

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**



**Федотов Данило Вадимович
Романов Максим Юрійович**

**АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ**

Монографія

Дніпро 2025

Автори:

Данило Федотов – старший слідчий відділу розслідування злочинів загальнокримінальної спрямованості слідчого управління Головного управління Національної поліції в Дніпропетровській області, доктор філософії в галузі права, капітан поліції;

Максим Романов – старший науковий співробітник науково-дослідної лабораторії превентивної діяльності та соціологічних досліджень Дніпровського державного університету внутрішніх справ, доктор філософії в галузі права.

Рецензенти:

Олександр Кобзар – т. в. о. директора Навчально-наукового інституту № 1 Національної академії внутрішніх справ, доктор юридичних наук, професор, полковник;

Наталія Коваленко – суддя Касаційного адміністративного суду в складі Верховного Суду, доктор юридичних наук, професор.

Ф 34 Федотов Д. В., Романов М. Ю. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Національній поліції України: монографія. Дніпро : Дніпровський державний університет внутрішніх справ. Київ : «7БЦ», 2025. 208 с.

ISBN 978-617-549-514-8

Монографію присвячено дослідженню адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України. Обґрунтовано позицію, що правовий режим інформації, що діє в Національній поліції України має режимні обмеження, щодо роботи з нею, що в свою чергу, потребує особливого підходу до забезпечення дії відповідного адміністративно-правового механізму, що спрямовується не лише на внутрішній захист інформації, що використовується в роботі поліції, а й потребує запобігання її витоку назовні, що може порушити права і свободи людини і громадянина.

Видання стане корисним для практичних працівників органів охорони та захисту правопорядку України (зокрема й працівників Національної поліції України), практикуючих юристів, а також науково-педагогічних працівників закладів освіти правничого фаху та здобувачів вищої освіти.

ISBN 978-617-549-514-8

© Федотов Д. В., Романов М. Ю., 2025
© ДДУВС, 2025

ЗМІСТ

ВСТУП	5
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ.....	13
1.1. Інформаційна безпека як об'єкт адміністративно- правового забезпечення	13
1.2. Поняття адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України	32
1.3. Структура адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України	52
Висновки до розділу 1.....	76
 РОЗДІЛ 2. ЗМІСТ ОКРЕМИХ ЕЛЕМЕНТІВ АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ	 78
2.1. Нормативно-правове регулювання інформаційної безпеки в Національній поліції України	78
2.2. Суб'єкти забезпечення інформаційної безпеки в Національній поліції України	97
2.3. Адміністративна відповідальність за порушення вимог до інформаційної безпеки в Національній поліції України	128
Висновки до розділу 2.....	145

РОЗДІЛ 3. УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ	149
3.1. Зарубіжний досвід забезпечення інформаційної безпеки в поліцейських підрозділах та шляхи його запровадження в Україні	149
3.2. Пріоритетні напрями вдосконалення адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України	164
Висновки до розділу 3.....	175
ВИСНОВКИ	177
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	184

ВСТУП

Конституцією України та іншими законодавчими нормативно-правовими актами визначено, що права і свободи людини та громадянина в Україні є найвищою соціальною цінністю, а держава забезпечує належне функціонування системи органів правопорядку, обов'язком яких є забезпечення дотримання відповідних прав і свобод, а також якісне відновлення відповідних прав у межах своєї компетенції. Водночас Національна поліція України як орган правопорядку й основний інститут забезпечення прав і свобод людини та громадянина в Україні виконує широке коло функцій та обов'язків, реалізація яких в умовах триваючої збройної агресії росії, системного порушення прав і свобод людини та громадянина окупаційними військами рф на територіях України дедалі більше ускладнюється.

Система (механізм) забезпечення інформаційної безпеки в загальнодержавному значенні є однією з найбільш фундаментальних інституцій впливу на правовідносини у сфері інформації. В умовах активних бойових дій, постійних загроз ракетних обстрілів та інших виявів інформація є ключовим чинником забезпечення прав і свобод людини та громадянина. Крім того, правоохоронна діяльність поліції, що здебільшого має гласний характер, жорстко регулюється засадами та правилами інформаційної безпеки, механізм забезпечення якої наразі є недосконалим.

