5. Про затвердження Положення про Міністерство фінансів України : Постанова Кабінету Міністрів України; від 20.08.2014 № 375.

6. Про Антимонопольний комітет України / Закон України від 26.11.1993 № 3659-XII.

7. Державна служба як суб'єкт економічних відносин. Державна служба. 2003. URL: http://library.if.ua/book/112/7590.html.

8. Зозуля І.В., Шулатова І.С. Особливості Державної фіскальної служби України як суб'єкта державного управління. *Право і Безпека*. 2015. № 2. С. 59–66.

9. Болдін М.Я. Адміністративно-правові засади діяльності Національного банку України у сфері рефінансування банків. Дисертація кандидата юридичних наук: 12.00.07. Київський міжнародний університет, Науково-дослідний інститут публічного права. Київ, 2017. 207 с.

10. Барановський О.І. Філософія безпеки : монографія. Київ : Київ. нац. торг.-екон. ун-т, 2014. 715 с.

11. Про Національний банк України / Закон України від 20.05.1999 № 679-XIV.

12. Погореленко Н.П. Роль Національного банку України у забезпеченні стабільного розвитку банківської системи. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія : Економічна.* 2017. Вип. 93. С. 57–76.

УДК 342.9
DOI https://doi.org/10.32844/2618-1258.2020.1.26

ДІОРДІЦА І.В.

ЗМІСТ ПРАВОВІДНОСИН У СФЕРІ КІБЕРБЕЗПЕКИ: ПРОБЛЕМИ ТЕОРІЇ ТА ПРАКТИКИ

У статті пропонуються до розгляду авторські результати визначення концептуальних положень змісту правовідносин у сфері кібербезпеки. Розглянуто трактування змісту правовідносин у сфері кібербезпеки як елементу таких правовідносин. Проаналізовано теоретичні та практичні аспекти змісту правовідносин у сфері кібербезпеки. Визначено, що зміст правовідносин у сфері кібербезпеки складає конкретна поведінка суб'єктів правовідносин у сфері кібербезпеки та її юридичне закріплення нормами права у вигляді суб'єктивних прав та юридичних обов'язків. Запропоновано власне бачення компонентів структури змісту правовідносин у сфері кібербезпеки: юридичний – суб'єктивне право та юридичний обов'язок, законний інтерес; фактичний – реальна поведінка суб'єктів. Встановлено зміст поняття «законний інтерес» – усвідомлена суб'єктом правовідносин у сфері кібербезпеки необхідність задоволення своїх потреб способом, що допускається, але прямо не гарантується чинним інформаційним законодавством. З урахуванням положень загальної теорії права, а також робіт з безпекової тематики виокремлено загальні (матеріальні) і спеціальні (юридичні) передумови виникнення правовідносин у сфері кібербезпеки. У рамках узагальнення теоретичних та практичних аспектів функцій правовідносин визначено такі риси правовідносин у сфері кібербезпеки: 1) встановлюють конкретно визначене коло осіб – суб'єктів правовідносин у сфері кібербезпеки, на яких поширюється дія норм права в конкретному просторово-часовому форматі; 2) закріплюють конкретну поведінку, якої повинні або можуть дотримуватися суб'єкти правовідносин у сфері кібербезпеки; 3) слугують умовою для можливого приведення в дію спеціальних юридичних засобів (суб'єктами забезпечення кібербезпеки) з метою забезпечення суб'єктивних прав, обов'язків, відповідальності. Висновується, що правовідносини у сфері кібербезпеки можуть

© ДІОРДІЦА І.В. – доктор юридичних наук, доцент, професор кафедри приватного та публічного права (Київський національний університет технологій та дизайну)

служити засобом переведення загальних розпоряджень юридичних норм у площину суб'єктивних прав і обов'язків як для суб'єктів забезпечення кібербезпеки, так і для суб'єктів правовідносин у цій сфері загалом.

