридичних осіб за порушення нормативно-правових положень.

Суб'єктами скоєння адміністративного правопорушення в сфері забезпечення інформаційної безпеки корпорацій можуть бути: акціонери, посадові особи органів акціонерного товариства, засновники, учасники корпорацій тощо. Перераховані суб'єкти є відмінними за статусом, для кожного з них може бути встановлено різну ступінь вини із врахуванням соціально-економічного чинника відповідного суб'єкта адміністративного правопорушення.

Наступний вид застосування заходів адміністративного примусу у сфері забезпечення інформаційної безпеки корпорацій полягає у складанні протоколу про адміністративне правопорушення як заходу адміністративного стягнення та притягнення правопорушників, як винних осіб до адміністративної відповідальності відповідно до КУпАП.

Відповідальність за порушення у сфері інформаційного забезпечення корпорацій в Україні передбачено в наступних статтях, а саме: ст. 163-5, 163-9, 163-10, 163-11, 166-4.

Організаційними методами є способи, засоби і прийоми за допомогою яких здійснюються відповідні форми організаційної діяльності корпорацій.

Організаційні методи залежно від напрямків і мети діяльності поділяють на загальні і конкретні. До основних методів належать такі методи: планування, координації, контролю, а до допоміжних – методи надання допомоги, забезпечення своєчасного виконання завдань, сприяння проведенню відповідних заходів та інші [151, с. 163-166].

Важливими методами аналізу стану забезпечення інформаційної безпеки корпорацій є методи опису та класифікації. Для здійснення ефективного захисту системи корпорацій слід по-перше, описати, лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

У якості розповсюдження методів аналізу стану забезпечення інформаційної безпеки корпорацій використовуються методи дослідження причинних зв'язків. За допомогою даних методів виявляються причинні зв'язки між загрозами, ризиками, викликами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи щодо їх нейтралізації. У числі даних методів причинних зв'язків можна назвати наступні: метод спорідненості, метод розбіжності, метод сполучення спорідненості і розбіжності.

Вибір методів аналізу стану забезпечення інформаційної безпеки корпорацій залежить від конкретного рівня і сфери організації захисту. Залежно від загрози унеможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується безпосередньо сфери забезпечення інформаційної безпеки корпорацій, то у ній зазвичай виділяють: фізичний, програмно-технічний, управлінський, технологічний, рівень користувача, сітьовий, процедурний. Розглянемо дещо детальніше кожен з цих рівнів.

Фізичний рівень – здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій.

Програмно-технічний рівень – здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

Управлінський рівень – здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління з боку єдиної системи забезпечення інформаційної безпеки органів державного управління.

Технологічний рівень – здійснюється реалізації політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.

На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на суб'єктів корпорацій, унеможливлення інформаційного впливу з боку соціального середовища.

На сітьовому рівні дана політика реалізується у форматі координації дій конкретних органів корпорації, які пов'язані між собою однією метою.

Процедурний рівень – вживаються заходи, що реалізуються акціонерами, учасниками корпорацій. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Серед організаційний методів, можна виокремити декілька методів забезпечення інформаційної безпеки корпорацій:

- однорівневі методи будуються на підставі одного принципу управління інформаційною безпекою;
- багаторівневі методи будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких слугує вирішення власного завдання. При цьому приватні технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;
- комплексні методи – багаторівневі технології, які об'єднані до єдиної системи координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки корпорацій виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;
- інтегровані високоінтелектуальні методи – багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів із організаційним управлінням [7, с. 169-170].

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якій стадії управління загрозами. До таких стадій належать: прийняття рішення з визначення галузі та контексту інформаційної загрози і складу учасників процесу протидії; ухвалення загальної стратегії і схеми дій в політичній, економічній і соціальній сферах життєдіяльності; забезпечення адекватного сприйняття загрози та небезпеки у більш низьких організаційних ланках системи управління корпораціями; виділення необхідних економічних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози і збереження сталого розвитку інформаційних ресурсів управління корпораціями.

Специфіка методів, що використовуються, значно залежить від суб'єкта діяльності, об'єкта впливу, а також цілей, що переслідуються. Так, методи діяльності індивіда у зв'язку із його обмеженою можливістю з забезпечення інформаційної безпеки здебільшого зводяться до джерела загрози, апелювання до суспільної думки, а також до держави, яка має вживати рішучих заходів із нейтралізації інформаційних загроз.

Слід констатувати, що в нашій країні не на достатньому рівні усвідомлюють небезпеку саме в інформаційній сфері корпорацій, немає штатних одиниць в органах управління корпораціями щодо забезпечення інформаційної безпеки.

Суттєво важливим є застосування аналітичних методів пізнання і дослідження у сфері інформаційної безпеки корпорацій. Нині важливою умовою забезпечення інформаційної безпеки корпорацій є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від загроз. Отже, система має відповідно реагувати та гарантувати ефективну діяльність у цьому напрямі.

Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передачі, тобто забезпечення її цілісності. Таким чином конфіденційність інформації, яка забезпечується за допомогою криптографічних методів не є головною вимогою при проектуванні систем захисту інформації корпорацій. Виконання процедур криптокодування і декодування може уповільнити передачу даних та зменшити доступ до них, через те, що працівник корпорації буде позбавлений можливості своєчасного та швидкого доступу до

цих даних та інформації, через функціонування механізму захисту. Саме тому, забезпечення конфіденційності інформації має відповідати можливості доступу до неї. Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки в першу чергу має гарантувати доступність і цілісність інформації, а її конфіденційність у випадку необхідності [7, с. 171]. Багато корпорацій в Україні, які мають солідний грошовий обіг і достатні фінансові джерела, не мають не те щоб цілісної системи безпеки взагалі, а й навіть окремо функціонуючої підсистеми забезпечення інформаційної безпеки. Можна перераховувати й інші методи захисту інформації в корпораціях, водночас, нині ототожнення забезпечення інформаційної безпеки із забезпеченням безпеки комп'ютерних систем є просто концептуальною помилкою. Тому не є дивиною, що на сьогодні більша частина українських корпорацій втратила внаслідок власної недбалості чимало коштів. І характерною рисою українського суспільства є те, що жодна корпорація жодного разу не визнала факту вчиненого кіберзлочину проти себе.

Також необхідно зазначити, що серед вищезазначених методів забезпечення інформаційної безпеки корпорацій є такі важливі методи, які поділяються на правові, організаційно-технічні та економічні.

До правових методів відноситься розробка нормативних правових актів, що регламентують відносини в інформаційній сфері, а також нормативно-методичних документів з питань забезпечення інформаційної безпеки в Україні.

Організаційно-технічними методами забезпечення інформаційної безпеки в Україні є:

- створення і вдосконалення системи забезпечення інформаційної безпеки України;
- посилення правозастосовчої діяльності органів виконавчої влади, включаючи попередження і припинення правопорушень в інформаційній сфері, а також виявлення, викриття та притягнення до відповідальності осіб, які вчинили злочин та інші правопорушення в цій сфері;
- розробка, використання і вдосконалення засобів захисту інформації та методів контролю ефективності цих засобів,

розвиток захищених телекомунікаційних систем, підвищення надійності спеціального програмного забезпечення;

• створення систем і засобів запобігання несанкціонованому доступу до оброблюваної інформації та спеціальних впливів, що викликають руйнування, знищення, перекручення інформації, а також зміна штатних режимів функціонування систем і засобів інформатизації та зв'язку;

• виявлення технічних пристроїв і програм, які становлять небезпеку для нормального функціонування інформаційно-телекомунікаційних систем, запобігання перехоплення технічними каналами, застосування криптографічних засобів, захисту інформації при її зберіганні, обробці та передачі по каналах зв'язку, контроль за виконанням спеціальних вимог щодо захисту інформації;

• сертифікація засобів захисту інформації, ліцензування діяльності в галузі захисту державної таємниці, стандартизація способів і засобів захисту інформації;

• вдосконалення системи сертифікації телекомунікаційного обладнання та програмного забезпечення автоматизованих систем обробки інформації за вимогами інформаційної безпеки;

• контроль за діями персоналу в захищених інформаційних системах, підготовка кадрів в галузі забезпечення інформаційної безпеки України;

• формування системи моніторингу показників і характеристик інформаційної безпеки України в найбільш важливих сферах та діяльності суспільства і держави.

Економічні методи забезпечення включають:

• розробку програм забезпечення інформаційної безпеки України та розірвання дипломатичних відносин;

• вдосконалення системи фінансування робіт, пов'язаних з реалізацією правових та організаційно-технічних методів захисту інформації, створення системи страхування інформаційних ризиків фізичних і юридичних осіб.

Інформаційна безпека України є однією зі складових національної безпеки України та впливає на захищеність національних інтересів України в різних сферах життєдіяльності суспільства і держави. Загрози інформаційної безпеки України та методи її забезпечення є загальними для цих сфер.

У кожної з них є свої особливості забезпечення інформаційної безпеки, пов'язані зі специфікою об'єктів забезпечення безпеки, ступенем їх вразливості та відносини загроз інформаційній безпеці України. У кожній сфері життєдіяльності суспільства і держави поряд із загальними методами забезпечення інформаційної безпеки України можуть використовуватися приватні методи і форми, зумовлені специфікою чинників, що впливають на стан інформаційної безпеки України.

Основними складовими в інтенсифікації інформаційних процесів при системно кібернетичному і соціальний підхід до формалізації ходу суспільного розвитку є:

- неухильне зростання швидкостей інформаційного обміну;
- збільшення обсягу видобутої і переданої інформації;
- прискорення процесів обробки інформації;
- розширення застосування адаптивного управління (з використанням зворотних зв'язків);
- розширення наочного (візуального) подання інформації в процесах управління;
- бурхливе зростання технічної оснащеності управлінської праці;
- врахування особливостей соціально-психологічних взаємодій людського соціуму і утворень.

У цілому ж слід зазначити, що обрання цілей і методів протидії конкретним загрозам та небезпекам інформаційній безпеці становить собою важливу проблему і складову частину діяльності з реалізації основних напрямів державної політики інформаційної безпеки. У межах вирішення даної проблеми визначаються можливі форми відповідної діяльності органів державної влади, що потребує проведення детального аналізу економічного, соціального, політичного та інших станів суспільства, держави і особи, можливих наслідків вибору тих чи інших варіантів здійснення цієї діяльності.

Розділ 3
ПРАВОВІ ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

3.1. Інформація, що міститься в установчих документах суб'єктів господарювання та режим їх використання

Установчими документами суб'єктів господарювання називають комплект документів встановленої законодавством форми, згідно з якими суб'єкт господарювання виникає і діє як суб'єкт права [152, с. 256]. Установчі документи є правовою формою, в якій врегульовані завдання суб'єктів господарювання. Виходячи із завдань врегульовуються такі поняття, як цілі і предмет діяльності суб'єкта господарювання. На думку Н.О. Саніахметової установчі документи – статут та/або засновницький договір, необхідні для врегулювання порядку, умов узгодженої діяльності засновників, а також визначення правового статусу підприємства – юридичної особи [153, с. 64]. В.К. Мамутов вважає, що статут і засновницький договір є установчими документами, на підставі яких створюються і діють засновані організації [154, с. 389]. Установчі документи, поряд з нормами законодавства, визначають правовий статус господарської організації та встановлюють правову основу її господарської діяльності. Розробка і затвердження установчих документів є одним з етапів створення організації [155, с. 95].

Поняття «установчий документ» опосередковано вказує на те, що результатом їх складання, затвердження та реєстрування є створення суб'єктом господарювання – господарської організації. Незважаючи на наявність у філій, представництв та інших відокремлених підрозділах суб'єкту господарювання пакету документів, на підставі яких вони здійснюють свою діяльність, статусу установчих документів вони не мають. Чинне законодавство України не містить легального визначення поняття установчих документів, зокрема, статуту і

засновницького договору. Форму і зміст установчих документів визначають залежно від видів суб'єктів господарювання Господарський та Цивільний кодекси України, загальні закони про підприємства та закони про окремі види суб'єктів господарювання.

Стаття 87 ЦК України та ст. 57 ГК України містять перелік актів, які належать до установчих документів. По-перше, це рішення одного чи кількох власників або уповноваженого ним (ними) органу про створення суб'єкта господарювання або засновницький договір. Законодавчі акти не встановлюють будь-яких спеціальних вимог щодо форми та змісту рішення про створення суб'єкта господарювання, тому, на нашу думку, слід виходити з того, що таке рішення має бути оформлене правочином, вчиненим власником майна (уповноваженим ним органом) відповідно до його компетентності, визначеної чинним законодавством. По-друге, це статут (положення) суб'єкта господарювання. На підставі індивідуального або спільного установчого акта, складеного засновником (засновниками) створюється установа.

Стаття 57 ГК України та ст. 88 ЦК України визначають перелік обов'язкових відомостей, інформацію, яку необхідно включати до установчих документів суб'єктів господарювання. Установчі документи повинні містити обов'язкові дані про суб'єкт господарювання,без яких вони вважаються такими, що не відповідають вимогам законодавства. Зокрема, згідно зі ст. 57 ГК України в установчих документах повинні бути зазначені найменування суб'єкта господарювання, мета і предмет господарської діяльності, склад і компетенцію його органів управління, порядок прийняття ними рішень, порядок формування майна, розподілу прибутків та збитків, умови його реорганізації та ліквідації, якщо інше не передбачене законом. У засновницькому договорі засновники зобов'язуються утворити суб'єкт господарювання, визначають порядок спільної діяльності щодо його утворення, умови передачі йому свого майна, порядок розподілу прибутків і збитків, управління діяльності суб'єкта господарювання та участі в ньому засновників, порядок вибуття та входження нових засновників, інші умови діяльності суб'єкта господарювання, які передбачені законом, а також порядок його реорганізації та ліквідації

відповідно до закону. Статут суб'єкта господарювання повинен містити інформацію про його найменування, мету і предмет діяльності, розмір і порядок утворення статутного і інших фондів, порядок розподілу прибутків і збитків, про органи управління і контролю, їх компетенцію, про умови реорганізації та ліквідації суб'єкта господарювання, а також містити відомості, пов'язані з особливостями організаційної форми суб'єкта господарювання., передбачені законодавством. Статут може містити і іншу інформацію, яка не суперечить законодавству. Крім обов'язкових, до установчих документів можуть включатися альтернативні положення, які не повинні суперечити законодавству України. Це положення, пов'язані з особливостями діяльності підприємства: про трудові відносини, засновані на членстві, про раду підприємства, про інші органи, які реалізують повноваження трудового колективу.

Установчі документи установи є установчий акт. Однак це питання в законодавстві урегульоване недостатньо ясно. Так, у ч. 3 ст. 88 ЦКУ вказується, що установчий акт може міститися в заповіті. У такому випадку: по-перше, в установи буде відсутній окремий установчий документ, оскільки він буде сполучений із заповітом. Тоді установа буде змушена діяти на підставі заповіту як установчого документу; по-друге, у випадку відсутності у заповіті положень про мету установи, майно, що передається установі для досягнення цієї мети, структури управління установою, їх встановлює орган, що здійснює державну реєстрацію. Однак викликає складність відповідь на питання про те, у якому документі буде втілене вирішення цих питань і наскільки такий орган вправі їх вирішувати у випадку нечіткості побажань заповідача. При цьому може йти мова і про тлумачення заповіту (ст. 1256 ЦКУ), право на що мають спадкоємці і суд, і про виконання заповіту (ст. 1290 ЦКУ) виконавцем, який може інакше, ніж орган державної реєстрації, розуміти волю заповідача; по-третє, як будуть співвідноситися і діяти заповіт і документ, виданий органами державної реєстрації; по-четверте, у цілому сумнівно те, наскільки юридична природа заповіту як одностороннього правочину відповідає трансформації цього заповіту по суті в установчих документах установи?

У процесі створення суб'єкта господарювання істотним є, по-перше, підписання установчого акту. Яким є рішення Єдиного засновника або угода двох і більше засновників про створення суб'єкта господарювання. По-друге, державна реєстрація, що встановлює юридичну особистість [156, с. 301-310]. Дії засновників як юридичні факти в сукупності з державною реєстрацією складають юридичний склад, що породжує виникнення нового суб'єкта права [157, с. 34].

Значна частина дій, виконуваних фізичними та/чи юридичними особами як засновниками, являє собою правочини або інші юридично значимі дії, спрямовані на встановлення зобов'язальних взаємовідносин між ними, а також корпоративних відносин між ними і створюваною юридичною особою. Одним з основних обов'язків кожного засновника є внесення майнового вкладу до статутного фонду юридичної особи. Отже, для вчинення правочинів щодо здійснення внесків до статутного фонду фізичні та юридичні особи повинні: мати необхідну правоздатність і дієздатність; дотримуватися вимог чинного законодавства, що обмежує їх можливості розпоряджатися своїм майном; враховувати правовий режим цього майна, а також вимоги, встановлені стосовно порядку вчинення правочинів з конкретним майном. Державні органи, що виступають як засновники, також зобов'язані діяти в рамках закону. Цивільний кодекс України (ст. 81) передбачає можливість створення суб'єкта господарювання – юридичну особу публічного права розпорядчим актом Президента України, органу державної влади, органу місцевого самоврядування. У деяких випадках законодавець встановлює обмеження на участь окремих категорій суб'єктів у договорах про створення деяких видів юридичних осіб. Наприклад, Декрет Кабінету Міністрів України «Про впорядкування діяльності суб'єктів підприємницької діяльності, створених за участю державних підприємств» від 31.12.1992 (редакція від 01.01.2004) [158] установив, що державні підприємства (за винятком будівельних організацій, підприємств будівельної індустрії та будівельних матеріалів, які є засновниками господарських товариств, що здійснюватимуть проектування та перспективне будівництво за кордоном) не можуть бути

засновниками підприємств будь-яких організаційних форм та видів, господарських товариств.

У правовій літературі ми спостерігаємо, що «установчий документ», «засновницький договір» і «договір про заснування юридичної особи» іноді змішуються, а легальні терміни, що застосовуються для їхнього позначення, вживаються як синоніми [159, с. 30]. Зазначені поняття мають певні спільні риси. Вони спрямовані на створення нового суб'єкта права, за своєю правовою природою є консенсуальними, багатосторонніми, взаємними і фідуціарними угодами.

У разі коли два (або більше) засновника домовляються між собою про спільні дії, спрямовані на створення юридичної особи, вони укладають договір про заснування юридичної особи або засновницький договір, залежно від обраної організаційно-правової форми створення суб'єкта господарювання, що містить умови, покликані регламентувати відносини засновників у процесі створення нового суб'єкта права. Разом з тим, відзначимо, що засновницький договір є установчим документом повного товариства і командитного товариства, але не є таким для акціонерного. Акціонерне товариство (публічне, приватне) створюється на підставі статуту.

Таким чином, договір про заснування юридичної особи не відноситься до установчих документів юридичної особи. Він регламентує тільки зобов'язальні відносини засновників у процесі створення юридичної особи і закріплює бажання засновників здійснити спільні дії, спрямовані на затвердження статуту юридичної особи та державну реєстрацію нового суб'єкта права, зобов'язує також кожного засновника передати внесок до її статутного фонду. Після державної реєстрації юридичної особи і завершення формування її статутного фонду зобов'язання, що виникли з цього договору, звичайно припиняються належним виконавцем.