Сучасна система органів правопорядку, покликаних здійснювати ефективне забезпечення прав і свобод людини та громадянина, не має належно функціонуючого механізму

забезпечення інформаційної безпеки. Це твердження, зокрема, стосується й Національної поліції України.

Системні вияви витоку інформації для службового користування, негласних оперативно-розшукових матеріалів, імовірні порушення засад дотримання режиму таємності та непрофесійність працівників у питаннях дотримання інформаційної безпеки ставлять під загрозу можливість відповідного органу ефективно забезпечувати дотримання прав і свобод людини та громадянина в Україні й за її межами (у межах компетенції). Саме тому, на нашу думку, урахуовуючи такий фактор, як триваюча збройна агресія рф та правовий режим воєнного стану в Україні, відповідне питання потребує додаткового опрацювання з урахуванням позицій дослідників і законодавства України, а також міжнародних нормативно-правових актів і думок відповідних правників.

Деякі аспекти окресленої проблеми досліджували такі вітчизняні дослідники в галузі адміністративного права та супутніх правових галузей, як Л. Аркуша, Л. Багрій-Шахматов, О. Бандурка, О. Безпалова, Ю. Битяк, М. Бурбика, О. Бусол, С. Васюк, О. Винник, І. Голосніченко, В. Грохольський, Ю. Дем'янчук, Л. Доля, О. Дрозд, Є. Зеленський, І. Зозуля, О. Кобзар, О. Копан, А. Куліш, М. Логвиненко, М. Мельник, О. Музичук, Н. Міняйло, Т. Міщенко, Є. Невмержицький, І. Пастух, Р. Сербин, О. Стрельченко, С. Шатрава, О. Шевченко та ін.

Водночас, належно оцінюючи значний науковий внесок авторів у вивчення питання формування та вдосконалення адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України, слід зазначити, що стрімкі євроінтеграційні процеси, триваючі

бойові дії з військами держави-окупанта росії, а також потреба в суттєвому вдосконаленні фундаментальних засад забезпечення дотримання інформаційної безпеки в Національній поліції України зумовлюють необхідність додаткового наукового опрацювання відповідних аспектів у галузі адміністративного права.

Тема ґрунтується на Національній стратегії у сфері прав людини (Указ Президента України від 24 березня 2021 року № 119/2021), Стратегії кібербезпеки України на 2023-2024 роки (розпорядження Кабінету Міністрів України від 19 грудня 2023 р. № 1163-р), Стратегії інформаційної безпеки (Указ Президента України від 28 грудня 2021 року № 685/2021), Цілях сталого розвитку України на період до 2030 року (Указ Президента України від 30 вересня 2019 року № 722/2019), Стратегії розвитку Національної академії правових наук України на 2021–2025 роки, затвердженій постановою загальних зборів НАПрН України від 26 березня 2021 року № 12-21; відповідає тематиці наукових досліджень і науково-технічних (експериментальних) розробок на 2020–2024 роки (наказ МВС України від 11 червня 2020 року № 454).

Мета і завдання дослідження. Метою дослідження є надання комплексної характеристики адміністративно-правовому механізму забезпечення інформаційної безпеки в Національній поліції України.

Поставлена мета зумовила потребу в розв’язанні таких завдань:

– дослідити інформаційну безпеку як об’єкт адміністративно-правового забезпечення;

- визначити поняття адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України;

- схарактеризувати структуру адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України;

- проаналізувати нормативно-правове регулювання інформаційної безпеки в Національній поліції України;

- встановити суб'єкти забезпечення інформаційної безпеки в Національній поліції України;

- окреслити межі адміністративної відповідальності за порушення вимог у сфері інформаційної безпеки в Національній поліції України;

- проаналізувати зарубіжний досвід забезпечення інформаційної безпеки в поліцейських підрозділах та шляхи його впровадження в Україні;

- визначити пріоритетні напрями вдосконалення адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України.

У монографічному дослідженні вперше визначено сутність адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України, уточнено напрями його функціонування, сформульовано науково обґрунтовані пропозиції та рекомендації щодо його вдосконалення. Запропоновано розв'язання проблеми в контексті адаптації норм вітчизняного законодавства до європейського з метою оптимізації адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України.