Ключові слова: *кібербезпека, кіберпростір, правовідносини, суб'єктивне право, юридичний обов'язок.*

The article presents the author's results of determining the conceptual provisions of the content of legal relationships in cybersecurity. The interpretation of the content of legal relationships in the field of cybersecurity as an element of such legal relationships is considered. Theoretical and practical aspects of the content of legal relationships in the field of cybersecurity are analyzed. It is determined that the content of cybersecurity relationships is determined by the specific behavior of the cybersecurity entities and their legal fixing with the rules of law in the form of subjective rights and legal obligations. We propose our own vision of the components of the content structure of the legal relationship in the field of cybersecurity: legal – subjective law and legal obligation, legitimate interest; factual – the real behavior of the subjects. The content of the concept of "legitimate interest" has been defined – the subject of the cyber security legal subject is aware of the need to satisfy his needs in a way that is allowed, but is not directly guaranteed by the current information legislation. Taking into account the provisions of the general theory of law, as well as the works on security topics, the general (material) and special (legal) prerequisites for the emergence of legal relationships in the field of cybersecurity are distinguished. Within the framework of generalization of theoretical and practical aspects of legal relations functions, the following features of legal relations in the sphere of cybersecurity are defined: 1) identify a specific circle of persons (subjects of legal relations in the field of cybersecurity) who are subject to the rules of law in a specific space-time format; 2) enshrine specific behaviors that cybersecurity subjects must or can observe; 3) serve as a condition for possible enforcement of special legal remedies of cybersecurity entities for the purpose of securing subjective rights, obligations, responsibilities. It is concluded that legal relationships in the field of cybersecurity can serve as a means of translating the general provisions of legal norms into the sphere of subjective rights and obligations for both the subjects of cybersecurity and legal entities in the field in general.

Key words: *cybersecurity, cyberspace, legal relationships, subjective right, legal obligation.*

Вступ. Інтеграція України до світового кіберпростору призвела до утворення перманентних джерел загроз національним інтересам, пов'язаних із функціонуванням комп'ютерних мереж та систем. Це зумовлює необхідність у концептуальному переосмисленні нової кібербезпекової реальності, впорядкуванні інформаційного законодавства відповідно до сучасних тенденцій розвитку не лише інформаційних відносин, а й кібернетичних відносин з урахуванням необхідності створення правових умов для реалізації національних інтересів у цій сфері, передусім розбудови систем ефективного нормативно-правового регулювання.

Дослідження кібербезпеки загалом є доволі новим явищем, тому акцентуємо увагу на необхідності та перспективності проведення ґрунтовного дослідження не лише формування національної системи кібербезпеки, а й структурних елементів правовідносин у сфері кібербезпеки.

Одним із структурних елементів правовідносин у сфері кібербезпеки виступає *зміст правовідносин* – органічно об'єднана цілями кібербезпекової політики сукупність прав та обов'язків суб'єктів національної системи кібербезпеки. Зміст кібербезпеки містить ті суспільні відносини, які виникають під час реалізації правових і технічних норм, що спрямовані на забезпечення кібербезпеки відповідних об'єктів, а також включають проведення проактивних заходів у рамках реалізації кібербезпекової політики.

Постановка завдання. Метою статті є здійснення правового аналізу теоретичних та практичних аспектів змісту правовідносин у сфері кібербезпеки.

Результати дослідження. Зауважимо, що якщо правники більшою мірою звертають увагу на надлишкову зарегульованість і втручання держави в правовідносини, то стосовно сфери кібербезпеки ситуація кардинально протилежна – у цій сфері держава має найменший вплив на

регулювання суспільних відносин, а отже, поряд із уявною свободою дій формуються чіткі умови для сталих системних порушень прав і свобод українських громадян, інтересів української нації та Української держави в кіберпросторі. Наразі постає нагальна потреба у формуванні такої правової бази, яка за умови врахування базових стандартів прав людини в кіберпросторі створила б умови для реалізації державної кібербезпекової політики, в рамках якої, окрім посилення ролі держави в кіберпросторі, потрібно розробити чіткі механізми правового регулювання діяльності громадян у кіберпросторі з метою можливостей держави вимагати від суб'єктів правовідносин у сфері кібербезпеки правомірної поведінки, яка відповідала б встановленим нормам права [1], *що загалом і корелюється з актуальністю цього дослідження.*