Договір засновників варто віднести до оплачуваного договору. У більшому ступені, ніж це відноситься до засновницького договору, договір засновників носить фідуціарний характер. Взаємовідносини сторін за договором носять особливо довірчий характер. Договір засновників закріплює лише той мінімум правових положень, що застосовні до відносин засновників. Велика частина відносин засновників

не складає предмета правового регулювання, оскільки відноситься до фактичного порядку і визначається особистими домовленостями, єдиною настроєністю і метою. Руйнування договірних відносин може призвести до невиконання окремими засновниками обов'язків щодо заснування акціонерного товариства і, відповідно, до недосягання мети, коли не створюється товариство, яке б відповідало встановленим законом ознакам.

Зрозуміло, що договір засновників, як і будь-який інший договір, вимагає для свого виникнення двох чи більше учасників, а тому цей договір відноситься до двох чи багатосторонніх правочинів. Особливістю договору, укладеного трьома і більше особами, є його багатосторонній характер. Такі договори породжують для кожного із засновників однакові юридичні наслідки, крім того, між його учасниками немає такої протилежності, антагонізму інтересів, як у двосторонніх договорів [160, с. 8]. Вказівка на однакові юридичні наслідки зовсім не рівнозначна твердженню, що багатосторонній правочин породжує права й обов'язки в рівному обсязі для кожного учасника. Договір засновників може закріплювати асиметрію прав і обов'язків окремих засновників товариства. Це може відбуватися при однакових і незмінних об'єктивних чи інших правах засновників конкретних суб'єктивних прав, а особливо обов'язки, які надаються чи накладаються на засновників можуть істотно відрізняться за своїм обсягом. Конкретний обсяг прав і обов'язків окремої сторони за договором пропорційний кількості придбаних секцій, розміру майнового внеску, здійсненого в оплату статутного фонду.

Договір засновників відноситься до консенсуальних договорів, оскільки закон не пов'язує момент його укладання з обов'язковою передачею майна. Із зазначеного випливає, що для укладання договору достатньо досягнення згоди стосовно всіх істотних умов договору, перелік яких чітко визначений законом. Подібний прийом юридичної техніки не залишає місця для яких-небудь суперечок чи незрозумілостей, що має місце, наприклад, у випадку з умовою про ціну в окремих оплатних договорах.

Однією з найбільших ознак договору засновників виступає його організаційний характер. У даному випадку договір

засновників протиставляється майновим договорам. Договір у цьому змісті не тільки опосередковує передачу майна або виконання певних операцій, а й закріплює, конструює систему передумов для створення нового суб'єкта права – юридичної особи. При недосягненні мети договір припиняє свою дію. За цією ж ознакою варто проводити розмежування договору засновників і засновницького договору господарського товариства. Засновницький договір визначає не тільки порядок створення юридичної особи, а й також у більшій чи меншій ступені визначає структуру і порядок здійснення діяльності юридичної особи. Договір засновників у силу прямої вказівки в законі не відноситься до установчих документів і зв'язує зобов'язаннями лише засновників.

Аналіз великої кількості установчих документів різноманітних видів договірних об'єднань свідчить про те, що всі істотні особливості їх організаційно-правового статусу знаходять відображення в умовах засновницького договору.

Засновницький договір підписується всіма його учасниками. Зазначимо, що Державна регуляторна служба України вважає, що на підставі довіреності, засвідченої нотаріально, засновник може підписувати установчі документи від імені інших засновників. В засновницькому договорі подається інформація щодо найменування товариства, органи управління товариством, їх компетентність, порядок прийняття ними рішень, порядок вступу до товариства та виходу з нього, зобов'язання учасників створити товариство, порядок їх спільної діяльності щодо створення, умови передання товариством майна учасників, він має також містити інформацію про розмір та склад складеного капіталу товариства, розмір та порядок зміни часток кожного з учасників у складеному капіталі, розмір, склад та строки внесення ними вкладів.

Згідно з ч. 3 ст. 134 ЦКУ, якщо внаслідок виходу, виключення чи вибуття у командитному товаристві залишився один повний учасник, засновницький договір переоформлюється в одноособову заяву, підписану повним учасником. Якщо командитне товариство створюється одним повним учасником, то установчим документом є одноособова заява (меморандум),

яка має містити усі відомості, встановлені ст. 134 ЦКУ для командитного товариства.

Таким чином, ч. 3 ст. 134 ЦКУ містить новелу, що закріплює фактично новий вид установчого документу – одноособова заява (меморандум).

У багатьох засновницьких договорах вказується також інформація, що спадкоємці (правонаступники) одного з учасників відповідають за зобов'язаннями товариства, що виникли при житті спадкодавця або до реорганізації юридичної особи – учасника товариства, на тих же умовах і в тих же межах, що і даний учасник.

Іноді у засновницьких договорах включається умова, що учасник, який систематично не виконує, чи виконує не належним чином обов'язки, покладені на нього товариством, або який перешкоджає своїми діями (бездіяльністю) досягненню цілей товариства може бути виключений із товариства.

Закон України «Про державну реєстрацію юридичних осіб та фізичних осіб – підприємців» встановлює, що зміни до установчих документів юридичної особи, а також зміна прізвища та/або імені, та/або по батькові або місця проживання фізичної особи – підприємця підлягають обов'язковій державній реєстрації шляхом внесення відповідних змін до записів Єдиного державного реєстру. У ст. 89 ЦКУ законодавець встановлює, що зміни до установчих документів юридичної особи набирають чинності для третіх осіб з дня їх державної реєстрації, а у випадках, встановлених законом, – з моменту повідомлення органу, що здійснює державну реєстрацію, про такі зміни.

Для більшості суб'єктів господарювання – юридичних осіб установчими документами є тільки статут, що затверджується їх засновником. Статут є єдиним установчим документом для господарських товариств, створюваних одним засновником (ч. 2 ст. 87 ЦКУ). Будучи установчим документом, статут закріплює правовий статус суб'єкта господарювання – юридичної особи.

У навчальній, науковій та дослідницькій літературі було висловлено кілька суджень щодо того, що являє собою статут тієї чи іншої організації.

Як підкреслював Д.І. Мейер, хоча проект статуту складається засновниками компанії, його зміст обумовлений волею лише законодавця, оскільки статут є актом його діяльності [161, с. 15].

М.Н. Марченко вказує, що будучи формою (джерелом) права нормативно-правові акти відрізняються від актів, що не мають нормативного характеру, насамперед від актів застосування норм права, чи індивідуальних актів. Індивідуальні акти також є юридичними за своїм характером і викликають певні юридичні наслідки. Акти індивідуально звернені до строго визначених осіб або кола осіб і видаються з визначеного приводу. Індивідуальний акт розрахований на строго визначений вид суспільних відносин і його дія припиняється з припиненням існування конкретних відносин [162, с. 510-511].

Прикладами такого роду індивідуальних актів, що є юридичними фактами, служать статути державних підприємств, що затверджуються уповноваженими державними органами України, зокрема Статут Академії правових наук України, затверджений постановою КМУ від 02.02.2000 р. № 210 [163], Статут публічного акціонерного товариства «Державний ощадний банк України», затверджений постановою КМУ від 25.02.2003 р. № 261, Статут Державного концерну «Укроборонпром», затверджений постановою КМУ від 31.08.2011 р. № 993. Можливо допустити, що наведені приклади статутів можна визнати своєрідним адміністративним правочином, що має природу, подібну з адміністративним договором [164, с. 221-236].

Як зазначають А.В. Міцкевич, В.Д. Попов статут юридичної особи є корпоративним нормативним правовим актом, що містить корпоративні норми, які є джерелами права [165, с. 70-71].

На думку І.В. Єлисєєва, статут можна розглядати в якості локального нормативного акта, що визначає правове становище юридичної особи і регулює відносини між учасниками і самої юридичної особи [166, с. 160].

Як зазначає Д.І. Степанов, статут юридичної особи є особливим актом застосування права, особливим документом (установчим документом), що закріплює, обмежує або передбачає конкретну дію. Статут юридичної особи оформлює процес правозастосування, що відбувається в момент створення юридичної особи, у статуті здійснюється реалізація правових

норм про юридичних осіб. Разом з тим, статут не є одномоментним актом застосування права, він має певний нормативний характер, тому що розпорядження, що міститься в ньому, не будучи нормами позитивного права, мають безстроковий характер і розраховані на багаторазову реалізацію. Основна частина правозастосування відбувається суб'єктами приватного права, а державні органи завершують цей процес, легітимізуючи створену юридичну особу актом державної реєстрації [167, с. 44].

Статут суб'єкта господарювання – юридичної особи, що існує у вигляді установчого документа, затвердженого (прийнятого) засновником (засновниками), являє собою корпоративний правочин.

Згідно зі ст. 88 ЦКУ у статуті товариства вказується інформація щодо найменування юридичної особи, органів управління товариством, їх компетенція, порядок прийняття ними рішень, порядок вступу до товариства та виходу з нього.

Згідно з ч. 2 ст. 82 ГКУ установчий документ суб'єкта господарювання – господарського товариства повинен містити інформацію про вид товариства, предмет і цілі його діяльності, склад засновників та учасників, склад і компетенцію органів товариства та порядок прийняття ними рішень, перелік питань, з яких необхідна одностайність або кваліфікована більшість голосів та інші відомості, передбачені ст. 57 ГКУ.

Однак, крім цих двох кодексів, вимоги до інформації, яка повинна міститися у статуті суб'єктів господарювання – господарських товариств вказується і в спеціальному Законі України «Про господарські товариства», «Про акціонерні товариства».

Отже, необхідно зазначити, що установчі документи суб'єктів господарювання – документи встановленої законом форми, згідно з якими суб'єкт господарювання виникає і діє як суб'єкт права, що є правовою формою, в якій врегульовані завдання суб'єкта господарювання та які необхідні для врегулювання порядку, умов узгодженої діяльності засновників, а також визначення правового статусу створюваного суб'єкта господарювання – господарської організації.

У контексті нашого дослідження інформація, що міститься в установчих документах суб'єктів господарювання

розглядається як сукупність організаційно-правових засобів, які опосередковані імперативним методом юридичного впливу на відносини, пов'язані з одержанням, використанням, поширенням, зберіганням відповідних відомостей. Таким чином, класифікація інформації, що міститься в установчих документах суб'єктів господарювання – за режимом доступ до інформації поділяється на відкриту та інформацію з обмеженим доступом. Відповідно критерієм такого розподілу виступає режим доступу до інформації, який визначається як передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації (ч. 1 ст. 28 ЗУ «Про інформацію»).

Відкритою інформацією є будь-які відомості про суб'єкт господарювання, що є у володінні, користуванні або розпорядженні суб'єкта та не віднесені до категорії інформації з обмеженим доступом. Доступ до відкритої інформації забезпечується через публікації в офіційних друкованих виданнях, поширення через засоби комунікації, надання інформації на запит зацікавлених осіб [168, с. 157].

У систему забезпечення доступу до інформації варто насамперед включити створення адміністративно-правових умов для отримання суб'єктами інформаційних відносин необхідної їм інформації. Правове забезпечення доступу до інформації в установчих документах полягає у формуванні системи загальнообов'язкових правил поведінки у сфері отримання інформації, юридична сила яких охороняється державою. Адміністративне (інституційне) забезпечення доступу до інформації виражається у створенні суб'єктом господарювання та наділення їх відповідними повноваженнями щодо задоволення інформаційних потреб учасників інформаційних відносин [169, с. 100].

Російський вчений В.Н. Лопатін під «інформацією з обмеженим доступом» розуміє інформацію, доступ до якої обмежено у відповідності з законом з метою захисту прав та законних інтересів її власників [170, с. 86].

Доступ фактично з певною дозвільною процедурою, яка полягає в отриманні згоди компетентного органу (особи) на одержання документа чи інформації, отримання якої

безпосередньо пов'язане з можливістю реалізації права на інформацію, та, відповідно, обмежує це право [171, с. 27].

Правовий режим інформації з обмеженим доступом покликаний охороняти відомості, вільний обіг яких може порушити права й інтереси держави, суспільства, окремої особи, забезпечити інформаційну незалежність суб'єктів приватного права у відносинах із державою і особою, узгодити публічну потребу у свободі інформації та право кожного на збереження таємниці [172, с. 3-4].

Вітчизняний науковець А.І. Марущак розділяє правомірні та неправомірні засоби доступу громадян до інформації. Перші – це засоби та процедури, які прямо передбачені законодавством або не порушують його і які дають змогу реалізувати право громадян на отримання інформації. Другі – це засоби та процедури, які безпосередньо порушують законодавство, що зумовлює юридичну відповідальність [173, с. 18].

Т.Ю. Ткачук розмежовує санкціонований та несанкціонований доступ до інформації. Визначаючи несанкціоновані як сукупність прийомів і порядок дій з метою одержання (добування) охоронюваних даних протиправним шляхом (таємне спостереження, перехоплення повідомлень, крадіжки зразків, документів тощо) [174, с. 248].

Легальну можливість володіти інформаційним ресурсом має лише його власник або особа, яка отримала у власника відповідний дозвіл. Цей дозвіл, наданий власником за власною волею чи за вказівкою закону, необхідно розуміти як юридично забезпечена можливість доступу до інформаційних ресурсів або як право на доступ. У власника інформаційного ресурсу таке право існує початково і може бути реалізовано у відношенні належного йому ресурсу. Для третіх осіб, що виступають в ролі користувачів, закон встановлює ряд правових підстав для реалізації права на доступ. Цей зв'язок проявляється в тому, що без права на доступ право користування і право ознайомлення законно не можуть бути реалізовані [175, с. 118-120].

Інформація з обмеженим доступом за своїм режимом поділяється на конфіденційну, таємну та службову [80].

Таємниця як соціальне явище виникає там, де існують інтереси, які передбачають конфліктний взаємозв'язок, за якого та чи інша інформація може слугувати інструментом у

протистоянні. Дана обставина спонукала суб'єкти господарювання приховувати і охороняти відомості, які можуть бути використані або їм на шкоду, або на користь конкуруючої сторони [176, с. 19]. саме по собі приховування, захист інформації завжди відіграє службову роль, обслуговуючи якусь сферу людських відносин, діяльності, розвитку суспільства та держави.

Таємність або секретність вказує на певне відокремлення, наявність у зв'язку з цим спеціального режиму доступу володіння, користування і розпорядження, що закріплено у відповідних нормах або локально-нормативному акті [177, с. 109]. Отже, відповідно до ч. 2 ст. 21 Закону України «Про інформацію» конфіденційну інформацію розглядаємо як певні відомості, які перебувають у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і які, власне, поширюються по їх бажанню згідно з передбаченими ними умовами.

До таємної інформації законодавець відніс інформацію, яка містить відомості, складові державну і іншу передбачену законом таємницю, розголошення якої заподіює збиток особі, суспільству і державі. І хоча в нормах закону чітко не вказано, що до таємної інформації належить комерційна таємниця, на нашу думку, в поняття «інша передбачена законом таємниця» законодавець вклав саме цей сенс. Також нам вбачається суттєвим той факт, що не одним Законом України «Про інформацію» вводиться в дію поняття «комерційна таємниця». Слід зауважити, що це поняття розглядається і іншими нормативно-правовими актами. Так, Цивільний кодекс України в ст. 505 дає визначення комерційної таємниці, але не говорить про конфіденційну інформацію. Комерційною таємницею є інформація, яка є секретною в тому сенсі, що вона в цілому або в певній формі і сукупності її складових є невідомою і не є легкодоступною для осіб, які зазвичай мають справу з видом інформації, до якої вона належить, у зв'язку з цим має комерційну цінність і є предметом адекватних існуючим обставинам засобів відносно збереження її секретності, прийнятих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути данні технічного, організаційного, комерційного, виробничого і іншого характеру,

за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці [178, с. 119-124].

Відповідно ч. 1 ст. 36 Господарського кодексу України відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою і іншою діяльністю суб'єкта господарювання, які не є державною таємницею, розголошування яких може заподіяти збиток інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею. Склад і об'єм відомостей, які складають комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання відповідно до закону [179, с. 41-45].

В юридичній літературі поняття «комерційна таємниця» визначається неоднаково. Так, Г.Андрощук вказує, що під комерційною таємницею суб'єкта господарювання треба розуміти відомості, які не є державними секретами, пов'язаними з виробництвом, технологією, управлінням, фінансами та іншою діяльністю суб'єкта господарювання, розпорядженням яких може завдати шкоди його інтересам [180, с. 10]. Є. Соловйов вважає, що комерційна т таємниця – це економічні інтереси та відомості про різні сторони і сфери виробничо-господарської, управлінської, науково-технічної, фінансової діяльності суб'єкта господарювання, які навмисно приховуються з комерційних міркувань, охорона яких обумовлена інтересами конкуренції і можливої загрози економічної діяльності суб'єкта [181, с. 8]. Ю. Плаксін та Ю. Макогон вважають, що комерційна таємниця – це будь-яка ділова інформація, яка має для підприємства реальну або потенційну цінність на комерційних засадах, витік якої може спричинити йому шкоду; вона не є загальновідомою та загальнодоступною на законних підставах, вона певним чином визначена та підприємством вживаються певні заходи для збереження її конфіденційності; вона не є державною таємницею і не захищена авторськими та патентними правами; вона не стосується негативної діяльності підприємства, яка здатна завдати шкоду суспільству [182, с. 8]. В. Лопатін вказує, що комерційна таємниця «это научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, имеющая действительную потенциальную коммерческую

ценность в силу ее неизвестности третьим лицам, которые могли бы получить выгоду от ее разглашения или использования, к которой нет свободного доступа на законном основании, и по отношению к которой принимаются адекватные ее ценности меры охраны.» [170, с. 86-87]. О.П. Сергєєва розуміє під комерційною таємницею – інформацію конфіденційного характеру, яка безпосередньо пов'язана з підприємницькою діяльністю суб'єктів права як індустріального, так і торговельного характеру, або з діяльністю щодо надання послуг, яка має реальну або потенційну економічну цінність та надає переваги в конкурентній боротьбі, за розголошення якої настає юридична відповідальність та існує особливий режим її охорони [183, с. 87].

Говорячи в цілому, комерційна таємниця і конфіденційна інформація – це відомості, які підприємство має право не придавати гласності, а його співробітники зобов'язані не розголошувати. Маючи багато спільного, поняття і зміст комерційної таємниці і конфіденційної інформації в той же час не є тотожними.

Комерційна таємниця підприємства :

– це відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою і іншою діяльністю підприємства, яке не є державною таємницею, розголошування яких може завдати шкоди інтересам суб'єкта господарювання (ч. 1 ст. 36 Господарського кодексу України) [184];

– це інформація, яка має комерційну цінність, в цілому або в певній формі і сукупності її складових є невідомою і немає легкодоступної для осіб, які зазвичай мають справу з видом інформації, до якої вона належить, була предметом адекватних існуючим обставинам заходів по збереженню секретності такої інформації, спожитих особою, яка законно контролює цю інформацію (ч. 1 ст. 505 Цивільного кодексу України) [185].

Таке визначення допомагає відокремити конфіденційну інформацію, як будь-яку інформацію з обмеженим доступом, у тому числі ту, яка торкається комерційної діяльності підприємства, від комерційної таємниці – тобто інформації, яка має комерційну цінність.