У монографії аргументовано також деякі положення, що становлять наукову новизну, а саме:

вперше:

– запропоновано удосконалення статті 212⁻⁵ «Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію» Кодексу України про адміністративні правопорушення, шляхом доповнення її новими частинами, що урегулюють порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що є конфіденційними (згідно з статтею 6 (Публічна інформація з обмеженим доступом) Закону України «Про доступ до публічної інформації» та викладу назви статті в такій редакції: «Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять публічну інформацію з обмеженим доступом»;

– доведено необхідність виокремлення, в структурі Закону України «Про національну безпеку України» інформаційну безпеку, як окремий напрям державної безпекової політики, оскільки наразі таке визначення не регламентується;

– запропоновано доповнити законодавство України, зокрема Закон України «Про Національну поліцію» положеннями щодо обов'язковості отримання сертифікату про підготовку у сфері кібербезпеки та безпеки інформації, перед призначенням на посаду поліцейського з метою підвищення рівня цифрової грамотності та посилення спроможності протидіяти кіберзагрозам тощо.

удосконалено:

– поняття інформаційної безпеки як об'єкта адміністративно-правового забезпечення розглядати крізь призму національної та державної безпеки, що найбільш

виразно виявляється в умовах постійно діючих загроз і дії надзвичайних правових режимів, що прямопропорційно впливає на зміст, сутність і межі застосування правового інструментарію щодо її забезпечення;

– позицію про те, що створення спеціально уповноваженого на забезпечення інформаційної безпеки підрозділу у Національній поліції України значно посилило б її інституційну спроможність у цій сфері та дозволило б уникнути дублювання повноважень і функцій щодо забезпечення інформаційної безпеки, покладених (віднесених) до компетенції різних підрозділів;

– систематизовано суб'єкти забезпечення інформаційної безпеки в Національній поліції України. До кола таких суб'єктів віднесено підрозділи документального забезпечення (зокрема режиму й технічного захисту інформації), інформаційно-аналітичної підтримки, внутрішньої безпеки, головної інспекції та дотримання прав людини, спеціального зв'язку (зокрема їх територіальні підрозділи в складі головних управлінь Національної поліції);

– положення, згідно з яким позитивні європейські практики щодо забезпечення інформаційної безпеки в поліцейських підрозділах, зокрема в частині створення єдиного інформаційно-аналітичного простору органів правопорядку та забезпечення можливості безперешкодного й безпечного користування ним усіма без винятку поліцейськими, мають бути імплементовані в організаційно-управлінському та нормативно-правовому контексті в Україні;

– структуру адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України як таке конструктивно-організаційне поєднання

мети, завдань, специфічних функцій, принципів і гарантій, що дозволяє втілити в життя запланований результат соціально-правового впорядкування цієї сфери правовідносин;

дістали подальший розвиток:

– розуміння пріоритетних напрямів удосконалення адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України, до яких належать організаційно-управлінський, нормативно-правовий, аналітико-технічний.

Практичне значення одержаних результатів дослідження полягає в тому, що монографія є одним з перших в Україні комплексних досліджень, присвячених аналізу адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України.

Особистий внесок у розвиток відповідного напрямку в межах науки адміністративного права полягає в обґрунтуванні найбільш суттєвих положень стосовно визначення фундаментальних понять і категорій, уточненні сутності адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України. Результати дослідження можуть бути використані:

– у законодавчій діяльності – шляхом імплементації положень дослідження до чинних законів України та надання пропозицій до проєктів законів України до адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України;

– у науково-дослідній діяльності – для розширення меж теоретичного осмислення питань забезпечення ефективного функціонування адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції

України (акт впровадження Національної академії внутрішніх справ від 09.06.2025 № 101-НД);

– в освітньому процесі – під час розроблення спеціальних курсів, написання підручників, навчальних посібників, практикумів, аналітичних оглядів, енциклопедичних видань та інших навчальних праць з питань забезпечення функціонування адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України (акт впровадження Національної академії внутрішніх справ від 09.06.2025 № 100-ОП);

– у практичній діяльності – для підвищення ефективності функціонування адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України (акт впровадження Департаменту інформаційно-аналітичної підтримки Національної поліції України від 20.06.2025 № 58431-2025).