Таким чином, формалізовані вимоги з виконання інформаційно-правових норм знаходитимуть свій вияв у системі обов'язків, що встановлюють міри відповідальності за невиконання приписів. Адже здебільшого, коли робляться ті чи інші намагання держави сформулювати бодай якісь конкретні рамки та межі відповідальності для громадян, в тому числі журналістів, це одразу ж знаходить свій вияв у зловживанні ЗМІ власними правами з метою дискредитації законних приписів і нав'язуванні в масовій свідомості патерну про те, що будь-яке правове регулювання у кіберпросторі є кроком до авторитаризму або тоталітаризму. Натомість, порушуючи питання про нехіть до виконання обов'язків і встановлення меж відповідальності, я не спостерігаю свідомого обмеження власних прав громадянами у кіберпросторі. Таким чином порушується баланс прав та обов'язків, а отже – втрачається постульована в цій дихотомії синергія.

Ми таку безвідповідальну позицію не підтримуємо і всіляко виступаємо за ефективне правове регулювання суспільних відносин у сфері кібербезпеки з *чітким встановленням прав та обов'язків,* а головне – відповідальності усіх без винятку учасників правовідносин, у тому числі й посадових осіб – суб'єктів національної системи кібербезпеки. Утім, наразі відбувається така дивна ситуація, коли держава, не маючи достатніх повноважень прав, має нести відповідальність як за рівень кібербезпеки держави, так і за рівень гарантування прав і свобод громадян України у кіберпросторі.

Такі дискусії виникають почасти через банальне незнання засад правового регулювання, а також через свідоме небажання здійснювати аналіз тих чи інших спірних питань, ґрунтуючись на теорії. *Занедбання теорії й постулювання практики як вищого взірця розвитку – шлях неосвічених утопістів, які свідомо спрямовують соціальну систему у вирій невизначеності та хаосу, унеможливлюючи формування «антихрупкості»*.

Тому, зберігаючи лінію дискусії в наукових рамках, зазначимо, що для розуміння необхідності правового регулювання потрібно усвідомлювати, що *зміст правовідносин у сфері кібербезпеки* складає конкретна поведінка суб'єктів правовідносин у сфері кібербезпеки та її юридичне закріплення нормами права у вигляді суб'єктивних прав та юридичних обов'язків. Без такого закріплення змісту не існує, а отже, апріорі не існує правовідносин, а відтак держава не може гарантувати реалізації та захисту інформаційних прав громадян у кіберпросторі. Навіть більше, особи не мають права висувати до держави жодних правових претензій, оскільки, діючи чітко в межах чинного законодавства, держава за відсутності відповідних норм права, а відповідні державні органи через відсутність виникаючої внаслідок цих норм адміністративно-правової компетенції не мають правових механізмів щодо втручання в цей вид вже *соціальних* відносин.

Отже, *за умови відсутності змісту правовідносин правовідносин не існує.*

Для розуміння умов, за яких ці правовідносини можуть мати зміст, потрібно розуміти, що структуру цього змісту складають такі компоненти:

– *юридичний* – суб'єктивне право та юридичний обов'язок, законний інтерес;

– *фактичний* – реальна поведінка суб'єктів.

У нашій реальності фактичний зміст правовідносин у сфері кібербезпеки є, а юридичний, незважаючи на достатню кількість і загалом масив НПА, що регулюють суспільні відносини у кібербезпековій сфері, досі не оформлений належним чином, оскільки бракує системності.

Про це йдеться і в Щорічному посланні Президента, в якому вказується на те, що на виконання Указу Президента України від 13.02.2017 р. № 32/2017, яким було введено в дію рішення РНБО України від 29.12.2016 р. «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», відбувається стратегічний процес – кардинально оновлюються системні механізми реалізації Національної програми інформатизації, яка *тривалий час фактично не виконувалася* (курсив наш – *І.Д.*). Здійснюється контроль за формуванням завдань Національної програми інформатизації на 2018–2020 рр. та поданням відповідних пропозицій на розгляд Верховної Ради України разом із проєктом Закону України «Про Державний бюджет України на 2018 рік» [2, с. 56].