Склад і обсяг відомостей, які складають комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання згідно

з (ст. 36 ГКУ). Відразу відмітимо: на сьогодні в Україні немає спеціального закону, який регулює правовий режим, порядок використання комерційної таємниці. Таким чином, вказана норма посилає до невизначеного законодавчого на сьогодні акту, у тому числі до ЦКУ і до самого ГКУ.

Відповідно до ч. 2 ст. 505 ЦКУ, комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого і іншого характеру, за винятком тих, які згідно із законом не можуть бути віднесені до комерційної таємниці. Як видно зі змісту приведеної норми перелік відомостей, які можуть складати комерційну таємницю, невичерпний і обмежується тільки законом.

Відомості, які не можуть складати комерційну таємницю :

– засновницькі документи, документи, які дозволяють займатися підприємницькою діяльністю і її окремими видами;

– інформація за усіма встановленими формами державної звітності;

– відомості про чисельність і склад працюючих, їх заробітну плату в цілому і за професіями і посадами, а також наявність вільних робочих місць;

– документи про сплату податків і обов'язкових платежів;

– інформація про забруднення природного довкілля, недотримання безпечних умов праці, реалізації продукції, яка завдає шкоди здоров'ю, а також інших порушеннях законодавства України і розмірах заподіяних при цьому збитків;

– документи про платоспроможність;

– відомості про участь посадовців підприємства в кооперативах, малих підприємствах, союзах, об'єднаннях і інших організаціях, які займаються підприємницькою діяльністю;

– відомості, які відповідно до чинного законодавства підлягають оголошенню тощо.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом (ч. 2 ст. 21 Закону «Про інформацію»).

Громадяни і юридичні особи самостійно відносять до конфіденційної:

– інформацію професійного, ділового, виробничого, банківського, комерційного і іншого характеру;

– інформацію, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного і іншого інтересу.

– Виняток становить інформація:

– комерційного і банківського характеру;

– правовий режим якої встановлений Верховною Радою за поданням КМУ (з питань статистики, екології, банківських операцій, податків тощо);

– приховування якої представляє загрозу життя і здоров'ю людей.

Якщо підприємство використовує інформацію, яка належить державі, доступ до такої інформації може бути обмежений шляхом поширення на неї статусу конфіденційної інформації.

Не може бути віднесена до конфіденційної інформація, вказана в ч. 4 ст. 21 Закону «Про інформацію»:

– про стан довкілля, якість харчових продуктів і предметів побуту;

– про аварії, катастрофи, небезпечні природні явища і інші надзвичайні події, які сталися або можуть статися і погрожують безпеці громадян;

– про стан здоров'я населення, його життєвий рівень, житло, медичне обслуговування і соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

– відносно стану справ з правами і свободами людини і громадянина, а також фактів їх порушень;

– про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових і службових осіб;

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

Уся інформація, яка згідно з Постановою Кабінету Міністрів України **«**Про перелік відомостей, що не становлять комерційної таємниці» від 09.08.93 р. № 611 не може складати комерційну таємницю, все ж може бути віднесена до конфіденційної інформації. Тому, створити вичерпний перелік відомостей, які

можуть складати комерційну таємницю або конфіденційну інформацію, нереально в результаті різноманіття суб'єктів і універсальності об'єкту правовідносин [186]. Приблизний же перелік відомостей (за винятком перерахованих у Постанові Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці» від 09.08.93 р. № 611), які можуть складати комерційну таємницю/конфіденційну інформацію, включатиме:

Комерційна таємниця:

– оригінальна технологічна, управлінська, маркетингова, організаційна та інша інформація, яка складає таємниці виробництва та інших сфер господарської діяльності;

– відомості про структуру і масштаби виробництва, виробничі потужності, тип і розміщення устаткування, запаси сировини, матеріалів, компонентів і готової продукції;

– відомості про зміст винаходу, корисної моделі або промислового зразка до офіційної публікації інформації про них;

– відомості про підготовку, прийняття і виконання окремих рішень керівництва організації;

– відомості про плани розширення або згортання виробництва різних видів продукції і їх техніко-економічні обґрунтування, про плани інвестицій, закупівель і продажу;

– відомості про факти проведення, мету, предмет і результати нарад і засідань органів управління організації тощо.

Конфіденційна інформація:

– персональні дані співробітників/клієнтів (відомості про факти, події і обставини приватного життя громадянина, що дають можливість ідентифікувати його обличчя) та інформація про їх особисте життя;

– відомості, пов'язані з професійною діяльністю (лікарська, нотаріальна, адвокатська таємниця);

– відомості, доступ до яких обмежений відповідно до Конституції України (таємниця листування, телефонних переговорів, поштових відправлень, телеграфних або інших повідомлень тощо);

– система технічного захисту інформації (відомості, які розкривають систему, засоби і методи захисту інформації в

автоматизованих системах від несанкціонованого доступу, значення діючих кодів і паролів тощо);

– режим безпеки на підприємстві (відомості про порядок і стан організації охорони, системи сигналізації, пропускний режим і т. п.);

– відомості, надані третіми особами на умовах конфіденційності (наприклад, про джерело тієї або іншої інформації).

Так, наприклад, для регулювання інформаційного поля в акціонерному товаристві, визнання частини інформації комерційною таємницею рада акціонерного товариства затверджує перелік інформації, відкритої для ознайомлення акціонерів. Іноді розробляються положення, які регулюють інформаційні потоки в акціонерному товаристві. Ці положення часто мають назву «Про ознайомлення з інформацією в акціонерному товаристві», «Про комерційну таємницю в акціонерному товаристві» тощо. Практично в усіх товариствах документами, відкритими для ознайомлення акціонерів, є свідоцтво про реєстрацію акціонерного товариства, статут із змінами та доповненнями; установчий договір, ліцензії, що дозволяють акціонерним товариствам займатися підприємницькою чи господарською діяльністю та її окремими видами, фінансовий звіт та баланс з додатками по підсумках кварталів та року, внутрішні нормативні акти. Для регулювання цих відносин розробляють і затверджують положення, яке встановлює право акціонера на отримання інформації про діяльність акціонерного товариства, обов'язки правління та структурних підрозділів щодо надання такої інформації акціонерам, обмеження доступу до інформації.

Кожен акціонер повинен бути повідомлений про те, яка інформація є відкритою для ознайомлення, а також де, коли і на яких умовах він може ознайомитися з нею. Крім того, слід ознайомити всіх акціонерів з переліком даних, які є комерційною таємницею [187, с. 68-72].

Перелік інформації, яка є комерційною таємницею акціонерного товариства, визначається у положенні згідно з чинним законодавством. Крім того, в положенні можуть міститися деякі додаткові пункти щодо надання інформації

реєстратором. Звичайно, зміст такого положення не повинен виходити за межі, встановлені чинним законодавством України.

Отже, необхідно зазначити, що практичне розділення конфіденційної інформації і комерційної таємниці має на меті:

1. Обкреслити межі відповідальності, яка може настати за розголошування (незаконний збір) відповідних відомостей.

2. Визначити коло питань, яке підприємство має право зберігати в таємниці від тих або інших осіб.

Якщо розглядати питання щодо службової інформації, то на думку багатьох фахівців ця інформація може бути класифікована на два основних типи.

По-перше, це службова інформація про діяльність суб'єкта господарювання, доступ до якої обмежено законом в цілях захисту їх інтересів. По-друге, це інформація, що підлягає охороні, яка стала відома через виконання службових обов'язків посадовим особам суб'єкта: комерційна банківська таємниця, професійна таємниця, а також конфіденційна інформація про приватне життя особи [27, с. 5-10].

Таким чином, підсумовуючи все вище сказане, можна стверджувати, що інформація, що міститься в установчих документах суб'єктів господарювання та режими щодо її використання потребують вдосконалення законодавства щодо правового регулювання окремих видів інформації. Ми бачимо, що сьогодні у зв'язку із постійним зростанням ролі правової інформації взагалі та інформації з обмеженим доступом зокрема, ускладненням інформаційно-правових відносин, розвитком інформаційно-комунікаційних систем існує об'єктивна необхідність подальшого вдосконалення матеріальних та процесуальних норм щодо доступу до цієї інформації. Усунення неузгодженості, пов'язаної з цими визначеннями, дасть можливість підняти рівень законодавства України до вимог сьогодення у більшій мірі підвищити рівень захищеності від незаконного розповсюдження та використання зазначених видів інформації.

3.2. Правове забезпечення захисту інсайдерської інформації суб'єктів господарювання

Правове забезпечення захисту інсайдерської інформації в нашій країні є дуже актуальною. Останніми роками збільшилась кількість справ, у яких власники великих підприємств звинувачувалися у використанні інформації інсайдерів з метою отримання надприбутків. Зловживання інсайдерською інформацією змушує державні органи жорстко підходити до розкриття підприємством інформації про свою діяльність і до використання не публічної інформації [188, с. 104].

Інсайдер (від англ. Inside – всередині) – будь-яка особа, що має доступ до конфіденційної інформації про стан справ суб'єкта господарювання завдяки своєму службовому становищу або родинним зв'язкам [189, с. 131]. Проте В.В. Саєнко стверджує, що інсайдерською інформацією є будь-яка конкретна не оприлюднена інформація про емітента, його цінні папери або договори щодо них, що є істотною, тобто у випадку оприлюднення може значно вплинути на ринкову вартість цінних паперів [190, с. 4].

Відповідно до ч. 1 ст. 44 Закону України «Про цінні папери та фондовий ринок» під інсайдерською інформацією слід розуміти будь-яку не оприлюднену інформацію про емітента, його цінні папери або правочини щодо них. До інформації, що містить відомості про емітента можна віднести наступні дані: про зміну керівництва емітента; про чисельний склад керівної ланки емітента; отримання (надання) або дострокове погашення кредиту; утворення дочірнього підприємства або злиття з ним тощо.

До інформації, що містить відомості про цінні папери емітента або правочинів щодо них можна віднести наступні дані: відомості про дострокову сплату відсотків інвесторам, продаж-купівля великого обсягу цінних паперів тощо. Слід зазначити, що це не вичерпний перелік відомостей, що можуть містити інсайдерську інформацію. І як відмічає В.В. Саєнко, тлумачення щодо того, яка ж інформація є інсайдерською недоцільно закріплювати на рівні нормативних актів.

Інсайдерська інформація може міститись як у бухгалтерських, фінансових, установчих документах, договорах, звітах, так і в усній

формі. Порядок розкриття інсайдерської інформації встановлюється виключно нормативно-правовими актами Національної комісією цінних паперів та фондового ринку.

Однак слід зазначити, що у ст. ст. 163-9, 163-11 Кодексу України про адміністративні правопорушення окрім терміна «несвоєчасне розкриття» використовується термін «нерозкриття інформації», обидва терміна відносяться до якості інформації, сам факт несвоєчасності або нерозкритості робить інформацію про емітента, його цінні папери або правочини щодо них охоронюваною адміністративним законом. Коли інформація стає відомою іншим особам з публічних джерел або засобів масової інформації, така інформація перестає бути інсайдерською.

Під інсайдерською інформацією у адміністративно-правовому сенсі слід розуміти інформацію, яка є не опублікованою або не оприлюдненою, тобто вона є невідомою колу потенційних інвесторів. І як справедливо стверджує В.В. Саєнко, оприлюдненою інформація вважається тоді, коли вона відома необмеженому колу осіб. Причому, немає необхідності, щоб кожен суб'єкт господарювання мав цю інформацію або щоб вона була оприлюднена у засобах масової інформації. Достатньо, щоб вона була доступною через інформаційні системи широкого користування. У ФРН навіть існує підхід, згідно з яким розкритою вважається інформація, що доступна лише інвесторам, які звичайно здійснюють операції з відповідними цінними паперами. Тому не потрібно розголошувати інформацію через засоби масової інформації, адже розголошення навіть вузькому колу зацікавлених інвесторів призведе до відображення інформації у курсовій вартості відповідного цінного папера [191, с. 45].

Зрозуміло, що інсайдерська інформація як спеціальний об'єкт забезпечення інформаційної безпеки суб'єктів господарювання пов'язана з інформаційною прозорістю.

Відкритість ринку у цивілізаційному суспільстві стає однією з основних умов його функціонування.

Без інформаційної прозорості прийняття ефективних рішень будь-яким інвестором стає просто не можливим, відсутність інформації про емітента у відкритому доступі призводить до того, що інвестори просто знижують свою інвестиційну

активність, а кошти, які б могли працювати на вітчизняному ринку цінних паперів, сьогодні у кращому разі працюють у тіньовому секторі країни, а в гіршому – на закордонних ринках. Від руху інформаційних потоків на ринку змінюються і напрям фінансових потоків.

Таким чином, інсайдерська інформація означає будь-яку конкретну (точну) інформацію, яка не була оприлюднена та яка безпосередньо чи опосередковано стосується одного або кількох емітентів фінансових інструментів або одного чи кількох фінансових інструментів, та яка у разі її розголошення може суттєво вплинути на ціну фінансових інструментів або на ціну похідних фінансових інструментів. Зважаючи на це, інформація, яка, якщо вона розкрита, може суттєво вплинути на ціни фінансових інструментів чи пов'язаних похідних фінансових інструментів означає інформацію, яку розсудливий інвестор, ймовірно, використає як частину підґрунтя для свого рішення з інвестування.

Стосовно товарних похідних інструментів, інсайдерська інформація означає будь-яку конкретну інформацію, яка не була оприлюднена та яка безпосередньо чи опосередковано стосується цих похідних інструментів, і яку користувачі ринків, на яких обертаються такі похідні інструменти, очікували б отримати відповідно до усталеної ринкової практики, що склалася на цих ринках.

Стосовно осіб, які уповноважені виконувати розпорядження щодо фінансових інструментів, інсайдерська інформація має також означати будь-яку конкретну інформацію, що представлена клієнтом і стосується його розпоряджень, що виконуються, і яка стосується безпосередньо чи опосередковано одного чи кількох емітентів фінансових інструментів або одного чи кількох фінансових інструментів, і яка, у випадку оприлюднення вірогідно могла б мати значний вплив на ефективність цих фінансових інструментів або на ефективність похідних від них фінансових інструментів.

Дослідження і розрахунки, зроблені на підставі загальнодоступних джерел інформації, не можуть розглядатися як інсайдерська інформація, отже, будь-які операції, проведені на основі таких досліджень або розрахунків, не можуть вважатись інсайдерською діяльністю. Інсайдерською діяльністю

є випадки, коли джерелом інсайдерської інформації виступає не сфера професійної діяльності або функціонування, а злочинна діяльність, підготовка і здійснення якої може справити значний вплив на ціну одного чи кількох фінансових інструментів, або на хід формування цін на організованих ринках.

Особі, яка володіє інсайдерською інформацією на підставі свого членства в управлінському, виконавчому чи наглядовому органі емітента, або на підставі її участі у капіталі емітента, або на підставі володіння доступом до такої інформації внаслідок виконання своїх службових чи професійних обов'язків, або через вчинення нею кримінальних дій забороняється використовувати цю інформацію, купуючи чи продаючи або намагаючись купити чи продати, за свій власний рахунок або за рахунок третьої особи, безпосередньо або опосередковано, фінансові інструменти, яких стосується ця інформація. Якщо вищезазначена особа є юридичною особою, то зазначені заборони також застосовуються до фізичних осіб, які беруть участь в ухваленні рішення щодо здійснення операції за рахунок цієї юридичної особи. Однак ці заборони не стосується операцій, що здійснюються для виконання зобов'язання щодо купівлі або продажу фінансових інструментів, якщо таке зобов'язання є наслідком правочину, який було укладено до того, як згадана особа отримала інсайдерську інформацію.

До таких осіб належать:

– члени органу управління або нагляду емітента;

– найвищі посадові особи, які постійно мають доступ на постійній основі до інсайдерської інформації емітента і наділені владними повноваженнями щодо прийняття стратегічних рішень емітента.

Використання інсайдерської інформації може полягати в придбанні або відчуженні фінансових інструментів особою, яка знає або мала знати, що інформація, якою вона володіє, має статус інсайдерської. У цьому контексті уповноважені органи мають виходити з того, що за таких самих обставин знала б або мала б знати звичайна та розумна особа. Більше того, простий факт того, що дилери та брокери, особи, яким дозволено діяти як контрагенти, або особи, які уповноважені виконувати розпорядження від імені третіх осіб, які володіють інсайдерською інформацією, обмежуються в перших двох

випадках веденням власної законної діяльності з купівлі та продажу фінансових інструментів, а в останньому випадку – старанним виконанням розпорядження, не може сам по собі означати використання цієї інсайдерської інформації.

Оскільки придбання або відчуження фінансових інструментів неодмінно включає прийняття попереднього рішення про придбання або про відчуження особою, яка провадить цю чи іншу операцію, здійснення придбання або відчуження не може саме по собі вважатись використанням інсайдерської інформації. Доступ до інсайдерської інформації щодо іншого товариства та використання її у контексті публічної пропозиції про поглинання з метою отримання контролю над цим товариством або пропозиції про злиття з цим товариством не може саме по собі вважатися інсайдерською діяльністю.

Забороняється будь-якій особі, яка володіє інсайдерською інформацією з підстав, зазначених вище:

а) розголошувати інсайдерську інформацію будь-якій іншій особі, крім випадків, коли таке розголошення відбувається в результаті виконання нею своїх звичайних професійних чи службових обов'язків;

б) на основі інсайдерської інформації рекомендувати іншій особі або спонукати її до купівлі або продажу фінансових інструментів, яких ця інформація стосується.

На осіб, які відповідальні за безпеку інсайдерської інформації покладається обов'язок забезпечувати опублікування емітентами всієї інсайдерською інформації, яка підлягає оприлюдненню, у належний строк на їхніх Інтернет-сайтах, складати, регулярно оновлювати та подавати до компетентного органу список осіб, що працюють у них на підставі трудового договору або інших підставах і мають доступ до інсайдерської інформації.

Розміщення інсайдерської інформації емітентів на Інтернет-сайтах має відбуватися відповідно до чинних правил передачі особистих даних третім державам.

Емітент не може поєднувати надання громадськості інформації та діяльність з маркетингу у спосіб, який може ввести в оману. Будь-які суттєві зміни, що стосуються вже публічно розкритої інсайдерської інформації, публічно

розкриваються одразу ж після настання цих змін за допомогою того ж каналу, що й під час публічного розкриття початкової інформації. На осіб, які відповідають за безпеку інформації покладено обов'язок вимагати, щоб емітенти належно дбали про забезпечення якомога синхронізованішого публічного розкриття інсайдерської інформації серед всіх категорій інвесторів у всіх державах–членах, в яких емітенти просили або отримали доступ своїх фінансових інструментів до торгівлі на регульованому ринку.

Емітент може під свою власну відповідальність відстрочити оприлюднення інсайдерської інформації, наприклад, для запобігання порушенню його законних інтересів, за умови, що таке відстрочення не може ввести громадськість в оману, та за умови, що емітент буде в змозі забезпечити конфіденційність цієї інформації. Однак, при цьому державам–членам надано право вимагати негайного інформування відповідного компетентного органу про рішенця емітента відстрочити оприлюднення інсайдерської інформації.