У праці використано законодавство України, якщо інше спеціально не застережене, станом на 01 вересня 2025 року.

Автори дякують за допомогу в підготовці монографічного дослідження рідним і близьким, друзям, наставникам, іншим науковцям і практикам. Особлива подяка рецензентам монографії Олександру Кобзарю та Наталії Коваленко, а також голові спеціалізованої вченої ради Національної академії внутрішніх справ, створеної з правом разового захисту дисертації одного з авторів монографії – Денису Тихомирову, а також її членам – Андрію Коваленку, Віті Кононець та Максиму Пендюрі, за мотивацію до подальших наукових пошуків і конструктивну критику.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ АДМІНІСТРАТИВНО- ПРАВОВОГО МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ

1.1. Інформаційна безпека як об'єкт адміністративно- правового забезпечення

Необхідність забезпечення прав і свобод людини і потребує системного та виваженого розвитку законодавства, пов'язаного з його забезпеченням, оскільки принципи правової державності, перш за все, базуються на конкретних нормативно-правових актах. Інформаційна безпека, в умовах стрімкого розвитку цифровізаційних процесів і цифрової цивілізації суспільства розглядається не як благо, а як конкретна та точна умова стабільного та виваженого функціонування суспільства та, відповідно, всіх без виключення соціально-правових відносин. Тому, належне наукове опрацювання інформаційної безпеки, як об'єкта адміністративно-правового забезпечення, на нашу думку, слід розглядати якомога більш детально, зокрема з урахуванням сучасних безпекових тенденцій, триваючий правовий режим воєнного стану на території України, а також заходи х відсічі збройної агресії росії проти нашого суверенітету, територіальної цілісності та державності загалом.

Ці та інші загрози для всього цивілізованого світу, мають також і інформаційний, а також і кібер характер,

оскільки станом на сьогодні, інформація шириться саме завдяки цифровим медіа та інформаційним ресурсам із можливістю здійснення своєї діяльності онлайн. Ба більше, органи державної влади, що апелюють значним обсягом інформації, пов'язаної, у тому числі з персональними даними людини і громадянина також використовуються в своїй діяльності інформаційні онлайн ресурси, що дозволяють оперативно обмінюватись даними та накопичувати відповідні інформаційні бази, відслідковувати результативність своєї діяльності, безпосередньо моніторити правопорядок у суспільстві тощо [135].

Економічну та інформаційну безпеку підприємства можна розглядати як практичне використання таких принципів сучасного менеджменту, як своєчасна реакція на зміни в зовнішньому середовищі, бачення підприємства, тобто чітке подання про те, що воно повинно собою представляти, а також одного з основних положень сучасної теорії управління – ситуаційного підходу до керування, який означає важливість швидкості й адекватності реакції, що забезпечують адаптацію підприємства до умов його існування. Звідси економічну та інформаційну безпеку підприємства слід розглядати як еволюційний розвиток ситуаційного підходу до керування. Економічна та інформаційна безпека викликають усе більшу зацікавленість підприємств, які стикаються із труднощами при реалізації принципово нових підходів до керування підприємствами, при організації керування підприємством у ринкових умовах [49]. Водночас, можливість належного адміністративно-правового забезпечення інформаційної безпеки діяльності будь-якого органу державної влади прямопропорційно співвідноситься з його належним нормативно-правовим

забезпеченням, оскільки всі без виключення органи державної влади та їх посадові особи зобов'язані діяти виключно в межах і у спосіб прямо передбачені указаними нормами законодавства. При цьому, інформаційна безпека, як об'єкт адміністративно-правового забезпечення в діяльності Національної поліції України, розглядається нами, як необхідна та важлива умова ефективного функціонування зазначеного органу державної влади, а також можливості та спроможності виконання ним покладених на нього завдань і обов'язків.