Аналізуючи юридичний компонент змісту правовідносин, інтерпретуючи загальнотеоретичні положення до предмета свого дослідження, визначимо розуміння суб'єктивного права та юридичного обов'язку.

Суб'єктивне право – це вид і міра можливої поведінки суб'єкта, що забезпечується з боку держави. *Структуру суб'єктивного права* складають*:*

1) *праводія*, тобто право поводити себе відповідним чином (право на свої дії) – найбільш розповсюджена форма суб'єктивного права в кіберпросторі;

2) *правовимога*, тобто право вимагати відповідної поведінки від інших суб'єктів, які мають юридичні обов'язки (право на чужі дії);

3) *праводомагання*, тобто право звертатися до держави за захистом свого юридичного права. Право звертатися мають водночас і самі суб'єкти правовідносин, які не бажають нести інші юридичні обов'язки, окрім праводій і правовимог, чим саме і спричинюється конфлікт інтересів.

Саме тому важливим є розуміння сутності ***юридичного обов'язку*** – міра необхідної і належної поведінки, що є гарантією реалізації суб'єктами наданих їм прав. Це об'єктивно необхідна та можлива поведінка, котра забезпечує реальність можливостей, наданих суспільством та державою окремій особі. У разі позитивного ставлення особи до необхідності виконання покладених на неї обов'язків їх реалізація настає лише за певних умов, що передбачені правовою нормою. Держава у системі обов'язків визначає доцільний, соціально корисний та необхідний варіант поведінки суб'єктів з метою забезпечення кібербезпеки. Нормами реалізації обов'язку є дотримання певних зобов'язань, які мають форму заборон, та виконання активних обов'язків, що існують як зобов'язання [3, с. 167].

Структура юридичного обов'язку включає:

– необхідність *належної дії*, тобто здійснювати певні діяння (активні або пасивні обов'язки);

– необхідність *належного виконання*, тобто реакція на законні вимоги суб'єктів забезпечення кібербезпеки, які виступають правомочною стороною;

– необхідність *належного претерпіння*, тобто нести інформаційно-правову відповідальність у разі відмови від виконання юридичних обов'язків або несумлінного їх виконання.

У такому разі виокремлюється потреба у з'ясуванні змісту поняття *«законний інтерес»* – простий юридичний дозвіл, що закріплений у законі або випливає з його змісту та виражається в можливостях суб'єкта права користуватися конкретним соціальним благом, а іноді звертатися по захист до компетентних державних органів або громадських організацій з метою задоволення своїх потреб, які не суперечать суспільним [4], а саме з метою забезпечення нормального існування суспільних відносин у сфері кібербезпеки.

Законний інтерес – це усвідомлена суб'єктом правовідносин у сфері кібербезпеки необхідності задоволення своїх потреб способом, що допускається, але прямо не гарантується чинним інформаційним законодавством.

Таким чином, суб'єктивне право, юридичний обов'язок і законний інтерес виступають об'єктами правової охорони.

Для виникнення, зміни чи припинення правовідносин необхідна не лише зацікавленість у цьому суб'єктів права, а й певні життєві обставини, факти. Останні можуть бути різноманітними. Не всі з них спричиняють виникнення правовідносин, а лише ті, що зазначені у нормативно-правових актах, з якими законодавець пов'язує можливість здійснення учасниками правовідносин їх суб'єктивних прав і юридичних обов'язків [5].

Правовідносини у сфері кібербезпеки виникають (змінюються і припиняються) за наявності необхідних *передумов* – комплексу різних за змістом взаємопов'язаних юридичних явищ, взаємодія яких тягне за собою рух правовідносин [6].

З урахуванням положень загальної теорії права, а також робіт з безпекової тематики можу виокремити загальні (матеріальні) і спеціальні (юридичні) передумови виникнення правовідносин у сфері кібербезпеки [7, с. 144–145].