Безпека інформації, яка стосується суб'єктів господарювання визначає, що законні інтереси можуть стосуватися, зокрема, таких обставин, перелік яких не є вичерпним:

а) триваючі переговори або пов'язані обставини, коли на результат чи на звичний хід цих переговорів, ймовірно, може вплинути публічне розкриття. Зокрема, коли фінансовому стану емітента загрожує серйозна небезпека, хоча вона й не підпадає під дію відповідних правових норм про неплатоспроможність, публічне розкриття інформації можна відкласти на визначений строк, впродовж якого таке публічне розкриття може серйозно зашкодити інтересам існуючих та потенційних акціонерів, зриваючи конкретні переговори, призначені для забезпечення довгострокового фінансового оздоровлення емітента;

б) коли прийняті рішення чи укладені керівним органом емітента контракти потребують схвалення іншого органа емітента для того, щоб вступити в силу, коли організація такого емітента вимагає розподілу повноважень між цими органами, за умови, що публічне розкриття інформації до такого схвалення разом з одночасним оголошенням про те, що передбачається таке схвалення, поставить під загрозу правильну оцінку інформації громадськістю.

Суб'єкти господарювання вимагають, щоб з метою забезпечення конфіденційності інсайдерської інформації емітент контролював доступ до такої інформації та щоб емітент вжив ефективні та необхідні заходи:

– для запобігання доступу до такої інформації осіб, інших ніж ті, яким така інформація потрібна для виконання своїх службових функцій;

– для забезпечення того, щоб кожна особа, яка має доступ до такої інформації, усвідомлювала пов'язані з цим обов'язки, встановлені законами та підзаконними актами, а також санкції, що застосовуються в разі неправильного використання або неналежного поширення такої інформації;

– що уможливлюють негайне публічне розкриття у разі, коли емітент не зміг забезпечити конфіденційність важливої інсайдерської інформації.

У разі, коли емітент або особа, що діє від його імені або за його рахунок, розголошує будь-яку інсайдерську інформацію будь-якій третій особі, виконуючи свої звичайні професійні чи службові обов'язки, як це передбачено у статті 3 (а), емітент повинен зробити повне та ефективне розкриття цієї інформації, одночасно – якщо розкриття має міжнародний характер, та швидко – за внутрішньодержавного розкриття крім випадків, коли особа, яка отримує таку інформацію, зобов'язана зберігати її конфіденційність відповідно до закону, положення, статуту або договору.

Будь-яка особа, яка професійно здійснює операції з фінансовими інструментами і яка обґрунтовано підозрює, що такі операції можуть бути класифіковані як інсайдерська діяльність або маніпуляції на ринку, повинна негайно повідомити про це компетентний орган.

Стабілізаційні дії щодо фінансових інструментів або торгівлі власними акціями в програмах з викупу власних акцій можуть бути законними за певних обставин, зокрема, з економічних міркувань, і тому не можуть самі по собі розглядатись як зловживання на ринку.

На суб'єктів господарювання покладається також обов'язок запровадити належне регулювання діяльності осіб, які проводять дослідження або поширюють результати таких досліджень у сфері фінансових інструментів чи емітентів

фінансових інструментів, а також осіб, які надають рекомендації або пропозиції щодо стратегії інвестування, призначені для розповсюдження або оприлюднення, для забезпечення неупередженого подання інформації та висвітлювання їхніх інтересів або конфлікту інтересів стосовно фінансових інструментів, яких така інформація стосується. Також було покладено обов'язок ухвалити заходи з імплементації стосовно: спеціальних правил щодо належного оприлюднення інсайдерської інформації, спеціальних правил відстрочення оприлюднення інсайдерської інформації, умов, за яких емітенти або інші юридичні особи, що діють від імені емітента, повинні укладати список осіб, які працюють на них, або мають доступ до інсайдерської інформації та умов, за яких такі списки мають оновлюватись, категорій осіб, які підпадають під обов'язок розкриття та ознаки операцій, включаючи їхній розмір, які породжують такий обов'язок, а також спеціальних правил щодо розкриття компетентному органу; спеціальних заходів щодо різних категорій осіб, що вживатимуться з метою забезпечення неупередженого оприлюднення результатів досліджень або будь-якої іншої інформації стосовно стратегії інвестування, розкриття приватних інтересів або конфлікту інтересів; спеціальних правил, які регулюють порядок інформування компетентного органу.

Так, зокрема, інформація про осіб, які мають доступ до інсайдерської інформації, розкривалася у спеціальних інсайдерських списках. До останніх пред'являються вимоги щодо їхнього регулярного відновлення і публічної доступності протягом 5 років з дати складання або відновлення. Всі угоди осіб, що здійснюють управлінські функції емітента, підлягають обов'язковому нагляду з боку компетентного органа суб'єкта господарювання за винятком угод, вартість яких не перевищує 5000 євро на кінець року.

Суб'єкти господарювання повинні забезпечити гарантію розкриття особами, які пропонують рекомендації і прогнози щодо вартості фінансових інструментів, усіх зв'язків і відносин, що свідчать про конфлікт інтересів і можуть послабити об'єктивність цих рекомендацій. У випадку поширення рекомендацій і прогнозів, отриманих від третіх.

Цілісність ринку вимагає відповідного публічного розкриття інформації зі стабілізаційної діяльності емітентів та суб'єктів, що вдаються до стабілізації, і незалежно від того, чи діють вони від імені таких емітентів. Методи, використані для відповідного розкриття такої інформації, повинні бути ефективними і можуть враховувати ринкові правила, прийняті компетентними органами влади.

Діяльність всіх інвестиційних товариств та кредитних установ, що вдаються до стабілізації, повинна відповідно узгоджуватися. Під час стабілізації інвестиційне товариство чи кредитна установа виступає в якості центрального довідкового пункту для будь-якого регуляторного втручання компетентних органів влади зацікавлених держав–членів.

Стабілізація означає будь-яку купівлю чи пропозицію купівлі відповідних цінних паперів, або будь-яку операцію з подібними їм пов'язаними інструментами, що здійснюється інвестиційними товариствами чи кредитними установами в рамках суттєвого розподілу таких відповідних цінних паперів виключно для підтримки ринкової ціни на ці відповідні цінні папери впродовж визначеного періоду в результаті напливу пропозицій з продажу.

Проблема розкриття інформації та використання інсайдерської інформації при укладанні угод з цінними паперами є актуальною навіть для країн, де відповідне законодавство діє вже не перший рік.

В Україні довгий час залишались неврегульованими проблеми використання інсайдерської інформації під час укладання угод з цінними паперами, що спотворювало ціни на фондовому ринку, знижувало довіру до ринку цінних паперів та його учасників. Па захист прав і законних інтересів емітентів та інвесторів, контроль за діяльністю інсайдерів на ринку цінних паперів спрямовані норми нещодавно прийнятого Закону України «Про цінні папери та фондовий ринок».

У новоприйнятому Законі України «Про цінні папери та фондовий ринок» питання розкриття інформації на фондовому ринку присвячений розділ 5.

Відповідно до ст. 39 Закону України «Про цінні папери та фондовий ринок» емітенти, які здійснили відкрите (публічне)

розміщення цінних паперів, зобов'язані своєчасно та в повному обсязі розкривати інформацію про:

– фінансово-господарський стан і результати діяльності емітента у строки, встановлені законодавством;

– будь-які дії, що можуть вплинути на фінансово-господарський стан емітента та призвести до значної зміни ціни на його цінні папери;

– власників великих пакетів (10 відсотків і більше) акцій.

Інформація про власників великих пакетів (10 відсотків і більше) акцій подається Державній комісії з цінних паперів та фондового ринку особою, яка веде облік права власності на акції емітента у депозитарній системі України, у строки, порядку та за формою, що встановлені Національною комісією з цінних паперів та фондового ринку.

Інформація про власників великих пакетів (10 відсотків і більше) акцій є відкритою і оприлюднюється Національною комісією з цінних паперів та фондового ринку шляхом розміщення у загальнодоступній інформаційній базі даних Національної комісії з цінних паперів та фондового ринку про ринок цінних паперів.

Стаття 40 Закону України «Про цінні папери та фондовий ринок» дає визначення поняття та визначає порядок надання регулярної інформації емітента. Регулярна інформація про емітента – річна та квартальна звітна інформація про результати фінансово-господарської діяльності емітента, яка подається Національній комісії з цінних паперів та фондового ринку (в тому числі в електронному вигляді).

Звітним періодом для складання річної інформації про емітента є календарний рік. Річна інформація про емітента повинна містити такі відомості: найменування та місцезнаходження емітента, розмір його статутного капіталу; орган управління емітента, його посадові особи та засновники; господарська та фінансова діяльність емітента; цінні папери емітента (вид, форма випуску, тип, кількість), розміщення та лістинг цінних паперів; річна фінансова звітність; аудиторський висновок. Емітент має право додатково подавати іншу інформацію.

Річна інформація про емітента є відкритою і підлягає оприлюдненню емітентом у строк не пізніше 30 квітня року,

наступного за звітним, шляхом опублікування її в одному з офіційних друкованих видань Верховної Ради України, Кабінету Міністрів України або Національної комісії з цінних паперів та фондового ринку і розміщення у загальнодоступній інформаційній базі даних Національної комісії з цінних паперів та фондового ринку про ринок цінних паперів. Примірник офіційного друкованого видання, в якому опубліковано річну інформацію про емітента, вій (емітент) надсилає до Національної комісії з цінних паперів та фондового ринку.

Звітним періодом для складання квартальної інформації про емітента є квартали поточного року. Квартальна інформація про емітента повинна містити такі відомості: найменування та місцезнаходження емітента, розмір його статутного капіталу; орган управління емітента, його посадові особи та засновники; господарська та фінансова діяльність емітента; цінні папери.

До особливої інформації належать відомості про:

– прийняття рішення про розміщення цінних паперів на суму, що перевищує 25 відсотків статутного капіталу;

– прийняття рішення про викуп власних акцій;

– факти лістингу/делістингу цінних паперів на фондовій біржі;

– отримання позики або кредиту на суму, що перевищує 25 відсотків активів емітента;

– зміну складу посадових осіб емітента;

– зміну власників акцій, яким належить 10 і більше відсотків голосуючих акцій;

– рішення емітента про утворення, припинення його філій, представництв;

– рішення вищого органу емітента про зменшення статутного капіталу;

– порушення справи про банкрутство емітента, винесення ухвали про його санацію;

– рішення вищого органу емітента або суду про припинення або банкрутство емітента.

Строки, порядок та форми подання особливої інформації про емітента встановлюються

Національною комісією з цінних паперів та фондового ринку та становлять два робочих дні. Особлива інформація про емітента є відкритою і оприлюднюється шляхом опублікування

її в одному з офіційних друкованих видань Верховної Ради України, Кабінету Міністрів України або Національної комісії з цінних паперів та фондового ринку і розміщення у загальнодоступній інформаційній базі даних Національної комісії з цінних паперів та фондового ринку про ринок цінних паперів.

Стаття 43 Закону України «Про цінні папери та фондовий ринок» визначає порядок розкриття інформації про облік іменних цінних паперів учасниками депозитарної системи України. Інформація про облік іменних цінних паперів розкривається учасниками депозитарної системи України:

– на письмовий запит власника інформації або з його письмового дозволу, крім випадків, передбачених абзацами третім і четвертим цієї частини;

– за рішенням суду;

– на письмову вимогу органів прокуратури, служби безпеки, внутрішніх справ, Національної комісії з цінних паперів та фондового ринку і Антимонопольного комітету України, інших державних органів відповідно до законодавства – стосовно операцій у системах обліку іменних цінних паперів, що здійснюються конкретною юридичною особою або фізичною особою за конкретний проміжок часу.

Учаснику депозитарної системи України забороняється надавати інформацію про клієнтів іншого учасника депозитарної системи України, навіть якщо їх дані зазначено у документах та договорах клієнта. Особи, винні в порушенні порядку розкриття та використання інформації про облік іменних цінних паперів, несуть відповідальність згідно із законом.

Порядок розкриття та захист інформації з системи депозитарного обліку визначається також розділом 5 проекту Закону України «Про систему депозитарного обліку цінних паперів», розробленого Національною комісією з цінних паперів та фондового ринку України.

Частина 1 статті 44 Закону України «Про цінні папери та фондовий ринок» визначає, що інсайдерською інформацією є будь-яка не оприлюднена інформація про емітента, його цінні папери або правочини щодо них, оприлюднення якої може значно вплинути на вартість цінних паперів. Інформація щодо

оцінки вартості цінних паперів та/або фінансово-господарського стану емітента, якщо вона отримана виключно на основі оприлюдненої інформації або інформації з інших публічних джерел, не заборонених законодавством, не є інсайдерською інформацією.

Отже, на підставі вищевикладеного ми можемо виділити три ключових елементів, зокрема це: статус інформації (неоприлюднена), точний характер (юридичний факт) та зміст інформації (стосовно емітента цінних паперів). Всі три ключі безпосередньо пов'язані з інформацією з обмеженим доступом. І безпека цієї інформації, зрозуміло, напряму залежить від осіб, які будуть відповідати за її збереження.

Отже розглянемо кожен ключ окремо.

Статус інформації. Як вже зазначалось, інсайдерська інформація є неоприлюденою, тобто нерозголошеною, невідомою широкому колу сторонніх осіб. Тому не важливо, чи є інформація секретною, чи відноситься до інформації з обмеженим доступом. Оприлюдненою інформація вважається тоді, коли вона відома необмеженому колу осіб. Причому, не має необхідності, щоб кожен інвестор мав цю інформацію або щоб вона була оприлюднена через засоби масової інформації. Достатньо, щоб вона була доступною через інформаційні системи широкого користування.

Зрозуміло, що інсайдери не мають права здійснювати операцію з цінними паперами одразу після повідомлення інсайдерської інформації громадськості. Необхідно витримати певний час не тільки для того, щоб інформація поширилася через засоби масової інформації, а і для того щоб громадськість відреагувала і курс цінних паперів відображав новину. Такий підхід є консервативним. Директива ЄС не передбачає конкретного часу, протягом якого інвестори мали б можливість оцінити інформаційне повідомлення і відреагувати на нього. Але вона не забороняє державам-членам зробити це на рівні їх законодавства, щоб запровадити більш об'єктивний критерій.

Отже, тільки якщо інформація вже була оприлюднена (незалежно від того, чи було це оприлюднення правомірним), то будь-які обмеження на операції з цінних паперів у зв'язку з інсайдерською інформацією знімаються.

Характер інформації. По-перше, інформація повинна бути «точного характеру». Цікавим є досвід німецького законодавства, яке застосовує термін «інсайдерські факти», а не «інсайдерська інформація». Термін факти вказує на те, що інсайдерською інформацією можуть бути лише об'єктивні явища або події, а не чиясь точка зору, висновки, рекомендації чи чутки. Зрозуміло, що інформація, яка є результатом зведення і аналізу оприлюднених даних, не може бути інсайдерською.

По-друге, інформація повинна бути істотною у тому розумінні, що її вплив на курс відповідних цінних паперів у випадку розголошення буде «значним». Хоч ця вірогідність повинна оцінюватись на момент укладення угоди, а не після оприлюднення, фактична зміна курсу після розкриття інформації буде першим показником істотності інформації [192, с. 73-76].

Зміст інформації. Необхідно, щоб існував зв'язок між інформацією і емітентом. Інформація повинна стосуватися одного чи кількох емітентів, або одного чи кількох цінних паперів. Змістом інсайдерської інформації може бути збільшення або зменшення статутного фонду, укладення договорів про розподіл прибутків або збитків, тендерні пропозиції, реорганізація суб'єкта господарювання, продаж активів, зміна організаційно-правової форми, ліквідація тощо.

Інсайдерам забороняється використовувати інформацію з повним знанням справи шляхом придбання або продажу обігових цінних паперів емітента або емітентів, яких ця інформація стосується, для себе або для третіх осіб прямо або опосередковано.

Заборона поширюється не тільки на здійснення операцій з цінними паперами на біржі, але також і на позабіржовому ринку, якщо така операція здійснена через професійного посередника.

У той час, як володіти інсайдерською інформацією можуть лише фізичні особи, інсайдерські операції можуть здійснюватись і на користь юридичних осіб. Якщо інсайдер є юридична особа, то заборона поширюється на фізичних осіб, які приймають рішення здійснити операцію на користь відповідної юридичної особи.

Для притягнення до відповідальності існує кілька істотних обмежень. По-перше, інсайдер повинен знати, що інформація,

яку він використовує, є інсайдерською. Отже, у діях інсайдера повинен бути умисел на використання інсайдерської інформації для проведення операції купівлі-продажу цінних паперів. Необережність, навіть у самих грубих її формах, не може бути підставою притягнення до відповідальності. По-друге, повинен бути присутній причинно-наслідковий зв'язок між володінням інформацією і рішенням здійснити операцію. По-третє, операція повинна бути завершена, тобто незаконним вважається виконання угоди, укладеної на основі інсайдерської інформації. укладання угоди на основі інсайдерської інформації лише створює зобов'язання, що є недостатнім для притягнення до відповідальності.

Директива ЄС не передбачає необхідності доводити умисел, на одержання прибутку або уникнення збитків для себе чи третіх осіб. достатньо довести умисел інсайдера на здійснення операції на основі інсайдерської інформації. Також немає необхідності доводити те, що операція принесла прибутки у будь-якому вигляді. Отже, навіть якщо у результаті інсайдерської операції інсайдер зазнав збитків, він все одно буде відповідати за порушення.

Директива ЄС забороняє не лише здійснення операцій з цінними паперами на основі інсайдерської інформацій, а і передачу інсайдерської інформації іншим особам, точніше «розкриття інсайдерської інформації третім особам за винятком, якщо таке розкриття здійснюється у ході звичайного здійснення трудових обов'язків». На перший погляд це правило виглядає зрозумілим. Насправді воно викликає більше запитань, ніж заборона здійснювати операції з цінними паперами. По-перше, Директива не вимагає наявності умислу в діях особи, яка передає інформацію. Це особа може навіть не знати про інсайдерський статус інформації і не підозрювати, що особа, яка одержує інформацію, може використати її для проведення операції з цінними паперами.

У той же час, розкриття інформації в рамках звичайного здійснення трудових професійних або інших обов'язків звільняє від відповідальності. Логіка цього положення зрозуміла: передача інформації в межах суб'єкта господарювання, а також консультантам, аудиторам тощо повинна бути дозволена. Наприклад, корпоративний секретар зобов'язаний інформувати

наглядову раду про стан справ акціонерного товариства (ст. 56 ЗУ АТ). Така передача інсайдерської інформації наглядовій раді не є забороненою. Аналізуючи коло осіб, яким інформація може передаватися «в рамках звичайного здійснення трудових, професійних або інших обвозів» можна побачити, що це будуть ті ж самі особи, які попадають у категорії інсайдерів. Отже, вони обов'язково будуть обмежені у своїй здатності здійснювати операції і передавати інсайдерську інформацію [193, с. 77-81].

3.3. Зміст адміністративно-правового захисту інформації у суб'єктах господарювання

Проблема захисту інформації завжди була і залишалась актуальною не тільки для приватного, але й для публічного права. Принциповою ознакою адміністративно-правового захисту інформації є його цілеспрямованість. Саме тому багато дослідників, зокрема Г.В. Атаманчук, В.Д. Бакуменко, Н.Л. Карданська, А.А. Кокошин, В.К. Колпаков, Б.А. Кормич, В.А. Ліпкан, Н.Р. Нижник, Г.П. Ситник, В.С. Цимбалюк та інші, загалом дотримуються спільної позиції в тому, що суттю управлінської діяльності є досягнення тих чи інших цілей, а змістом – дії щодо її досягнення, для чого залучаються певні ресурси, які в процесі досягнення згаданих цілей мають бути використані найбільш ефективно.