Вчені засвідчують співвідношення верховенства права та закону, що дає підстави ствердити про верховенство природного права над законами, а також обов'язок будь-якої держави «санкціонувати» такі права в спосіб, визначений загальнонародним договором про юридичні засади співіснування – конституцією [64; 65].

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 [78, с. 252]. Крім цього, складність зазначених процесів, на нашу думку, суттєво посилюється в умовах необхідності належного адміністративно-правового регулювання інформаційної діяльності системи Національної поліції України, оскільки зазначене коло нормативно-правових актів, що забезпечують впорядкування зазначених

соціально-правових відносин у вказаній сфері так само недосконале.

Загострення політичної ситуації, в останні роки, призвело до виведення даної проблеми на перші щаблі. У зв'язку з переходом країни на європейський шлях розвитку і зміни пріоритетів в діяльності з колишньої «міліції» в органи Національної поліції, переорієнтація їх на виконання функцій соціально-правового обслуговування населення. В даний час вирішити ці завдання можливо за умови пильної уваги керівництва Національної поліції до кадрової політики. З точки зору системного підходу до управління вона розглядається в двох значеннях – зовнішньому і внутрішньому. Зовнішній аспект управлінської діяльності пов'язаний із здійсненням широкого комплексу функцій органу управління виходячи з його соціального призначення. Внутрішній характеризує її як власне управлінську працю, що виражається в реалізації функцій органу шляхом законодавчо визначеного впливу у внутрішньому функціонуванні середовища [113; 148].

Підтримуючи наведену думку, В.В. Сокурєнко, О.М. Бандурки, О.І. Безпалова та О.В. Джафарова наголошують на тому, що керівник органу (підрозділу) поліції повинен: 1) бути прикладом дотримання Конституції та законів України, інших нормативноправових актів, прийнятих відповідно до Конституції та законів України, професійно-етичних вимог, основних принципів професійної діяльності та правил поведінки поліцейських, а також вимагати їх дотримання від підлеглих; 2) відповідати за віддані (видані) розпорядження (доручення) і накази, наслідки їх реалізації, відповідність їх законодавству України; 3) об'єктивно оцінювати виконання службових обов'язків підлеглими, а в разі порушення норм

законодавства України або недотримання їх вимог – ініціювати притягнення їх до відповідальності згідно із законодавством України [1; 14; 129, с. 250–251].

Загрози цілісності інформації направлені на заборонену режимом доступу (порядком отримання, використання, розповсюдження і зберігання інформації) її зміну або спотворення, що призводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена сумісно, а також внаслідок об’єктивного впливу з боку середовища, що оточує носій інформації. Інформація зберігає цілісність, якщо дотримується встановлена режимна адекватність щодо правил її модифікації (видалення) [49]. Спираючись на окреслену позицію необхідно зазначити, що в своїй діяльності Національна поліція України та всі підпорядковані їй посадові особи систематично використовують інформацію з різними режимними обмеженнями, що суттєво актуалізує необхідність забезпечення належного адміністративно-правового регулювання інформаційної безпеки у відповідній сфері. Крім цього, належить підкреслити, що наявність специфічних норм та відповідних положень у організаційно-управлінських актах, може суттєво посилити зазначений напрям роботи.

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 [121, с. 89]. Чільним необхідно зазначити, що поліваріативність підходів до визначення змісту і сутності інформаційної безпеки, як об'єкта адміністративно-правового регулювання загалом, та зокрема, в діяльності Національної поліції України безперечно негативно впливає на зазначений напрям роботи указанного органу державної влади. Така неточність може призвести до точкових та системних порушень прав і свобод людини і громадянина у поліцейській діяльності, що неминуче призведе до зниження стандартів правоохорони в державі, а також дотримання та забезпечення інституту прав і свобод людини і громадянина у контексті функціонування в Україні правового режиму державності та демократії.