Загальні (матеріальні) передумови виникнення правовідносин:

– наявність не менше двох суб'єктів права як учасників правовідносин у сфері кібербезпеки;

– об'єкт правовідносин – інтереси (блага, цінності) у сфері кібербезпеки (безпекові інтереси, інтерес безпеки) або блага безпеки як матеріальні, так і нематеріальні, щодо яких суб'єкти вступили у відносини між собою.

Спеціальні (юридичні) передумови виникнення правовідносин:

– *нормативна основа*, характерною ознакою якої виступають відповідні норми тих галузей права, що регулюють суспільні відносини у сфері кібербезпеки;

– *правосуб'єктна основа*, що визначає здатність особи до участі у правовідносинах у сфері кібербезпеки;

– *юридико-фактична основа*, тобто певні юридичні факти (фактичні склади) реальної дійсності, з наявністю яких норми права пов'язують виникнення, зміну або припинення відповідних прав і обов'язків правосуб'єктної особи.

З огляду на викладене зазначимо про проникнення відносин у сфері кібербезпеки в адміністративну, інформаційну, трудову, управлінську, аграрну, житлову, управлінську та інші сфери життєдіяльності.

Можу погодитись із В.А. Ліпканом, який влучно зазначає, що *суб'єкт управління безпекою* зобов'язаний реалізувати власні матеріально-правові та процесуальні права, тобто право виступає одночасно і обов'язком суб'єкта адміністративно-правових відносин у сфері національної безпеки [8, с. 24].

На мою думку, функція підвищення поінформованості громадян про безпеку в кіберпросторі повинна реалізовуватися усіма суб'єктами забезпечення кібербезпеки.

У цьому контексті також необхідним є усвідомлення, що за допомогою кібербезпекових правовідносин має відбуватися індивідуалізація положень відповідної правової норми, конкретизація суб'єктивних юридичних прав і обов'язки суб'єктів кібербезпекових відносин, їхні повноваження і міра можливої юридичної відповідальності за неправомірні дії або невчинення передбачених законодавством дій.

Особливості правовідносин, в тому числі у сфері кібербезпеки, полягають у тому, що вони суттєво залежать від характеру регулятивного впливу норм права, внаслідок чого власно і складаються різні види правовідносин – регулятивні чи охоронні, активні чи пасивні. Саме це спричинює одвічні спори та дискусії особливо в кібернетичній сфері: адже початково Інтернет утворювався як вільний від державного контролю простір, простір свободи. Незважаючи на те, що ця концепція себе не виправдала, більшість почасти фахово необізнаних журналістів або початківців-правників намагаються екстраполювати концепцію людиноцентризму, лібертарну концепцію і концепцію правовладдя до сфери кібербезпеки. Через це ортодоксальні кліше щодо так званої «тоталітарності» охоронних та активних норм є нічим іншим, як нерозумінням складності та концептуальної невизначеності цього виду відносин, а відтак і необхідності випереджувального, більш жорсткого державного регулювання. Заміна теоретичного обґрунтування застосування певних видів норм права призвела до фактичного утворення кіберімперій, які можуть не зважати на дії національного уряду та на місцеве законодавство. Ефективне протистояння глобальній кіберімперії та кіберкапіталізму демонструє лише Китай за допомогою золотого фаєрволу.

Відтак формування правовідносин у кібернетичній сфері і відповідне їх віддзеркалення у нормах права мають відповідати тенденціям їх розвитку, а не ґрунтуватись на застарілих уявленнях про баланс регулятивних і охоронних норм.

Правовідносини у кібернетичній сфері в механізмі їх адміністративно-правового регулювання відповідають за переведення загальних приписів норм права в суб'єктивні права і юридичні обов'язки, визначають повноваження та міру юридичної відповідальності для суб'єктів правовідносин у сфері кібербезпеки, сприяють реалізації національних інтересів у цій сфері.