Завдяки цим вченим сучасна наука отримала ряд теорій, які розкривають зміст інформації та його захисту. У свою чергу вчені із зазначеного переліку визначили різні аспекти теорії адміністративно-правового захисту інформації, визначили поняття, принципи, функції та засоби зазначеної теорії як відносно самостійного інституту правознавства. Поряд з цим усі вони цілеспрямовано вирішували проблему захисту інформації суб'єктів господарювання засобами публічного права, концентрували свої наукові пошуки на більш загальних чи суміжних студіях.

Таким чином, детальний аналіз юридичної літератури призводить до висновку, що вітчизняна теорія адміністративно-правового захисту інформації суб'єктів господарювання

залишається не повною мірою розробленою та потребує подальших досліджень.

У доступній нам юридичній літературі можна зустріти три основних підходи до розкриття сутності категорії адміністративно-правового захисту інформації.

Перший із них, прихильниками якого були вчені другої половини XX століття – засновники адміністративно-правової теорії охорони соціалістичної власності А.В. Венедиктов, З.М. Рахлін, В.Д. Резвих та ін. Зрозуміло, що всі вони виходили в своїх працях із теоретичних положень державного права країни, коли її головним напрямком діяльності у внутрішніх сфері була функція охорони соціалістичної державної й колективної власності.

Тим самим вони практично були змушені уникати проблеми охорони індивідуальної власності громадян. Поряд з таким негативом їхніми працями було закладено теоретичні аспекти адміністративно-правової охорони власності, які не втратили своєї актуальності і в умовах сьогодення.

Так, А.В. Венедиктов визначив, що інститут права власності не можна вважати виключно цивільно-правовим надбанням, бо він поряд із цивільно-правовими нормами включає в себе норми інших галузей права (адміністративного, фінансового, трудового тощо) [194, с. 326-329]. Тим самим уперше у вітчизняній юриспруденції були визначені нові напрямки юридичного захисту права власності (поряд із домінуючими до цього часу кримінально-правовим і цивільно-правовим). Зокрема почала розвиватись наука і практика адміністративно-правового захисту власності.

Першим корифеєм у сфері адміністративно-правової охорони соціалістичної власності по праву вважається З.М. Рахлін, який в 1965 р. у Харківському юридичному інституті захистив дисертацію на здобуття наукового ступеня доктора юридичних наук. Ним була остаточно утверджена теорія адміністративно-правової охорони права власності як відносно самостійного інституту правознавства [195, с. 45]. Серед іншого він стверджував, що адміністративно-правовий захист застосовується для попередження, недопущення збитків власності з боку злочинних елементів, так як одних

кримінально-правових засобів боротьби проти осіб, які посягають на власність, недостатньо.

Таким чином, він сформулював сталу вже у сучасному адміністративному праві точку зору, що адміністративно-правові засоби охорони використовуються не тільки безпосередньо для захисту права власності від дрібних розкрадань, але й є важливим засобом профілактики суспільно-небезпечної майнової злочинності.

Інший відомий вчений тієї доби В.Д. Резвих у 70-80 року XX століття поновив і вдосконалив теорію адміністративно-правової охорони права власності. Ним було розкрито розуміння способу адміністративно-правової охорони права власності, вдосконалено адміністративну складову профілактики майнових злочинів, визначено сутність контрольно-наглядової діяльності органів державної влади у сфері охорони власності тощо [196, с. 157-172]. Серед іншого він зазначав, що адміністративно-правовий спосіб охорони власності – це виконавчо-розпорядча діяльність державних органів та органів громадськості, змістом якої є попередження посягань на майно, організація охорони та безпосередня охорона, а також застосування заходів адміністративного впливу у випадках, передбачених правовими нормами [196, с. 23].

Таким чином, перша когорта вчених (А.В. Венедиктов, З.М. Рахлін, В.Д. Резвих та ін.), які працювали в другій половині XX століття, розкрила розуміння адміністративно-правової охорони власності як виконавчо-розпорядчої діяльності державних і громадських органів, яка здійснювалась з метою попередження посягань на майно, організації його охорони органами державної влади та забезпечення її безпосередньої охорони правоохоронними й іншими спеціально створеними для цієї мети державними і колективними структурами, з правом застосування до порушників режиму власності адміністративного впливу.

Отже, основним недоліком зазначеного розуміння адміністративно-правової охорони права власності було те, що вона обслуговувала головну для тієї держави – функцію охорони соціалістичної власності. Сутністю її в негативному плані було таке: по-перше, цінність державної та колективної власності у тій державі ставились на рівень, а інколи і вище невід'ємних,

невідчужуваних прав і свобод людини та громадянина; по-друге, заперечувалась приватна власність як засіб виробництва; по-третє, наявною була другорядність значення та захисту індивідуальної власності громадян.

Другий підхід до адміністративно-правового захисту власності формувався вченими в період глобальної перебудови політичної, економічної та юридичної сутності держави і суспільства в останні роки входження України до складу Радянського Союзу (з 1985 р.) та в перші роки відновлення незалежності України – включно до прийняття 28 червня 1996 р. Конституції України.

У цілому він може бути охарактеризований загальною демократизацією відносин між громадянами та державою, яка на початковому етапі реформ підняла ініціативу широких верст населення, зокрема у сфері боротьби з дрібним розкраданням народного надбання. Поряд з тим відмова від планової економіки при відсутності повноцінного ринкового законодавства, культури діяльності і праці органів державної влади та широких верст населення в умовах ринкової економіки, а також провал швидкої приватизації на початки 90-х років XX століття призвели до системної економічної, політичної та юридичної кризи, яка у сфері охорони державної і колективної власності, при загальній політиці правоохоронних органів на зниження адміністративного тиску зумовила негативні наслідки. Були розукомплектовані, а у подальшому розграбовані сотні тисяч державних і колективних підприємств, як зазначає В.В. Галунько [197, с. 42-43].

У таких складних умовах вчені І.П. Голосніченко, Ю.П. Полетаєв, О.І. Нікітенко та інші сконцентрували свої пошуки у напрямку вирішення нових проблем у сфері адміністративно-правового захисту власності.

Так, І.П. Голосніченко надав науковій спільноті, правотворчим і правоохоронним органам теорію «Попередження корисливих проступків засобами адміністративного права», в якій важливе місце було приділено питанню попередження дрібних розкрадань державного та громадського майна [144, с. 9]. При цьому він відповідно до публічної спрямованості та особливості адміністративного права виділяв як головний його напрям функцію охорони

суспільних відносин, механізм якої включає в себе правовідносини, породжувані діями, що посягають на регульовані суспільні відносини [144, с. 43]. Серед засобів попередження корисливих проступків, висвітлених І.П. Голосніченком, які не втратили своєї актуальності до сьогодні, можна відзначити застосування економічних способів господарювання; економне витрачання сировини та матеріалів; удосконалення охорони із забезпечення схоронності товарно-матеріальних цінностей; нагляд за веденням монтажних робіт з обладнання засобами охоронної сигналізації та ін. [144, с. 48].

У свою чергу Ю.М. Полєтаєв на початку 90-х років XX століття, досліджуючи питання «Правової охорони майна державного підприємства (об'єднання)», поставив собі за завдання надати відповіді на основні питання використання засобів права щодо забезпечення збереження власності в умовах розвитку товарно-грошових та регульованих ринкових відносин [198, с. 7]. При цьому він розкривав зазначене через категорію «збереження власності», під якою розумілось організована та постійна діяльність державних і громадських організацій, трудових колективів і громадян, які сприяють забезпеченню цілісності власності, попередження втрат майна, посилення режиму економіки, раціонального і ефективного використання ресурсів з метою примноження суспільного надбання [198, с. 65]. Він зазначав, що відома роль у процесі збереження власності належить саме адміністративно-правовій її охороні, яка представляє собою проведення заходів із захисту відношень власності засобами адміністративного права, що дозволяє попередити суспільно-небезпечне діяння й усунути його шкідливі наслідки. До основної визначної риси адміністративно-правового захисту Ю.М. Полєтаєв відніс те, що як орган, який здійснює її, в обов'язковому порядку виступає той чи інший орган державного управління чи державної влади, який здійснює чи контролює її законне використання. Серед способів такого захисту він назвав: по-перше, засоби, що забезпечують профілактику (попередження) порушень правового режиму майна; по-друге, засоби боротьби з конкретними посяганнями на майно [198, с. 96-97].

В умовах утвердження незалежності України О.І. Нікітенко здійснив спробу пристосувати кращі надбання теорії

адміністративно-правового захисту соціалістичної власності до нових соціально-економічних умов. Але, на наш погляд, відсутність на той час новітніх доктринальних теоретичних розробок і джерел конституційного права, які має доповнювати і розвивати наука адміністративне права, не дозволили йому сформулювати вітчизняну теорію захисту права власності, яка б відповідала вимогам соціальної правової держави [199, с. 109-115].

Таким чином, зусиллями І.П. Голосніченка, Ю.М. Полєтаєва, О.І. Нікітенка та інших учених, що досліджували проблему захисту власності в період останніх років входження українських земель до складу іноземних держав та у перші роки незалежності України, здійснювались намагання модернізувати теорію адміністративно-правової охорони соціалістичної власності до вимог ринкової, соціальної, правової держави, але відсутність відповідних новітніх розробок у галузі конституційного права, на які має опиратись та розвиватись адміністративне право, не дозволили їм сформулювати новітню теорію адміністративно-правого захисту права власності в Україні.

Третій новітній підхід до розкриття сутності захисту права власності був вироблений вітчизняними вченими В.Б. Авер'яновим, В.В. Галуньком, М.В. Ковалів, Т.М. Кравцовою, М.М. Пендюрою, Р.Б. Шишкою та ін. після прийняття 28 червня 1996 р. Конституції України, відповідно до ст. 3 якої людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю.

У сфері захисту права власності Конституція України визначила, що: по-перше, «Кожний громадянин має право користуватися природними об'єктами права власності народу відповідно до закону. Власність зобов'язує. Власність не повинна використовуватися на шкоду людині і суспільству. Держава забезпечує захист прав усіх суб'єктів права власності і господарювання, соціальну спрямованість економіки. Всі суб'єкти права власності рівні перед законом» (п. 2-4 ст. 13 Конституції України); по-друге, «Кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності [77].

Право приватної власності набувається в порядку, визначеному законом. Громадяни для задоволення своїх потреб можуть користуватися об'єктами права державної та

комунальної власності відповідно до закону. Ніхто не може бути протиправно позбавлений права власності. Право приватної власності є непорушним. Примусове відчуження об'єктів права приватної власності може бути застосоване лише як виняток з мотивів суспільної необхідності, на підставі і в порядку, встановлених законом, та за умови попереднього і повного відшкодування їх вартості. Примусове відчуження таких об'єктів з наступним повним відшкодуванням їх вартості допускається лише в умовах воєнного чи надзвичайного стану. Конфіскація майна може бути застосована виключно за рішенням суду у випадках, обсязі та порядку, встановлених законом. Використання власності не може завдавати шкоди правам, свободам та гідності громадян, інтересам суспільства, погіршувати екологічну ситуацію і природні якості землі» (ст. 41 Конституції України) [77].

Зазначені положення Конституції України, побудовані на кращих взірцях вітчизняної та світової ліберально-демократичної правової думки, створили благодатні вихідні положення для подальшого розвитку правотворчого процесу та розвитку доктринальних юридичних досліджень у сфері захисту права власності.

У правотворчому напрямку були прийняті важливі законодавчі акти, які позитивно вплинули на забезпечення захисту права власності. Серед них відзначимо Цивільний, Цивільний процесуальний, Господарський, Земельний, Митний, Кримінальний кодекси, Кодекс адміністративного судочинства України, закони України про зміни і доповнення до Кодексу України про адміністративні правопорушення тощо.

Поряд з цим на доктринальному рівні складні суспільні відносини у сфері адміністративно-правового захисту суб'єктів господарювання довгий час не були підтверджені вітчизняною демократичною та ефективною теорією, що б відповідала вимогам правової соціальної держави, в якій будується громадянське суспільство.

Лише в 2003 р. вийшла за цією тематикою перша монографічна спеціалізована праця (М.В. Ковалів) «Правові та організаційні засади забезпечення збереження вантажів на залізничному транспорті України» [200, с. 120]. У тому ж році Т.М. Кравцова захистила дисертацію на здобуття наукового

ступеня доктора юридичних наук на тему «Адміністративно-правові засади здійснення державної політики у сфері господарювання», в якій розкрила регуляторну функцію держави та регулятивну функцію права у сфері господарювання, чим було створено теорію адміністративно-господарського права як підгалузі адміністративного права [201, с. 167]. При цьому зазначимо, що сформована Т.М. Кравцовою теорія, в основу якої покладено регулятивні норми адміністративного права, на наш погляд, вимагає подальших досліджень щодо розкриття захисної функції права у зазначеній сфері.

Серед суміжних галузей права особливий інтерес для нас мають праці цивіліста Р.Б. Шишки, який досліджує проблеми цивільно-правової охорони суб'єктів інтелектуальної власності. Найбільш слушним для нашого дослідження серед його теоретичних надбань є те, що він одним із перших у вітчизняній доктринальній науці правознавства у сфері охорони права власності розглянув дану проблему через конституційну призму «захисту прав усіх суб'єктів права власності (ст. 13 Конституції України)», а не власності, як це традиційно розглядалось раніше. Р.Б. Шишка правильно на наш погляд, стверджує, що: «Генезис охорони виявляється у здатності його механізму врегулювати суспільні відносини на користь носія суб'єктивного права і правомірного інтересу...» [202, с. 24]. Тим самим він розвинув теорію охорони права власності у зазначеній ним сфері через призму забезпечення, охорони, захисту прав і свобод людини і громадянина.

Зазначені положення теорії охорони права суб'єктів інтелектуальної власності, на наш погляд, повністю корелюються з думкою провідного вітчизняного адміністративіста В.Б. Авер'янова, який вважає, що сучасне європейське адміністративне право за своїм «духом», за своєю ідеологією орієнтовано на забезпечення прав та інтересів людини, їх ефективний захист. При цьому ним відзначається відставання вітчизняного адміністративного права від зазначеного положення, бо воно орієнтовано на задоволення потреб держави, державного управління (фактично – державного апарату та його чиновників) [147, с. 57].

В умовах, коли відповідно до Закону України «Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу» від 18 вересня 2004 р. зазначається, що «Державна політика України щодо адаптації законодавства формується, спрямовується на забезпечення єдиних підходів до нормопроектування, обов'язкового врахування вимог законодавства Європейського Союзу під час нормопроектування…» [203], і впровадження основного підходу європейського права – забезпечення, охорони та захисту прав людини і громадянина у теорії адміністративного права та практиці адміністративної діяльності суб'єктів публічного управління є, на наш погляд, невідворотнім.

Таким чином, запропонований підхід до розкриття проблеми захисту права власності через призму забезпечення суб'єктивних прав і свобод людини і громадянина є придатним не тільки для приватного, але й для публічного права.

Виходячи з такого новітнього напрямку розвитку адміністративного права, В.В. Галунько при розкритті теорії адміністративно-правової охорони права власності в Україні виходить саме з таких зазначених нами вище позицій. Він вважає, що: по-перше, згідно з вимогами теорії природного права, як типу праворозуміння, захисту підлягає не власність сама по собі, а суб'єкти права власності, іншими словами – власники майна (особи, які здійснюють ним управління) [197, с. 10; 29, с. 129-149]; по-друге, на відміну від цивільного права власники майна (особи, які здійснюють ним управління в механізмі адміністративно-правового захисту права власності, є не тільки правоможними особами, але й зобов'язальними щодо широкого кола осіб, яким може бути завдано шкоду їх шкідливим майном [199, с. 109-128]; по-третє, теорія соціальної демократичної держави, аналіз положень Конституції України призвели його до висновку про непритаманність такій державі функції охорони власності, яку він з метою недопущення теоретичного вакууму пропонує замінити комплексною функцією охорони права власності, що складається з тріади – функції охорони приватної власності як невід'ємної природної власності людини і громадянина; функції охорони права власності суб'єктів господарювання та функції охорони всіх осіб, які перебувають на території країни, від власності підвищеної

небезпеки [199, с. 179– 202]; по-четверте, ним запропоновано ієрархічну шкалу цінностей у зазначеній сфері : охорона прав і свобод людини й громадянина взагалі – охорона прав власників майна та всіх осіб, які можуть потерпіти від шкідливого майна перших – забезпечення недоторканності (збереження якісних і кількісних властивостей) майна [199, с. 205].

На погляд В.В. Галунька, адміністративно-правова охорона права власності у вузькому розумінні (адміністративно-правовий захист) – це імперативно владна діяльність суб'єктів публічного управління із захисту прав усіх суб'єктів права власності (осіб, які здійснюють управління нею) від протиправних посягань і широкого загалу осіб від майна підвищеної небезпеки, з нормативно-прописаною можливістю застосування до порушників режиму власності засобів державного впливу [197, с. 224-225].

Таким чином, вітчизняні вчені В.Б. Авер'янов, В.В. Галунько, Т.М. Кравцова, Р.Б. Шишка на основі розвитку положень Конституції України, згідно із п. 4 ст. 13 яких держава забезпечує захист прав усіх суб'єктів права власності і господарювання, соціальну спрямованість економіки, здійснили дослідження проблеми захисту права власності через призму суб'єктивного права людини і громадянина на «володіння, користування та розпорядження своєю власністю, результатами своєї інтелектуальної, творчої діяльності» (п. 1 ст. 41 Конституції України).

Представником *четвертого* підходу до розкриття забезпечення права власності є російський вчений В.У. Хатуаєв, який вважає, що адміністративно-правовий захист майна складається із сукупності правових норм, які регулюють суспільні відносини у сфері забезпечення безпеки майна [204, с. 62].

До такого концептуального підходу, коли майно само по собі за своїми якостями в ієрархічній системі цінностей права піднімається до рівня забезпечення «безпеки», критично ставиться В.В. Галунько. Він вважає, що виходячи з непритаманності для сучасної демократичної правової держави функції охорони власності, У. Хатуаєв дещо перевищує значення «майна» у системі сучасних соціальних та юридичних цінностей, розвиваючи теорію адміністративного права до рівня «майнової безпеки». З цих міркувань вдалою є точка зору вітчизняного

вченого М.М. Пендюри, що розглядає забезпечення і захист майнових прав громадян через призму «безпеки людини» як найвищої соціальної цінності соціуму та держави, при якій домінуючим у системі безпеки має бути забезпечення безпечного існування особистості, її прав і свобод [205, с. 144].

Ми підтримує точку зору В.В. Галунька та М.М. Пендюри і вважаємо, що дослідження проблеми забезпечення права власності, запропоноване А.У. Хатуаєвим через категорію «майнової безпеки», є таким, що не відповідає сучасним вимогам Конституції України та європейським міжнародно-правовим актам.