Однією з таких загроз є розширення за допомогою сучасних цифрових технологій можливостей впливу на свідомість індивіда шляхом інформаційного маніпулювання задля досягнення певних інтересів третіх осіб, що негативно впливає на розвиток особистості та суспільства загалом. Хоча використання сучасних цифрових технологій у соціокультурній сфері дає нові можливості самореалізації через дистанційну освіту, зайнятість, доступ до світових культурних цінностей, воно одночасно створює загрози саморозвитку особистості та реалізації її інтересів через здійснення маніпулятивного впливу на її поведінку. Прикладами такого маніпулювання є пряма й прихована реклама у ЗМІ, інформація політичного та релігійного характеру, яка поширюється за допомогою сучасних інформаційно-комунікаційних технологій та може підривати

інформаційний суверенітет і формувати загрози інформаційній безпеці не тільки окремої особистості, але й суспільства загалом [130]. Дотримання інформаційної безпеки в діяльності Національної поліції України, а також укріплення відповідного адміністративно-правового механізму, перш за все, прямопропорційно співвідноситься із можливістю захисту різних ступенів інформації, що використовуються для ефективізації діяльності відповідного центрального органу виконавчої влади та забезпечення реалізації покладених на нього обов'язків, в контексті охорони прав і свобод людини громадянина громадянина. Крім цього, нами зауважується, що можливість ефективного здійснення поліцейських функцій забезпечується у тому числі у спосіб накопичення певного кола інформації та її систематичного і об'єктивного використання процесі реалізації правоохоронної функції держави, що покладено на Національну поліцію України. Саме тому інформаційна безпека, як об'єкт адміністративно-правового регулювання є надзвичайно важливою, зокрема з огляду забезпечення можливості здійснення визначених обов'язків та виконання покладених на Національну поліцію України завдань.

Наголошуючи на недосконалості загальнопоширеного визначення безпеки через стан захищеності життєво важливих інтересів особи, суспільства і держави від внутрішніх та зовнішніх загроз, автори зазначають, 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» [74, с. 58]. Таким чином, необхідно підкреслити, що інформаційна безпека крізь призму зазначеного загальноправового розуміння сутності поняття безпеки є комплексом умов і обставин, що прямопропорційно впливають на процес дотримання прав і свобод людини і громадянина в інформаційній сфері, з метою забезпечення його самореалізації та уможливлення контролю за цими процесами. Крім цього, слід звернути увагу на те, що безпека, як статичне явище не може діяти без динамічних елементів та забезпечується власне ними. Інформаційна безпека в сучасних безпекових умовах перебуває під впливом низки негативних факторів, що можуть серйозно вплинути на її становище, що в свою чергу потребує належного теоретико-правового опрацювання та пошуку ефективних інструментів вирішення проблемних питань.

Світовий досвід боротьби зі шкідливим інформаційним впливом полягає як у використанні інструментів обмеження політичної, економічної та соціальної реклами та іншої нав'язливої шкідливої інформації, так і в особистому свідомому контролі над інформацією, що надходить. Пріоритетними напрямками державної інформаційної політики в протидії масштабним негативним інформаційно-психологічним впливам мають бути як інтеграція країн у міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації, що протидіють негативним інформаційним впливам на свідомість, удосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та

дієве правове регулювання інформаційних процесів, так і ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригування державної політики в інформаційній сфері. Крім того, пріоритетними завданнями інформаційних структур владних органів мають бути контроль за інформаційними потоками; надання об'єктивної, вичерпної інформації, представлення фахових коментарів та пояснень щодо подій; систематичне висвітлення офіційної позиції посадових осіб та політичних лідерів [47]. Відповідно, механізм адміністративно-правового забезпечення інформаційної безпеки в діяльності Національної поліції України загалом, та зокрема в умовах дії правового режиму воєнного стану повинен включати низку інструментів, що полягають у обмеженні можливості розповсюдження конфіденційної інформації, тобто такої, що становить службовий інтерес та важливість, а також дотримання внутрішньокорпоративної етики та, перш за все, законодавства України у питаннях пов'язаних із адміністративно-правовими режимами інформації, у тому числі в контексті забезпечення інформаційної безпеки суспільства та держави в цілому.

Важливість належного дотримання визначених законодавством України інформаційно-правових режимів та принципів інформаційної безпеки, на нашу думку, прямопропорційно корелюється із діючою широкомасштабною агресією російської федерації, що виражається не лише в збройному аспекті, а полягає також і у веденні інформаційної та кібервійни, що відповідно потребує релевантного спротиву та здійснення превентивних заходів у цій сфері з боку органів правопорядку та всіх суб'єктів сектору безпеки і оборони України.