Узагальнюючи теоретико-правові положення стосовно функцій правовідносин [7, с. 139–140], до *рис правовідносин* у сфері кібербезпеки можемо включити:

– *встановлюють конкретно визначене коло осіб* – суб'єктів правовідносин у сфері кібербезпеки, на яких поширюється дія норм права в конкретному просторовому-часовому форматі. Цим може бути пояснена логіка ухвалення Закону України «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки;

– закріплюють конкретну поведінку, якої повинні або можуть дотримуватися суб'єкти правовідносин у сфері кібербезпеки;

– слугують умовою для можливого приведення в дію спеціальних юридичних засобів (суб'єктами забезпечення кібербезпеки) з метою забезпечення суб'єктивних прав, обов'язків, відповідальності.

Таким чином, правовідносини у сфері кібербезпеки можуть служити засобом переведення загальних розпоряджень юридичних норм у площину суб'єктивних прав і обов'язків як для суб'єктів забезпечення кібербезпеки, так і для суб'єктів правовідносин у цій сфері загалом.

Здійснений догматико-юридичний, структурно-функціональний, герменевтичний аналіз законодавства дозволив аргументувати думку про те, що у сфері кібербезпеки відчутно спостерігається відмінність в обсязі прав та обов'язків *суб'єктів* даних правовідносин залежно від їх правового статусу [9]. Наприклад, громадяни мають переважно права і не хочуть нести відповідальності. Натомість суб'єкти забезпечення кібербезпеки внаслідок колізійності інформаційного законодавства, тиражування одвічних помилок щодо дублювання повноважень у сфері кібербезпеки різними суб'єктами її забезпечення не можуть повною мірою реалізувати державну кібербезпекову політику, оскільки не наділені кореспондуючими їхньому адміністративно-правовому статусу правами.

Держава фактично видавлена зі сфери кібербезпекових правовідносин і в здебільшого виступає спостерігачем та фіксатором чи то відносин, що формуються, чи то правопорушень, чи то інших дій суб'єктів кібербезпекових відносин. Фактично відбувається транснаціональна монополізація глобального кібернетичного простору, включаючи і український сегмент Інтернету. Нерозробленість *концепції інформаційного волонтерства*, неврахування у правовій реальності відчутної ролі волонтерських та інших недержавних громадських організацій та об'єднань громадян у широкому смислі цього слова формують подальші умови для унеможливлення реалізації наступальної стратегії в кіберпросторі, формування сталих умов для стабільного процвітання національних інтересів у його межах. Про роль недержавних організацій і їхню безпосередню участь у реалізації окремих завдань кібербезпекової політики йшлося, зокрема, в Указі Президента України від 13 лютого 2017 р. № 32/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» [10], але в практичній площині в аспекті формування дієвої системи правового регулювання конкретної участі та відповідальності громадян та недержавних організацій щодо забезпечення кібербезпеки не було зроблено відчутних кроків.

Висновки. Отже, можемо **висновувати**, що роль громадянського суспільства, особливо в рамках кібервідносин, потрібно кардинально переоцінити та відповідним чином відобразити це на законодавчому рівні, чітко закріпивши оновлений перелік суб'єктів забезпечення кібербезпеки та включивши до нього інформаційних волонтерів та об'єднання громадян, в тому числі аналітичні центри, суб'єктів підприємницької діяльності, що безпосередньо здійснюють свою діяльність у цій сфері.

У рамках проведеного аналізу також можемо констатувати, що формування національної системи кібербезпеки загалом відбувається за схожим алгоритмом із формуванням систем національної безпеки, протидії тероризму, боротьби зі злочинністю тощо. У жодному чинному нормативно-правовому акті не передбачено критеріїв оцінки ефективності реалізації державної кібербезпекової політики, не визначені чіткі індикатори, за дотримання або створення умов для дотримання яких мають нести відповідальність ці суб'єкти, не визначені параметри юридичної відповідальності за недотримання визначеного рівня кібербезпеки. Таким чином, гіпотетично конкретна реалізація небезпеки в аналізованій сфері не тягне за собою настання юридичної відповідальності у конкретного суб'єкта забезпечення кібербезпеки. Отже, будь-який суб'єкт цієї системи є безвідповідальним.

Отже, наразі відчувається гостра потреба в юридичному оформленні реальної участі в забезпеченні кібербезпеки недержавних суб'єктів, а також закріпленні конкретної відповідальності за реалізацію чітко визначених функцій та завдань вже наявними та легітимними суб'єктами забезпечення кібербезпеки.