Здійснений аналіз думок провідних вчених у сфері захисту права власності приводить нас до обґрунтованого висновку, що найбільш слушною з точки зору Конституції України та теорії природного права як типу праворозуміння є точка зору вчених із третьої когорти В.Б. Авер'янова, В.В. Галунька, Т.М. Кравцової, М.М. Пендюри, Р.Б. Шишки. Наріжним каменем розуміння ними сутності адміністративно-правового захисту права власності є дослідження цієї проблеми через призму забезпечення, охорони, захисту суб'єктивного права людини і громадянина на володіння, користування та розпорядження своєю власністю, результатами своєї інтелектуальної творчості.

Одним із наступних питань, що вимагає теоретичного освітлення у нашому дослідженні, є розмежування розуміння адміністративно-правової «охорони» та «захисту». Цьому питанню були присвячені численні дискусії вчених у галузі приватного і публічного права. В умовах сьогодення переважна кількість вчених-юристів дотримується співвідношення «правової охорони» і «правового захисту» як цілого й частки. На основі аналізу думок провідних у цій сфері вчених, на наш погляд, найбільш слушно зазначену проблему розкрив В.В. Галунько. Він звертає увагу читачів на недопущення тотожності понять «охорона» та «захист» і вважає, що «охорона» в юридичному розумінні означає позитивний стан норм права, який направлений на безпосередній захист суб'єктивних прав і законних інтересів осіб від можливих порушень та відображає статику правовідносин. У свою чергу «захист» відображає динаміку та способи й форми, які передбачені законодавством для відновлення правового становища потерпілого,

притягнення винного до юридичної відповідальності, та застосовуються тоді, коли суб'єктивне право вже порушено [197, с. 195].

Таким чином, підтримуючи зазначені вище погляди В.В. Галунька, ми вважаємо, що правовий захист права власності характеризується такими ознаками: 1) є невід'ємною складовою більш широкої категорії «охорони права власності»; 2) застосовується тоді, коли суб'єктивне право власності вже порушене; 3) відображає динаміку (засоби і форми) відновлення порушеного стану власника майна (особи, яка здійснює ним управління).

Поряд з цим розкриті В.Б. Авер'яновим, В.В. Галуньком, Т.М. Кравцовою, М.М. Пендюрою, Р.Б. Шишкою положення щодо адміністративно-правових засобів захисту права власності суб'єктів господарювання можуть бути охарактеризовані як такі, що розкривають тільки загальні чи суміжні проблеми у зазначеній сфері. Тим самим, створивши загальний фон, вони потребують додаткової власної розробки з метою забезпечення ефективного та демократичного захисту прав суб'єктів господарювання.

В останні роки йде розвиток вітчизняних джерел права в напрямку адаптації правової системи України до стандартів Європейського Союзу. Одним із таких позитивів є прийняття Верховною Радою України 6 липня 2005 р. Кодексу Адміністративного судочинства, який ознаменував практичне втілення в життя вітчизняного суспільства адміністративного судочинства. Завданням останнього є захист прав, свобод та інтересів фізичних осіб, прав та інтересів юридичних осіб у сфері публічно-правових відносин від порушень з боку органів державної влади, органів місцевого самоврядування, їхніх посадових і службових осіб, інших суб'єктів при здійсненні ними владних управлінських функцій на основі законодавства, зокрема на виконання делегованих повноважень. В умовах сьогодення йде динамічне становлення нового інституту «Адміністративного судочинства», в багатьох вищих навчальних закладах запроваджено курс «Адміністративна юстиція. Адміністративне право».

Тим самим не враховувати можливості захисту суб'єктивних прав фізичних і юридичних осіб від порушень суб'єктами

владних повноважень засобами адміністративного судочинства буде, на наш погляд, невиваженим рішенням. Зазначене вимагає дослідити механізм забезпечення охорони права власності суб'єктів господарювання за допомогою системи адміністративних судів та виробити на цій основі рекомендації щодо її подальшого удосконалення.

Таким чином, одним із напрямків адміністративно-правового захисту права власності, на наш погляд, є використання власниками майна – суб'єктами господарювання – засобів адміністративного судочинства.

Критичний аналіз змісту Господарського кодексу України звертає нашу увагу на розділ 27 під назвою «Адміністративно-господарські санкції». Норми адміністративно-господарських санкцій є складовими інституту адміністративної та господарської відповідальності й формуються як комплексний інститут права. Тим самим, враховуючи точку зору В.В. Галунька на те, що в системі адміністративно-правового захисту права власності суб'єкти охорони (власники майна або особи, які здійснюють ним управління) є не тільки правоможними суб'єктами, але й зобов'язаними щодо недопущення шкідливого (небезпечного) використання своєї власності, ми вважаємо, що інститут адміністративно-господарських санкцій є предметом дослідження у сфері засобів адміністративно-правового захисту права власності суб'єктів господарювання.

Таким чином, з метою недопущення шкідливого використання майна, що використовується у сфері господарювання, одним із напрямків адміністративно-правових засобів захисту права власності суб'єктів господарювання є застосування суб'єктами публічного управління та Господарським судом засобів, що передбачені розділом 27 «Адміністративно-господарські санкції» Господарського кодексу України.

Викладене вище дає можливість сформулювати узагальнюючі ознаки розуміння адміністративно-правового захисту права власності суб'єктів господарювання:

1) забезпечення права власності суб'єктів господарювання має здійснюватись державою і суспільством силою адміністративного права через призму забезпечення

суб'єктивних прав людини і громадянина на володіння, використання та розпорядження своїм майном;

2) в адміністративно-правовій сфері власники майна (особи, які здійснюють ним управління) – суб'єкти господарювання – є не тільки правоможними суб'єктами, вони також одночасно є зобов'язальними об'єктами управління щодо недопущення шкідливого використання ввіреного їм майна та повноти і в установлені терміні сплати податків, інших обов'язкових державних і соціальних платежів;

3) у співвідношенні «адміністративно-правова охорона права власності суб'єктів господарювання» з «адміністративно-правовим захистом права власності суб'єктів господарювання» останньому притаманні такі риси: він є невід'ємною складовою першої; застосовується тоді, коли суб'єктивне право власності суб'єкта господарювання чи іншої особи від його майна вже порушене; відображає динаміку (засоби і форми) відновлення порушеного стану осіб які постраждали;

4) у вузькому розумінні адміністративно-правовий захист права власності суб'єктів господарювання – це імперативно владна діяльність суб'єктів публічного управління із захисту прав суб'єктів господарювання (осіб, які здійснюють управління нею) від протиправних посягань та широкого загалу осіб від майна підвищеної небезпеки, з нормативно-прописаною можливістю застосування до порушників режиму господарської власності засобів державного впливу;

5) важливим напрямком адміністративно-правового захисту права власності є використання суб'єктами господарювання – засобів адміністративного судочинства;

6) одним із напрямків адміністративно-правового захисту права власності є застосування до порушників режиму власності адміністративно-господарських санкцій, передбачених розділом 27 ГК України.

Отже, адміністративно-правовий захист права власності суб'єктів господарювання – це важливий напрямок активної діяльності суб'єктів публічного управління та адміністративного суду, який здійснюється на основі норм адміністративного права щодо забезпечення прав суб'єктів господарювання на володіння, користування та розпорядження своїм майном, поновлення прав осіб, які постраждали від майна

підвищеної небезпеки, з нормативно-прописаною можливістю застосування до порушників режиму господарської власності засобів державного впливу.

З ознак і наведеного поняття адміністративно-правового захисту права власності суб'єктів господарювання логічно випливають різні його види, класифікацію яких найбільш слушно здійснити за критеріями глибини юридичної регламентації, за суб'єктами забезпечення та за суб'єктами протиправного посягання.

За глибиною юридичної регламентації поділяється на правовий та організаційно-правовий. Правовий захист здійснюється не шляхом встановлення якихось механічних перепон з метою недопущення заволодіння осіб чужим майном, не фізичним наглядом за його кількісною та якісною наявністю, а силою адміністративно-правових норм, які стоять на захисті права власності суб'єкта господарювання і вимагають того, що ніхто не має право володіти, користуватись та розпоряджатись чужою власністю без дозволу господаря. У випадку ж порушення цього правила адміністративно-правові норми встановлюють, що особа, яка порушила суб'єктивне право іншої особи, буде невідворотно притягнута до юридичної відповідальності, а незаконно набуте майно у неї вилучене. Крім того адміністративно-правові норми вимагають від винного відшкодувати потерпілому власнику завдані матеріальні й моральні збитки.

Таким чином, у країні, в якій у суспільстві панує висока права культура і правосвідомість, підтримується високий правопорядок, ефективно працюють правоохоронні органи, здійснювати протиправні посягання на право власності стає недоцільним.

На жаль, у жодній з існуючих на сьогодні країн досягти зазначеного ідеального стану, коли захист права власності здійснюється виключно за допомогою правової охорони, ще не вдалось. Тому суб'єкти публічного управління та суб'єкти господарювання для захисту права власності використовують організаційно-правовий захист, який здійснюється шляхом постійного чи періодичного нагляду за кількісними і якісними властивостями майна, що знаходиться під охороною.

У цьому випадку порядок збереження майна встановлюється, як правило, за допомогою технічних норм, порядку охорони нормами цивільного права, а у випадку безпосереднього протиправного посягання та після нього – до моменту відновлення порушеного права власності – вступають у дію захисні норми адміністративного та кримінального права. Також до організаційного захисту в цілому можна, на наш погляд, віднести управлінську діяльність правоохоронних органів та судової системи України з метою відновлення порушеного права власності.

За суб'єктами забезпечення адміністративно-правовий захист може здійснюватись суб'єктами публічного управління, адміністративними судами та власниками майна (особами, які здійснюють ним управління) в процесі самоохорони.

Провідна роль у системі адміністративно-правового захисту права власності суб'єктів господарювання належить суб'єктам публічного адміністрування, які здійснюють його в процесі владно-розпорядчої діяльності відповідно до своєї визначеної нормативними актами компетенції. До них відноситься широкий перелік органів виконавчої влади, органи місцевого самоврядування, деякі громадські організації при здійсненні делегованих державних функцій у сфері охорони права власності суб'єктів господарювання, посадові і службові особи зазначених суб'єктів.

Серед них особливе місце для забезпечення прав і законних інтересів власників господарського майна та інших осіб від їх майна підвищеної небезпеки займають органи виконавчої влади, їх посадові та службові особи. По-перше, вони є основними функціонально-галузевими носіями виконавчої влади в державі, а статус органу виконавчої закріплюється за ними в нормативному порядку; по-друге, вони є найважливішою складовою органів державного управління і державного апарату в цілому; по-третє, вони об'єднані єдиним керівництвом і підпорядкуванням, внаслідок чого діють узгоджено і цілеспрямовано; по-четверте, кожен з органів цієї системи наділений державною специфічною компетенцією у сфері державного управління і реалізації державної виконавчої влади; по-п'яте, система органів виконавчої влади справляє регулюючий вплив на всі сфери державного й суспільного

життя; по-шосте, в рамках своєї компетенції органи виконавчої влади самостійні в організаційному та функціональному відношеннях; по-сьоме, здійснюється специфічний вид державної діяльності, яка за своїм юридичним змістом є виконавчо-розпорядчою.

Відповідно до ст. 140 Конституції України місцеве самоврядування є правом територіальної громади – жителів села чи добровільного об'єднання у сільську громаду жителів кількох сіл, селища та міста – самостійно вирішувати питання місцевого значення в межах Конституції і законів України [77]. Сутність місцевого самоврядування полягає в гарантованому державою праві територіальної громади, громадян та їх органів розв'язувати значну частину місцевих справ та управляти ними, діючи в межах закону, під свою відповідальність і в інтересах населення. Відносини суб'єктів господарювання з органами місцевого самоврядування регулюються ст. 23 Господарського кодексу України, згідно з якою органи місцевого самоврядування здійснюють свої повноваження виключно в межах, визначених Конституцією України, Законом України «Про місцеве самоврядування» від 21 травня 1997 р., іншими законами, що передбачають особливості здійснення місцевого самоврядування.

При цьому важливо зазначити, що правові акти органів та посадових осіб місцевого самоврядування, прийняті в межах їх повноважень, є обов'язковими для виконання всіма учасниками господарських відносин, які розташовані або здійснюють свою діяльність на відповідній території. Так, наприклад, відповідно до ст. 5 Закону України «Про державну реєстрацію юридичних осіб та фізичних осіб – підприємців» від 15 травня 2003 р. державна реєстрація юридичних осіб та фізичних осіб – підприємців – проводиться державним реєстратором виключно у виконавчому комітеті міської ради міста обласного значення або у районній, районній у містах Києві та Севастополі державній адміністрації за місцезнаходженням юридичної особи або за місцем проживання фізичної особи – підприємця.

Чільне місце в системі суб'єктів публічного управління, які здійснюють захист, належить об'єднанням громадян. Відповідно до ч. 1 ст. 36 Конституції України громадяни України для здійснення і захисту своїх прав і свобод, а також для

задоволення політичних, економічних, культурних та інших інтересів мають право об'єднуватись в політичні партії та громадські організації [77]. Наприклад, значний внесок у розвиток заходів щодо захисту права власності роблять різноманітні асоціації професійних охоронних структур України.

Важливе місце у системі органів, які здійснюють адміністративно-правовий захист права власності суб'єктів господарювання, належить адміністративним судам, у випадку коли порушником таких права є суб'єкт владних повноважень. У цьому випадку підприємець має можливість подати в адміністративний суд адміністративний позов про поновлення порушеного права власності. В свою чергу захист права власності суб'єктів господарювання, що забезпечується в господарських судах, на наш погляд, має для адміністративного права допоміжний характер, бо у господарських судах переважно вирішуються спори, що відносяться до цивільно-правової складової господарського права.

Залежно від галузі адміністративно-правового регулювання економіки адміністративно-правовий захист права власності суб'єктів господарювання забезпечується в промисловості, агропромисловому комплексі, у сфері фінансів та послуг, транспорту і зв'язку тощо. Всі зазначені галузі і сфери економіки є такими, що поділяються на підгалузі, сектори, об'єднання, групи підприємств. При цьому для вироблення теорії та практичних рекомендацій щодо забезпечення надійного захисту права власності на цих об'єктах є потреба здійснення їх специфікації. В цьому випадку діє правило: чим більш ґрунтовно досліджені специфічні умови на об'єкті, що підлягає захисту, тим більшою є можливість запропонувати ефективну та економічну схему його адміністративно-правового захисту.

За суб'єктами посягання адміністративно-правовий захист здійснюється від протиправних діянь (бездіяльності) суб'єктів владних повноважень та інших осіб. Останні в свою чергу за ступенем протиправного заволодіння чужим майном доцільно класифікувати на : осіб, які здійснюють протиправне посягання на чужу власність з метою незаконного заволодіння нею, коли правопорушення має незакінчений склад; осіб, які незаконно заволоділи чужим майном суб'єктів господарювання (віндикаційний правопорушник); та осіб, які протиправно

перешкоджають суб'єкту господарювання користуватись і розпоряджатись своєю власністю (негаторний правопорушник) без формального вилучення чужої власності у суб'єкта господарювання.

Таким чином, сформовані вище напрямки адміністративно-правового захисту права власності суб'єктів господарювання створюють основу та потребують подальшого розкриття і деталізації з метою вироблення демократичної та ефективної теорії адміністративно-правового захисту.

Отже, наведене поняття та сформовані види адміністративно-правового захисту права власності суб'єктів господарювання дозволяють перейти до дослідження питання, за допомогою якого адміністративно-правового механізму він здійснюється. Іншими словами – до висвітлення особливостей засобів адміністративно-правового захисту права власності суб'єктів господарювання.

ВИСНОВКИ

Узагальнивши зазначені праці, можна підсумувати, що: по-перше, достатньо стрімкий розвиток наукових досліджень в сфері забезпечення інформаційної безпеки у 90-х роках минулого століття змінився науковою байдужістю до цього питання, адже жодних концептуальних документів по інформаційній безпеці досі не прийнято; по-друге, аналіз наукових праць з питання інформаційної безпеки показує, що в цілому дана проблема досліджена неповно. Більшість наукових розробок представлена у вигляді лекцій, практичних посібників, монографій тощо. Це обумовлено такими причинами:

- інформаційна безпека згадується в сотнях нормативних актів, безпосередньо її захисту вже 15 років присвячуються десятки документів, серед яких Доктрина інформації безпеки, укази президентів, декілька рішень РНБО, міжнародні документи про співробітництво. Але в жодному з них немає визначення цього поняття, і що, власне, захищається, можна намагатися зрозуміти з переліку численних загроз та заходів щодо їх подолання.
- актуальним залишається встановлення сутнісних характеристик інформаційної безпеки шляхом дослідження підходів до визначення цього поняття.
- при дослідженні питання інформаційної безпеки спостерігається однобічність та поверховість (зокрема, взагалі не досліджувалась змістовна складова, яка виражається в захисті суспільства від поширення недостовірної або маніпулятивної інформації).
- тривалий час безпека інформації залишалася закритою, що не дозволяло повною мірою вивчати питання інформаційної безпеки як всередині, так і ззовні неї. Такий стан призвів до того, що наукові дослідження та обґрунтування здійснювалися обмеженим колом вчених, що призвело до однобічності і суб'єктивізму сформованих наукових положень та висновків;
- інформація, що міститься в установчих документах суб'єктів господарювання та режими щодо її використання

потребують вдосконалення законодавства щодо правового регулювання окремих видів інформації. Ми бачимо, що сьогодні у зв'язку із постійним зростанням ролі правової інформації взагалі та інформації з обмеженим доступом зокрема, ускладненням інформаційно-правових відносин, розвитком інформаційно-комунікаційних систем існує об'єктивна необхідність подальшого вдосконалення матеріальних та процесуальних норм щодо доступу до цієї інформації. Усунення неузгодженості, пов'язаної з цими визначеннями, дасть можливість підняти рівень законодавства України до вимог сьогодення у більшій мірі підвищити рівень захищеності від незаконного розповсюдження та використання зазначених видів інформації;

- у правовому регулюванні забезпечення інформаційної безпеки в Україні існує низка організаційних, нормативних, процесуальних проблем, які потребують комплексного опрацювання. Одним із найбільш оптимальних шляхів її вирішення є систематизація та кодифікація інформаційного законодавства.

Проведене дослідження не вичерпує всіх аспектів глибинної проблеми правових основ забезпечення інформаційної безпеки в Україні і є запрошенням до подальшої наукової дискусії щодо розвитку правової науки в умовах формування інформаційного суспільства та глобального інформаційного простору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Зустріч Петра Порошенка з членами Національної Ради з питань телебачення та радіомовлення [Електронний ресурс] / Режим доступу: http://www.president.gov.ua/news/prezident-zustrivsya.
2. Нижник Н.Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) [Текст] : навчальний посібник / Н.Р. Нижник, Г.П. Ситник, В.Т. Білоус. – Ірпінь : Акад. ДПС України, 2000. – 304 с.
3. Ситник Г. П. Національна безпека України: теорія і практика [Текст] : навчальний посібник / Г.П. Ситник, В.М. Олуйко, М.П. Вавринчук. – Київ : Кондор, 2007. – 616 с.
4. Данільян О.Г. Національна безпека України: сутність, структура та напрямки реалізації [Текст] : навчальний посібник / О.Г. Данільян [та ін.]. – Х. : Фоліо, 2002. – 285 с.
5. Про основи національної безпеки України: Закон України від 19 червня 2003 р. № 964– IV // ВВРУ. – 2003. – №39. – Ст. 352.
6. Потреба часу – створення Інформаційного кодексу України [Електронний ресурс] / Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=70301&cat_id=64654.
7. Ліпкан В.А. Теоретичні основи та елементи національної безпеки України [Текст] / В. А. Ліпкан ; Національна академія внутрішніх справ України. – К. : Текст, 2003. – 599 с.
8. Фисун Ю.А. Материалы конференции «Проблемы внутренней безопасности России в XXI веке». – М. : Фонд «Отечество», 2001.
9. Захист інформаційних ресурсів в інформаційно-телекомунікаційних системах. – К., 2001.
10. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / О.Г. Додонов, В.П. Горбулін, Д.В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.
11. Панарин И.Н. Информационная безопасность / И.Н. Панарин [Електронний ресурс] / Режим доступу: http://panarin.com/info_voina/86-informacionnaya-bezopasnost.html.
12. Тер-Акопов А.А. Безопасность человека : Теоретические основы социально-правовой концепции / А.А. Тер-Акопов, Междунар. независимый экол.-политолог. ун-т (МНЭПУ). – М. : Изд-во МНЭПУ, 1998. – 196 с.