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 [78, с. 253]. Відповідно, слід зазначити, що питання пов'язані з забезпеченням ефективного здійснення контролю за інформаційною безпекою, в контексті діяльності Національної поліції України, перш за все розглядається крізь призму адміністративно-правового аспекта, оскільки будь-яка така діяльність має бути пов'язана з правом і безпосередньо правозастосовною практикою, що є можливою виключно в реаліях дії законодавства, що взаємопов'язане з дією права та принципами правової державності.

Окрім зазначених інструментів правового та регуляторного впливу держави на інформаційну сферу, до методів протидії шкідливому інформаційному впливу слід віднести розвиток у суспільстві здатності до особистого свідомого контролю над інформацією, що надходить. Цей метод передбачає формування критичного мислення, здатності орієнтуватися у величезному масиві інформації, кількість якої в інформаційну епоху зростає невпинно. Це потребує достатньо високого культурного та освітнього рівнів особистості та суспільства, тому основні зусилля

держави повинні бути націлені на розвиток відповідних сфер суспільного виробництва як інструментів формування адекватного інституціонального середовища [130].

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 [75; 103].

Існує два аспекти трактування інформаційної безпеки у контексті національної безпеки. З одного боку, інформаційну безпеку розглянуто як самостійний елемент національної безпеки будь-якої країни, а з іншого – інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної тощо. Найповнішим є таке визначення: інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства і держави, за якого зводиться до мінімуму завдання збитків через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [40]. Так, інформаційна безпека вченими та дослідниками, розглядається, перш за все як запобіжник

неправомірного поводження з нею, а також як інструмент управління суспільством, що дозволяє здійснювати конкретні волевиявлення та втілювати види соціально-правової поведінки в конкретних формах. Відповідно, інформаційна безпека, як вид правового режиму та інструмент безпечної комунікації в житті соціуму, уможливорює досягнення поставлених перед правовою державністю завдань. Проте, слід зауважити, що окремі аспекти інформаційної безпеки, перш за все прямопропорційно пов'язані з необхідністю групування та узагальнення інформації про конкретних осіб, зміст і сутність їх соціального життя (як от ДНК-профілі злочинців чи облікові картки осіб, засуджених до відбування покарання не пов'язаного з позбавленням волі), що кратно підсилює необхідність злагодженого функціонування механізму інформаційної безпеки крізь призму норм адміністративного законодавства.

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 [78, с. 253].

Україна стала об'єктом інформаційно-психологічних впливів, операцій, війн та її інформаційна безпека опинилась під загрозою. Можна констатувати, що: 1) український

інформаційний простір є незахищеним від зовнішніх негативних пропагандистсько-маніпулятивних впливів і стає об'єктом інформаційної експансії; 2) у світовому медіапросторі відсутній український національний інформаційний продукт, що поширював би об'єктивну, неупереджену та актуальну інформацію про події в Україні. Як наслідок – світова громадськість відчуває брак інформації або отримує її з інших джерел, які часом дезінформують, надають викривлену, спотворену, неповну інформацію. Водночас проти України активно застосовується потужний медіаресурс, здійснюється експансія іноземних суб'єктів на ринку інформаційних послуг, активізуються негативні інформаційні впливи, які спрямовані на викривлення реальності, заниження міжнародного іміджу держави; 3) діяльність вітчизняних ЗМІ щодо систематичного, об'єктивного висвітлення фактів, подій та явищ є недостатньою та позбавлена стратегічного планування; інформаційно-комунікативна політика України у сфері національної безпеки потребує невідкладного перегляду та удосконалення [47]. Необхідно зауважити, що не вся інформація, що використовується Національною поліцією України містить режимні обмеження, деяка з окресленої, перш за все безпосередньо відноситься до категорії «з публічним доступом», що на нашу думку може негативно впливати на окремі аспекти функціонування поліції, зокрема в умовах дії правового режиму воєнного стану на території України та реалізації заходів із відсічі збройній агресії росії проти України. Необхідність забезпечення не лише ефективної роботи механізму адміністративно-правового захисту режиму інформаційної безпеки, а й підвищення якості змістовного його наповнення є важливою запорукою

ефективізації охоронних процесів у відповідній площині, що в свою чергу дозволить підвищити якість забезпечення та дотримання прав і свобод людини і громадянина.