Список використаних джерел:

1. Діордіца І. Засади кібернетичної деонтології через співвідношення сущого та належного. *Підприємництво, господарство і право*. 2019. № 8. С. 244-249. DOI https://doi.org/10.32849/2663-5313/2019.12.45.

2. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 році». Київ : НІСД, 2017. 928 с.

3. Теорія держави і права. Академічний курс : підручник / за ред. О.В. Зайчука, Н.М. Оніщенко. Київ : Юрінком Інтер, 2006. 688 с.

4. Теорія держави і права : конспект лекцій. URL: http://pidruchniki.com/16011013/pravo/ponyattya_vidi_pravovih_vidnosin.

5. Государственная концепция развития малых городов и поселков городского типа. URL: http://municipalkg.narod.ru/cc.htm.

6. Теорія держави та права : підручник [за вимогами кредитно-модульної системи навчання] / Є.О. Гіда, Є.В. Білозьоров, А.М. Завальний та ін. ; за заг. ред. Є.О. Гіди. Київ : О.С. Ліпкан, 2010. 322 с.

7. Фатхутдінов В.Г. Адміністративно-правове регулювання у сфері громадської безпеки в Україні : монографія. Київ : Освіта України, 2016. 400 с.

8. Ліпкан В.А. Адміністративно-правові основи забезпечення національної безпеки України : автореф. дис. … д-ра юрид. наук : 12.00.07. Київ, 2008. 36 с.

9. Діордіца І. В. Кібербезпекова політика України: стан та пріоритетні напрями реалізації : монографія. Запоріжжя : Видавничий дім «Гельветика», 2018. 548 с.

10. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» : указ Президента України від 13 лют. 2017 р. № 32/2017. URL: http://zakon3.rada.gov.ua/laws/show/32/2017.

УДК 343.85:343.9.02(477)
DOI https://doi.org/10.32844/2618-1258.2020.1.27

ДОЦЕНКО О.С.

ПРОГНОЗУВАННЯ В АДМІНІСТРАТИВНО-ПРАВОВОМУ ЗАБЕЗПЕЧЕННІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УКРАЇНІ

Стаття присвячена досить важливій і актуальній проблемі – прогнозуванню адміністративно-правового забезпечення протидії організованої злочинності в Україні.

Визначено, що успішне формування ефективного адміністративно-правового механізму забезпечення протидії організованій злочинності повинно відбуватися на науковому прогнозуванні.

Обгрунтовується, що прогнозування базується на ретельному аналізі. Визначено взаємозв'язок аналітичної діяльності з прогнозуванням: чим більш точно і повно буде проаналізована інформація про стан організованої злочинності, її наміри і тенденції, тим більш об'єктивним і реалістичним буде прогноз та ймовірність його підтвердження у майбутньому.

Наголошено, що прогноз повинен будуватися на аналізі минулого і нинішнього стану організованої злочинності та адміністративно-правового забезпечення протидії їй з урахуванням закономірностей розвитку.

З'ясовано зміст прогнозування, його зв'язок із виробленням стратегії і тактики протидії організованій злочинності, перспективним і поточним плануванням.

Обгрунтовується використання прогнозування для вироблення правильної програми дій і прийняття управлінських рішень, що забезпечують досягнення найкращих результатів під час виконання поставлених завдань з протидії організованій злочинності.

Розглянуто окремі складнощі прогнозування організованої злочинності, зокрема її складної внутрішньої структури і розгалуженої злочинної діяльності. Підкреслено, що різноманітність злочинної діяльності організованих злочинних формувань зумовлює і відповідні види прогнозування.

Розглянуто методи прогнозування організованої злочинності: екстраполяцію, моделювання й експертну оцінку.

Визначено основні недоліки здійснення прогнозування організованої злочинності в Україні. Підкреслено, що проблема прогнозування адміністративно-право-

© ДОЦЕНКО О.С. – кандидат юридичних наук, доцент, професор кафедри публічного управління та адміністрування (Національна академія внутрішніх справ)