13. Литвиненко О.В. Інформаційні впливи та операції. Теоретико-аналітичні нариси: монографія / О.В. Литвиненко. – К.: НІСД, 2003. – 240 с.
14. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: Монографія. – Одеса: Юридична література, 2003. – 472 с.
15. Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство: монография / Санкт-Петербург, ун-т МВД России. – СПб.: Фонд «Университет», 2000. – 423 с.
16. Баранов О.П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України / О.П. Баранов // Вісник Національної академії державного управління при Президентові України. – 2014. – № 3. – С. 60-65.
17. Гурковський В.І. інформаційна безпека в Україні як складова національної безпеки // Зб. наук. праць УАДУ. – К.: Вид-во УАДУ. – 2002. – Вип. 2. – С. 9-18.
18. Петрик В.М. Інформаційна безпека України: поняття, сутність та загрози / В.М. Петрик, М.В. Галамба // Юридичний журнал. – 2006. – №11. – С. 49-52.
19. Словарь терминов и определений по безопасности и защите информации [Текст] / В. Ярочкин, Т. Шевцова. – М. : Ось-89, 1996. – 48 с. – (Безопасность предпринимательства).
20. Інформаційна безпека України [Текст] : глосарій / Л.С. Харченко, Н.А. Ліпкан, О.В. Логінов [и др.] ; заг. ред. Р.А. Калюжний. – К. : Текст, 2004. – 135 с.
21. Ліпкан В.А. Теоретико-методологічні засади управління у сфері національної безпеки України [Текст] / В.А. Ліпкан ; Національна академія внутрішніх справ України. – К. : [б.в.], 2005. – 350 с.
22. Оніщенко Н.М. Теоретико-методологічні засади формування та розвитку правової системи [Текст] : дис... д-ра юрид. наук: 12.00.01 / Оніщенко Наталія Миколаївна ; Інститут держави і права ім. В.М. Корецького, НАН України. – К., 2002. – 426 с.
23. Курс адміністративного права України [Текст] : підручник / Національна академія внутрішніх справ ; ред. В.В. Коваленко. – К.: Юрінком Інтер, 2012. – 808 с.
24. Алексеев С.С. Проблемы теории государства и права / С.С. Алексеев. – М.: Юрид. лит., 1987. – 448 с.
25. Алексеев С.С. Теория права / С.С. Алексеев. – 2-е изд. – М. : БЕК, 1995. – 375 с.

26. Теория государства и права: учебник для юрид. вузов и фак-ов / Под ред. С.С. Алексеева. – М. : БЕК, 1995. – 453 с.
27. Теорія держави і права [Текст] : навч. посібник / А. М. Колодій [и др.] ; Український педагогічний ун-т ім. М.П.Драгоманова. – К. : Юрінформ, 1995. – 189 с.
28. Тихомиров О. Забезпечення інформаційної безпеки: теоретико-правовий аспект / О. Тихомиров // Право України. – 2011. – № 4. – С. 252-259.
29. Кустовська О.В. Методологія системного підходу та наукових досліджень: Курс лекцій / О.В. Кустовська. – Тернопіль: Економічна думка, 2005. – 124 с.
30. Горбулін В. Актуальні проблеми системного забезпечення інформаційної безпеки України / В. Горбулін, М. Биченок, П. Копка // Форми та методи забезпечення інформаційної безпеки держави : збірник матеріалів науково-практичної конференції (м. Київ, 13 березня 2008 р.). – К. : Видавець Захаренко В.О., 2008. – 216 с.
31. Палій О.А. Національна безпека України в контексті євроатлантичної інтеграції [Текст] : дис... канд. політ. наук: 21.01.01 / Палій Олександр Андрійович ; Національний ун-т «Києво-Могилянська академія». – К., 2005. – 205 с.
32. Степко О.М. Аналіз головних складових інформаційної безпеки держави / О.М. Степко [Електронний ресурс]. – Режим доступу: jrnl.nau.edu.ua/index.php/IMV/article/download/.../3172.
33. Основи інформаційного права України [Текст] : навч. посіб. / В.С. Цимбалюк [та ін.] ; ред. М. Я. Швець [та ін.]. – К. : Знання, 2004. – 274 с.
34. Е-боротьба в інформаційних війнах та інформаційне право [Текст] / В.М. Брижко [и др.] ; Акад. прав. наук України. Н.-д. центр прав. інформатики. – К. : НДЦПІ АПрН України, 2007. – 233 с.
35. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Указ № 449/2014 про рішення РНБО від 28 квітня 2014 року.
36. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський. – К.: КНТ, 2006. – 280 с. (Серія: Національна і міжнародна безпека.
37. Стрельцов А.А. Направление совершенствования правового обеспечения информационной безопасности Российской

Федерации / А.А. Стрельцов // Информационное общество. – 1999 – № 6. – С. 15-21.
38. Курс адміністративного права України: підручник / В.К. Колпаков, О.В. Кузьменко, І.Д. Пастух, В.Д. Сущенко [та ін.] / за ред. В.В. Коваленка. – К.: Юрінком Інтер, 2012. – 815 с.
39. Про інформацію: Закон України від 2 жовтня 1992 року // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
40. Гатчин Ю.А. Теория информационной безопасности и методология защиты информации / Ю.А. Гатчин, В.В. Сухостат. – Санкт-Петербург: СПбГУ ИТМО, 2010. – 98 с.
41. Кавун С.В. Інформаційна безпека: навчальний посібник / С.В. Кавун, В.В. Носов, О.В. Манжай. – Ч.2. – Харків : Вид. ХНЕУ, 2008. – 196 с.
42. Забезпечення інформаційної безпеки цифрових програмно-керованих АТС: навчальний посібник / [Кононович В.Г., Стайкуца С.В., Тардаскіна Т.М., Шинкарчук Т.М.]; за ред. чл.-кор. В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2010. – 168 с.
43. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки / Г. Сащук [Електронний ресурс] / Режим доступу: journ.univ.kiev.ua/trk/.../satshuk_publ.php].
44. Макаренко С.И. Информационная безопасность: ученик для вузов / С.И. Макаренко. – Ставрополь: СФ МГГУ им. М.А. Шолохова, 2009. – 372 с.
45. Цимбалюк В.С. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті / В.С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Зб. наук. праць. – 2004.– Вип. 8. – С. 32.
46. Нижник Н.Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навчальний посібник [Н.Р. Нижник, Г.П. Ситник, В.Т. Білоус]; за заг. ред. П.В. Мельника, Н.Р. Нижник. – Ірпінь, 2000. – 304 с.
47. Тарасенко Р.Б. Інформаційне право: навчально-методичний посібник / МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. – Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2010. – 512 с.
48. Емельянов Г.В. Проблемы обеспечения безопасности информационного общества / Г.В. Емельянов, А.А. Стрельцов // Информационное общество. – 1999. – Вып. 2. – С. 15-17.

49. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: монографія / Б.А. Кормич. – Одеса: Юридична література, 2003. – 472 с.
50. Линник Г.М. Адміністративно-правове регулювання інформаційної безпеки України : автореф. дис.... канд. юрид. наук : 12.00.07 / Г.М. Линник / Нац. ун-т біоресурсів і природокористування України. – К., 2011. – 20 с.; Євдоченко Л.О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації : автореф. дис.... канд. наук з держ. упр. : 25.00.01 / Л.О. Євдоченко / Львів. регіон. ін-т держ. упр., Нац. акад. держ. упр. при Президентові України. – Л., 2011. – 20 с.
51. Шеломенцев В.П. Організована кіберзлочинність: до визначення поняття електронне джерело / В.П. Шеломенцев [Електронний ресурс] / Режим доступу: irbis– nbuv.gov.ua/.../ cgiirbis_64.exe?
52. Линник Г.М. Адміністративно-правове регулювання інформаційної безпеки України : автореф. дис.... канд. юрид. наук : 12.00.07 / Г.М. Линник / Нац. ун-т біоресурсів і природокористування України. – К., 2011. – 20 с.
53. Триняк В.Ю. Інформаційна безпека як соціокультурний феномен (соціально-філософський аналіз): автореф. дис... канд. філософ. наук : 09.00.03 / В.Ю. Триняк ; Дніпропетр. нац. ун-т ім. О.Гончара. – Д., 2009. –19 с.
54. Логинов О.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: Автореф. дис... канд. юрид. наук: 12.00.07 / О.В. Логінов ; Нац. акад. внутр. справ України. – К., 2005. – 20 с.
55. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності / О.Л. Морозов // Віче. – 2007. – №12.
56. Про Доктрину інформаційної безпеки України : Указ Президента України від 8 лип. 2009 р. № 514/2009 / [Електронний ресурс]. – Режим доступу: http://www. president. gov. ua/documents/9570. html.
57. Інформаційна безпека України: сутність та проблеми (матеріали «круглого столу») режим доступу http://old.niss.gov.ua/book/panorama/kr_stil.htm.
58. Фомін В.О. Сутність і співвідношення понять «інформаційна безпека», «інформаційна війна» та «інформаційна боротьба» /

В.О. Фомін, А.О. Рось [Електронний ресурс] / Режим доступу: http://www.security.ukrnet.net/search.php.
59. Косєвцов В.О. Оцінка стану воєнної безпеки України / В.О. Косєвцов, В.М.Телелим, В.І.Шевченко // Наука і оборона. – 1998. – № 2. – С. 3-6.
60. Вещицький І.В. Модель визначення джерел загроз інформаційній безпеці у воєнній сфері / І.В. Вещицький, В.О. Кацілап, П.Д. Рогов, Л.В. Бухало // Труди академии. – К., 2009. – № 89.– С. 38-45.
61. Рогов П.Д., Малахов М.А., Бухало Л.В. Методика визначення рівнів загроз інформаційній безпеці держави у воєнній сфері // Вісник військового інституту Національного університету імені Т.Г. Шевченка. – С. 143-147.
62. Бодрук О.С. Воєнно-політичні аспекти забезпечення безпеки / О.С. Бодрук // Стратегічна панорама. – 2002.– №2.– С. 65-66.
63. Морозов О. Інформаційна безпека в умовах сучасного стану і перспективи розвитку державності / О. Морозов // Віче. – 2007. – № 12.– Спецвипуск. – С. 23-25.
64. Марченко О.С. Інформаційна безпека фінансової системи: головні складові та загрози / О.С. Марченко // Збірник наукових праць Міжнародної науково-практичної Інтернет-конференції «Актуальні питання фінансової системи держави», м. Харків, 21 лютого 2014 р. – С. 34-37.
65. Шлемко В.Т. Економічна безпека України: сутність і напрямки забезпечення / В.Т. Шлемко, І.Ф. Бінько : монографія. – К. : НІСД,1997. – Серія «Національна безпека». – Вип. 2. – С. 118-120.
66. Концепція гуманітарного розвитку України на період до 2020 року (проект) [Електронний ресурс] / Режим доступу: www.kyiv– obl.gov.ua/files/.../concepciya.doc.
67. Арсентьев М.В. К вопросу о понятии «информационная безопасность» / М.В. Арсентьев // Информационное общество. – 1997. – Вып. 4-6. – С. 48-50.
68. Грушкевич Т.В. Інформаційно-правове забезпечення конституційних екологічних прав [Текст] : автореф. дис.... канд. юрид. наук : 12.00.07 / Грушкевич Тетяна Володимирівна ; Держ. податк. служба України, Нац. ун-т держ. податк. служби України. – Ірпінь, 2012. – 19 с.
69. Олійник О.В. Нормативно-правове забезпечення інформаційної безпеки України / О.В. Олійник // Право і суспільство. – 2012. – № 3. – С. 132-137.

70. Соснін О.В. Про правові основи удосконалення системи державного управління інформаційними ресурсами / О.В. Соснін, Л.Є. Шиманський // Політологічний вісник: Зб. наук праць. – №10. – К. : Т-во «Знання України», 2002. – 316 с.
71. Основи інформаційного права України [Текст] : навч. посіб. / В.С. Цимбалюк [та ін.] ; за ред. д-ра екон. наук М. Я. Швеця [та ін.]. – 2-е вид., перероб. і допов. – К. : Знання, 2009. – 414 с.
72. Віхрова В.В. Оперативно-розшукова інформація у сфері оподаткування / В.В. Віхрова // Право і безпека. – 2005. – №1. – С. 49-52.
73. Погорецький М.А. Проблеми боротьби з легалізацією доходів незаконного походження оперативно-розшуковими засобами / М.А. Погорецький // Проблеми боротьби з корупцією, організованою злочинністю та контрабандою: Міжвід. наук. зб.; гол. ред. А.І. Комарова. – К.: НДІ «Проблеми людини», 2003-2004. – Т. 29. – С. 348-350.
74. Файер Д.А. Злочинні групи, що діють у сфері економіки, як об'єкт оперативної розробки / Д.А. Файер: Зб. матеріалів Міжнародн. наук.-практ. семінару [«Фінансова злочинність»]. – Х., 2000. – С. 105-110.
75. Привалов О. Тіньова економіка і корупція в України / О. Привалов, Ю. Сапєлкін // Розбудова держави. – 1998. – № 10. – С. 22-28.
76. Декларація про державних суверенітет України: прийнята 6 липня 1990 р. – № 55-XII / ВВРУ. – 1990. – № 31. – Ст. 429.
77. Конституція України від 28 червня 1996 року // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.
78. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297 / [Електронний ресурс]. – Режим доступу : http://zakon. rada. gov. ua/cgi-bin/laws/main. cgi? nreg=2297-17.
79. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України 9 січ. 2007 р. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102. – 23 берез.
80. Про доступ до публічної інформації : Закон України від 13 січ.2011 р. № 2939. / [Електронний ресурс]. – Режим доступу : http://zakon1. rada. gov. ua/cgi-bin/laws/main. cgi? nreg=2939-17.
81. Про основи національної безпеки України: Закон України від 19 червня 2003 р. № 964-IV // ВВРУ. – 2003. – №39. – Ст. 352.

82. Ліпкан В.А. Національна і міжнародна безпека у визначеннях та поняттях [Текст] / В. А. Ліпкан, О. С. Ліпкан. – Вид. 2-ге, доп. і переробл. – К. : Текст, 2008. – 400 с.
83. Єрмоленко М.М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення : монографія / М.М. Єрмоленко. – К.: Київ. нац. торг.-екон. ун-т., 2001. – 399 с.
84. Барановський О.І. Фінансова безпека / О.І. Барановський. – К.: Фенікс, 1999. – 338 с.
85. Пастернак-Таранушенко Г.І. Економічна безпека держави / Г.І. Пастернак-Таранушенко // Розбудова держави. – 1998. – № 9-10. – С. 12-18.
86. Буряк П.Ю. Корпоративне управління: особливості розвитку в Україні / П.Ю. Буряк, Н.Б. Татарин // Фінанси України. – 2006. – №6. – С.116.
87. Кочетков Г.Б. Корпорация: американская модель / Г.Б. Кочетков, В.Б. Супян. – СПб.: Питер, 2005. – 320 с.
88. Румянцев С.А. Українська модель корпоративного управління: становлення та розвиток / Сергій Анатолійович Румянцев. – К.: Знання, 2003. – 149 с.
89. Формування та розвиток моделі корпоративного управління в трансформаційній економіці: навчальний посібник / [Круш П.В., Кавтиш О.П., Гречко А.В., Чихачьова Ю.С.; під заг. ред. П.В.Круша]. – К.: ЦУЛ, 2007. – 264 с.
90. Основи підприємницької діяльності: посібник / С.В. Мочерний, О.А. Устенко, С.І. Чеботар. – К.: Видавничий центр «Академія», 2001. – 280 с.
91. Варналій З.С. Основи підприємництва: навчальний посібник / Захарій Степанович Варналій. – К.: Знання-Прес, 2002. – 240 с.
92. Покропивний С.Ф. Підприємництво: стратегія, організація, ефективність: навчальний посібник / С.Ф. Покропивний, С.Ф. Колот. – К.: КНЕУ,1998. – 352 с.
93. Глусь Н.С. Корпорації та корпоративне право: поняття, основні ознаки та особливості захисту: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.03 «цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / Н.С. Глусь. – Київ, 2000. – 20 с.
94. Майєр К. Корпоративне управління в ринкових та перехідних економіках. У пошуках кращого директора: корпоративне управління в ринкових та перехідних економіках : [пер. з англ. С. Синиця]. – К.: Основи, 1996. – 189 с.

95. Розенберг Д.М. Бизнес и менеджмент. Терминологический словарь / Д.М. Розенберг. – М.: ИНФРА-М, 1997. – 469 с.
96. Дембе А. Корпоративне управління: віч-на-віч з парадоксами / А. Дембе, Ф. Нойбауер. – К.: Основи, 1997. – 302 с.
97. Новый экономический и юридический словарь / [Под ред. А.Н. Азрилияна]. – М.: Институт новой экономики, 2003. – 1088 с.
98. Тлумачний словник чужомовних слів в українській мові. Правопис. Граматика / [уклад. О.М. Сліпушко]. – Київ: Видавництво «Криниця»,1999. – 504 с.
99. Кравчук В.М. Корпоративне право: науково-практичний коментар законодавства та судової практики / Володимир Миколайович Кравчук. – К.: Істина, 2005. – 720 с.
100. Ожегов С.И. Словарь русского языка / Сергей Иванович Ожегов. – Москва: Русский язык, 1990. – 921 с.
101. Господарський кодекс України : чинне законодавство зі змінами та допов. – К.: Вид. ПАЛИВОДА А.В., 2005. – 180 с.
102. Політичний словник / [За ред. В.К. Врублевського]. – К.: Укр. рад. енцикл. – 1982. – 655 с.
103. Економічний словник-довідник / [За ред. С.В. Мочерного]. – К.: Феміна, 1995. – 368 с.
104. Про підприємництво: Закон України від 07.02.1991року // Відомості Верховної Ради УРСР. – 1991. – № 14. – Ст. 168.
105. Про власність: Закон України від 07.02.1991 року // Відомості Верховної Ради УРСР. – 1991. – № 20. – Ст. 249.
106. Про цінні папери і фондову біржу: Закон України від 18.06.1991 року // Відомості Верховної Ради України. – 1991. – № 38. – Ст. 508.
107. Про господарські товариства: Закон України від 19.09.1991року // Відомості Верховної Ради України. – 1991. – № 49. – Ст. 682.
108. Про приватизацію державного майна: Закон України від 04.03.1992 року // Відомості Верховної Ради України. – 1992. – № 24. – Ст. 348.
109. Про приватизацію невеликих державних підприємств (малу приватизацію): Закон України від 06.03.1992 року // Відомості Верховної Ради України. –1992. – № 24. – Ст. 350.
110. Про приватизаційні папери: Закон України від 06.03.1992 року // Відомості Верховної Ради України. – 1992. – № 24. – Ст. 352.

111. Про акціонерні товариства: Закон України від 17.09.2008 року // Відомості Верховної Ради України. – 2008. – № 50-51. – Ст. 384.
112. Нашинець-Наумова А.Ю. Правове регулювання інформаційної безпеки корпорацій / А.Ю. Нашинець-Наумова // Правова інформатика. – 2014. – №4/44. – С. 95-99.
113. Нашинец-Наумова А. Ю. К вопросу о развитии системы обеспечения информационной безопасности корпораций в Украине [Текст] / А. Ю. Нашинец-Наумова // Молодий вчений. – 2015. – №2 (17). – Частина 6. – С. 817-821.
114. Нашинець-Наумова А.Ю. Інститут неправдивої інформації в інформаційному праві / А.Ю. Нашинець-Наумова, А.В. Романська // Тенденції розвитку юридичної науки в XXI столітті : Всеукраїнська науково-практична конференція до Дня науки, 22 травня 2014 р.: тези доповіді. – К. : Комп'ютерпрес, 2014. – С. 117-120.
115. Про національну поліцію: Закон України // Відомості Верховної Ради України. – 2015. – № 40-41. – Ст. 379.
116. Про оперативно-розшукову діяльність: Закон України // Відомості Верховної Ради України. – 1992. – № 22. – Ст. 303.
117. Про боротьбу з тероризмом: Закон України // Відомості Верховної Ради України. – 2003. – № 25. – Ст. 180.
118. Про запобігання корупції: Закон України // Відомості Верховної Ради України. – 2014. – № 49. – Ст. 2056.
119. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України // Відомості Верховної Ради України. – 1993. – № 35. – Ст. 358.
120. Про очищення влади : Закон України // Відомості Верховної Ради України. – 2014. – № 44. – Ст. 2041.
121. Про затвердження Положення про Міністерство внутрішніх справ України: Постанова Кабінету Міністрів України від 28 жовтня 2015. – № 878.
122. Про Службу безпеки України : Закон України // Відомості Верховної Ради України. – 1992. – № 27. – Ст. 382.
123. Про прокуратуру: Закон України // Відомості Верховної Ради України. – 1991. – № 53. – Ст. 1697-VII.
124. Про Раду національної безпеки і оборони України: Закон України // Відомості Верховної Ради України. – 1998. – № 35. – Ст. 237.
125. Нашинець-Наумова А.Ю. Реалізація адміністративно-правових форм у сфері забезпечення інформаційної безпеки

корпорацій / А.Ю. Нашинець-Наумова // Підприємництво, господарство і право. – 2015. – № 8. – С. 46-48.
126. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.
127. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України 15 травня 2013 р. – № 386-р.
128. Положення про розкриття інформації емітентами цінних паперів: Рішення Національної комісії з цінних паперів та фондового ринку від 03.12.2013. – № 2826.
129. Про затвердження Змін до Положення про порядок складання та розкриття інформації компаніями з управління активами та особами, що здійснюють управління активами недержавних пенсійних фондів, та подання відповідних документів : Рішення Національної комісії з цінних паперів та фондового ринку №1249.
130. Про схвалення Концептуальних засад функціонування загальнодоступної інформаційної бази даних Національної комісії з цінних паперів та фондового ринку про ринок цінних паперів : Рішення Національної комісії з цінних паперів та фондового ринку від 25.12.2012. – № 1857.
131. Про затвердження Положення про формування інформаційної бази даних про ринок цінних паперів : Рішення Національної комісії з цінних паперів та фондового ринку від 03.06.2014. – № 733.
132. Нашинець-Наумова А.Ю. Адміністративно-правові методи забезпечення інформаційної безпеки корпорацій / А.Ю. Нашинець-Наумова // Підприємництво, господарство і право. – 2015. – № 10. – С.16-20.
133. Нашинець-Наумова А.Ю. Організаційно-правові методи забезпечення інформаційної безпеки корпорацій / А.Ю. Нашинець-Наумова // Підприємництво, господарство і право. – 2015. – № 11. – С.21-24.
134. Кормич Б.А. Інформаційна безпека: організаційно-правові основи [Текст] : навч. посібник для студ. вищих навч. закл. / Б.А. Кормич. – К. : Кондор, 2004. – 384 с. – (Юридична книга).
135. Зубок М.І. Інформаційна безпека [Текст] : навч. посібник / М.І. Зубок; Київський національний торговельно-економічний ун-т. – К. : КНТЕУ, 2005. – 133 с.

136. Бєгун А.В. Інформаційна безпека [Текст] : навч. посібник / А.В. Бєгун; Державний вищий навчальний заклад «Київський національний економічний ун-т ім. Вадима Гетьмана». – К. : КНЕУ, 2008. – 280 с.
137. Кавун С.В.Інформаційна безпека [Текст] : навчальний посібник / С.В. Кавун [и др.]. – Х. : Харківський національний економічний ун-т, 2008. – Ч. 2. – Х. : [б.в.], 2008. – 196 с.
138. Триняк В.Ю. Інформаційна безпека як соціокультурний феномен (соціально-філософський аналіз) [Текст] : дис.... канд. філос. наук : 09.00.03 / Триняк Віталій Юрійович ; Харк. ун-т повітр. сил ім. І. Кожедуба. – Д., 2009. – 189 с.
139. Гончарук С.Т. Основи адміністративного права: навчальний посібник/ Степан Тихонович Гончарук. – К.: ТОВ «Видавничий будинок «Аванпост-Прим», 2004. – 200 с.
140. Діхтієвський П.В. Адміністративно-правовий примус у механізмі забезпечення особистої безпеки: дисер. на здобуття наук. ступеня д-ра. юрид. наук: спец. 12.00.14 / П.В. Діхтієвський. – Москва, 2004. – 428 с.
141. Логінов О.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади [Текст] : дис... канд. юрид. наук: 12.00.07 / Логінов Олександр Володимирович ; Національна академія внутрішніх справ України. – К., 2005. – 236 с.
142. Коломоєць Т.О. Адміністративний примус у публічному праві України: теорія, досвід та практика реалізації: дисер. на здобуття наук. ступеня док. юрид. наук: спец. 12.00.07 «адміністративне право і процес; фінансове право; інформаційне право / Т.О. Коломоєць. – Харків, 2005. – 455 с.
143. Гладун З.С. Адміністративне право України: навчальний посібник / Зіновій Степанович Гладун. – Тернопіль: Карт-бланш, 2004. – 579 с.
144. Голосніченко І.П. Адміністративне право України (основні категорії і поняття) / Іван Пантелійович Голосніченко. – К.: МАУП, 1998. – 52 с.
145. Мазурин С. Административное право / С. Мазурин, Л. Попов, Ю. Козлов. – СПб: Питер, 2004. – 252 с.
146. Мосьондз С.О. Адміністративне право України (у визначеннях та схемах): навчальний посібник / Сергій Олександрович Мосьондз. – К.: Атіка, 2008. – 272 с.
147. Адміністративне право України. Академічний курс: підручник: у двох томах / [Битяк Ю.П., Колпаков В.К., Лук'янець Д.М. та ін.;

ред. колегія: В.Б. Авер'янов (голова)]. – К.: Видавництво «Юридична думка», 2004. – Т.1. Загальна частина. – 2004. – 584 с.
148. Колпаков В.К. Адміністративне право України: підручник / В.К. Колпаков, О.В. Кузьменко. – К.: Юрінком Інтер, 2003. – 537 с.
149. Адміністративне право України: підручник / [Битяк Ю.П., Гаращук В.М., Дьяченко О.В. та ін.]; за ред. Ю.П. Битяка. – К.: Юріном Інтер,2006. – 544 с.
150. Бахрах Д.Н. Административное право России: учебник / Демьян Николаевич Бахрах. – М.: Издательство НОРМА, 2000. – 640 с.
151. Нашинець-Наумова А.Ю. Особливості застосування адміністративних методів забезпечення інформаційної безпеки корпорацій / А.Ю. Нашинець-Наумова // Информационные технологии и безопасность: материалы XV международной научно-практической конференции ИТБ-2015 (г. Киев, 21 октября 2015 г.). – К.: ИПРИ НАН Украины, 2015. – С. 163-166.
152. Щербина В.С. Господарське право України: навчальний посібник. – 2-ге вид., перероб. і доп. – К.:Юрінком Інтер 2001. – 384 с.
153. Хозяйственное право: Учебное пособие / Под общ. ред., проф. Н.А. Саниахметовой. – Х.: Одисей, 2004. – 640 с.
154. Хозяйственное право: Учебник / Под ред. В.К. Мамутова. – К.: Юринком Интер, 2002. – 912 с.
155. Науково-практичний коментар Господарського кодексу України / за заг. ред. В.К. Мамутова. – К.: Юрінком Інтер, 2004. – 688 с.
156. Шершневич Г.Ф. Курс торгового права. – М.: Норма-Инфра, 2003. – Т. 1. – 482 с.
157. Грось Л.А. Участие публично-правовых образований в отношениях собственности: гражданско-правовые проблемы // Хозяйство и право. – 2001. – С. 33-37.
158. Про впорядкування діяльності суб'єктів підприємницької діяльності, створених за участю державних підприємств: Декрет Кабінету Міністрів України від 31.12.1992 (редакція від 01.01.2004).
159. Степанов Д. Срок действия учредительного договора // Журнал для акционеров. – 1999. – №9(89). – С. 29-32.
160. Перетерский И.С. Сделки, договоры. – М.: Наука, 1982. – 216 с.
161. Мейер Д.И. Русское гражданское право (В 2-х ч.-Ч. 1). – М.: Статут, 1997. – 672 с.

162. Марченко М.Н. Теория государства и права: Учебник. – 2-е изд., перераб. и доп. – М.: Статус, 2004. – 802 с.
163. Про затвердження Статуту Академії правових наук України: Постанова КМУ від 02.02.2000 р. № 210 // Офіційний вісник України. – 2000. – №5. – Ст. 177.
164. Гражданское и торговое право капиталистических государств / Отв. ред. Е.А. Васильев. – М.: Юрид.лит., 1993. – 680 с.
165. Мицкевич А.В. Позитивное право: система и категория // Проблемы общей теории права и государства / Под ред. В.С. Нерсесянца. – М., 2008.
166. Елисеев И.В. Юридические лица. Гражданское право: Учебник / Под ред. А.П. Сергеева, Ю.К. Толстого. – М.: Юрист, 2002. – Т. 1. – 456 с.
167. Степанов Д.И. Правовая природа устава юридического лица // Хозяйство и право. – 2000. – №7. – С.41-50.
168. Бондарчук Ю.В. Безпека бізнесу:організаційно-правові основи / Ю.В. Бондарчук, А.І. Марущак : наук.-практ. посібник. – К.: Вид.дім «Скіф», КНТ, 2008. – 372 с.
169. Марущак А.І. Зміст поняття «забезпечення доступу до інформації» / А.І. Марущак // Право України. – 2008. – № 5. – С. 99-104.
170. Лопатин В.Н. Правовая охрана и защита служебной тайны / В.Н. Лопатин // Государство и право. – 2000. – № 6. – С. 85-91.
171. Доступ до інформації та електронне урядування/ Автори-упорядники М.С. Демкова, М.В. Фігель. – К.: Факт, 2004. – 336 с.
172. Кулініч О.О. Інформація з обмеженим доступом як об'єкт цивільних прав / О.О. Кулініч: : дис... к. юрид. наук. – Одеса, 2006. – 200 с.
173. Марущак А.І. Проблеми правомірності доступу громадян до інформації / А.І. Марущак // Судова апеляція. – 2007. – № 2(7). – С. 12-19.
174. Ткачук Т.Ю. Інформація з обмеженим доступом на підприємстві: проблеми безпеки та захисту / Т.Ю. Ткачук // Право України. – 2011. – № 3. – С. 243-251.
175. Городов О.А. Основы информационного права России: Учеб.пособие. – Спб., 2003. – 305 с.
176. Пилипенко Ю.С. Общие теоретические аспекты института тайны / Ю.С. Пилипенко // Государство и право. – 2009. – № 7. – С. 19-24.
177. Радутний О.Е. Кримінальна відповідальність за незаконне збирання, використання та розповсюдження відомостей, що

становлять комерційну або банківську таємницю: Монографія. – Х.: Ксілон, 2008. – 202 с.
178. Нашинець-Наумова А.Ю. Проблеми правового регулювання доступу до конфіденційної інформації на підприємстві / А.Ю. Нашинець-Наумова // Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»: зб. наук. праць. – 2012. – №4 (25). – С. 119-124.
179. Нашинец-Наумова А.Ю. Правовые аспекты формирования парадигмы конфиденциальной информации в акционерном обществе / А.Ю. Нашинец-Наумова // Legea şi viaţa: Revistă ştiinţifico-practică. – 2014. – № 5/3 (269). – С. 41-45.
180. Андрощук Г. захист комерційної таємниці:економічно-правовий аспект / Г. Андрощук // Інтелектуальна власність. – 1999. – № 9. – С. 8-12.
181. Сергеева О. Коммерческая тайна / О. Сергеева // Юридическая практика. – 2000. – № 46. – С. 8-10.
182. Коммерческая тайна: правовые проблемы / В.А. Плаксин, Ю.В. Макогон // Государство и право. – 1992. – № 8. – С. 73-80.
183. Сергєєва О. Питання про співвідношення ноу-хау та комерційної таємниці в праві України / О. Сергєєва // Право України. – 2000. – № 11. – С. 85-87.
184. Господарський кодекс України // Відомості Верховної Ради України (ВВР). – 2003. – № 18, №19-20, 21-22. – Ст. 144.
185. Цивільний кодекс України // Відомості Верховної Ради України (ВВР). – 2003. – № 40– 44.– Ст. 356.
186. Про перелік відомостей, що не становлять комерційної таємниці Постанова Кабінету Міністрів України від 09.08.93 р. № 611.
187. Нашинець-Наумова А.Ю. Правове забезпечення формування системи інформаційної безпеки в акціонерному товаристві / А.Ю. Нашинець-Наумова // Підприємництво, господарство і право. – 2014. – № 5. – С. 68-72.
188. Музиченко Г.Г. Формування та розвиток світового ринку цінних паперів в умовах економічної глобалізації: Дис... канд. екон. наук: 08.05.01 / Г.Г. Музиченко ; Донец. нац. ун-т. – Донецьк, 2006. – 242 с.
189. Словник фінансово-правових термінів / [за заг. ред. д.ю.н., проф. Л.К. Воронової]. – 2-ге вид., переробл. і доповн. – К.: Алерта, 2011. – 558 с.

190. Саєнко В.В. Правове регулювання використання інсайдерської інформації на ринку цінних паперів: Автореферат дис… канд. юрид. наук : 12.00.04 / КНУ імені Тараса Шевченка. – К., 2002. – 20 с.
191. Кошкаров О.О. Кримінально-правова характеристика злочинів у сфері випуску та обігу цінних паперів: Дис... канд. юрид. наук: 12.00.08 / О.О. Кошкаров ; ХНУВС. – Х., 2006. – 219 с.
192. Нашинець-Наумова А.Ю. Поняття та ознаки інсайдерської інформації як особливого виду інформації з обмеженим доступом / А.Ю. Нашинець-Наумова // Підприємництво, господарство і право. – 2016. – № 4. – С. 73-76.
193. Нашинец-Наумова А.Ю. Инсайдерская информация как специальный субъект обеспечения информационной безопасности предприятий / А.Ю. Нашинец-Наумова // Legea şi viaţa: Revistă ştiinţifico-practică. – 2016. – № 6/2. – С. 77-81.
194. Венедиктов А. В. Государственная социалистическая собственность. – 834 с.
195. Рахлин З.М. Хозяйственные договоры [Текст] : Учеб.-метод. пособие по спецкурсу «Хоз. право» / Проф. З.М. Рахлин ; М-во высш. и сред. спец. образования УССР. Одес. ин-т нар. хоз-ва. – Одесса : [б. и.], 1970. – 79 с.
196. Резвых В.Д. Административная ответственность за хозяйственные правонарушения [Текст] : учебное пособие / В. Д. Резвых ; Министерство внутренних дел [МВД] СССР. Горьковская высшая школа. – Горький : Горьковская высшая школа МВД СССР, 1976. – 135 с.
197. Галунько В.В. Людина і держава : монографія / Валентин Васильович Галунько, Володимир Іванович Милько. – К. : Університет «Україна», 2014. – 158 с.
198. Полетаев Ю.Н. Материально ответственные лица / Ю.Н. Полетаев. – Изд-во «Городец», 2006.
199. Нікітенко О. І. Внутрішня безпека як стан захищеності життєво важливих інтересів особи, суспільства і держави / О.І. Нікітенко // Актуальні проблеми права: теорія і практика. – 2013. – № 26. – С. 109-115.
200. Ковалів М.В. Правові та організаційні засади забезпечення збереження вантажів на залізничному транспорті України [Текст] / М.В. Ковалів ; Львівський ін-т внутрішніх справ при Національній академії внутрішніх справ України. – Л. : Афіша, 2003. – 198 с.

201. Кравцова Т.М. Адміністративно-правові засади здійснення державної регуляторної політики в сфері господарювання [Текст] : дис... д-ра юрид. наук: 12.00.07 / Кравцова Тетяна Миколаївна ; Національний ун-т внутрішніх справ. – Х., 2004. – 460 с.
202. Шишка Р.Б. Договорные отношения вузов в области научно-технического прогресса [Текст] : дис.... канд. юрид. наук / Р.Б. Шишка. – Х. : Б. и., 1985. – 157 с.
203. Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу : Закон України від 18 вересня 2004 р. // ВВРУ. – 2004. – №29. – Ст. 367.
204. Хатуаев В.У. Административно-правовая система обеспечения имущественной безопасности / В.У. Хатуаев. – Воронеж: Воронежский государственный университет, 2004.
205. Теорія держави і права [Текст] : посіб. для підгот. до іспитів / М.М. Пендюра ; Київський національний ун-т внутрішніх справ. – К. : ТЕКСТ, 2008. – 188 с.

Наукове видання

Анфіса Юріївна Нашинець-Наумова

ІНФОРМАЦІЙНА БЕЗПЕКА: ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ

МОНОГРАФІЯ

Українською мовою

Верстка – Н.М. Ковальчук

Підписано до друку 14.11.2016. Формат 60х84/16.
Папір офсетний. Гарнітура Cambria. Цифровий друк.
Умовно-друк. арк. 9,77. Тираж 300. Замовлення № 1216м-328.
Ціна договірна. Віддруковано з готового оригінал-макета.

Видавництво і друкарня – Видавничий дім «Гельветика»
73034, м. Херсон, вул. Паровозна, 46-а, офіс 105.
Телефон +38 (0552) 39 95 80
E-mail: mailbox@helvetica.com.ua
Свідоцтво суб'єкта видавничої справи
ДК № 4392 від 20.08.2012 р.