О.П. Баранов визначає 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 [12, с. 60–62]. Відповідно, в контексті відбиття збройної агресії росії проти України, в новому світлі постають зазначені завдання, що мають на меті також ефективно забезпечення протидії агресору та мають створювати коло нормативно-правових і соціальних засад, що уможливлюють ефективну діяльність всіх, без виключення органів державної влади, щодо забезпечення ефективного функціонування механізму адміністративного правового забезпечення інформаційної безпеки.

На жаль, як зазначає В. Петрик, низький загальний рівень інформаційної інфраструктури України сприяє експансії іноземними компаніями ринку інформаційних послуг, що створює сприятливі умови для перерозподілу ефірного часу на користь іноземних програм, окремі з яких засмічують український інформаційний простір своїм баченням подій, пропагують спосіб життя та традиції, тим самим деструктивно впливаючи на суспільство і державу, руйнуючи морально-етичні основи генофонду української нації. Недостатній професійний, інтелектуальний і творчий рівень вітчизняного виробника інформаційного продукту та

послуг, його не конкурентоспроможність не лише на світовому ринку, а й в Україні, призводить до того, що українська аудиторія, природно, віддає перевагу іноземним інформаційним програмам. Недостатній контроль з боку держави за дотриманням законів України політичними силами, ЗМІ та окремими особами, які займаються підприємницькою діяльністю в інформаційній сфері, призводить до того, що нині трапляються непоодинокі випадки надання ефірного часу теле- та радіопрограмам, спрямованим на руйнування моральних цінностей, свідомості української нації [85]. Слід зауважити, що враховуючи характер і зміст інформації, що може бути висвітлено окремими медіа у прямому етері чи у форматі публікації, а також допускаючи недостовірність цієї інформації або її достовірність, проте отримання у спосіб, що суперечить, як інформаційному законодавству так і засадам поведінки з тим чи іншим видом інформації, адміністративний та кримінально-правовий характер ролі та місця Національної поліції України полягатиме у необхідності надання належної правової кваліфікації зазначеним діям, що в свою чергу також є одним із структурних елементів адміністративно-правового механізму забезпечення інформаційної безпеки Національною поліцією України.

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 [26, с. 9–18]. Слід підкреслити, що в епоху новітніх інформаційних технологій інформація дійсно стала основним із предметів обігу соціально-правових відносинах, а тому відповідні правові механізми її захисту, а також захисту всіх без виключення інформаційних прав людини і громадянина має бути суттєво вдосконалено, зокрема і у спосіб покращення адміністративних та організаційно-правових засад діяльності всіх, без виключення, органів правопорядку, чільне місце серед яких займає Національна поліція України, що має виключне коло компетенції, як в адміністративно-правовому так і в кримінально-правовому векторі притягнення осіб до юридичної відповідальності.

Для побудови ефективної системи інформаційної безпеки необхідно виміряти рівень значущості (важливості, суттєвості) загроз інформації. При цьому слід враховувати, що хоч загрози можуть бути спрямовані на різні властивості інформації (конфіденційність, цілісність, доступність, надійність тощо), необхідно якимсь чином забезпечити можливість співставлення та порівняння значущості цих загроз, а також обрахування інтегральної оцінки рівня значущості всієї множини загроз. Міжнародні стандарти у якості показника значущості загроз рекомендують використовувати ризик загроз, під яким розуміють ймовірну шкоду, що виникає внаслідок реалізації часткової загрози або усієї множини загроз [10; 154]. Слід зауважити, що не лише алгоритм виявлення та класифікації загроз тому чи іншому виду інформації має суттєве значення для ефективного

функціонування адміністративно-правового механізму її захисту, зокрема в діяльності Національної поліції України. Одним із найбільш важливих аспектів є також скрупульозний та виважений підхід до класифікації її видів, що в свою чергу прямопропорційно впливає на змістовне наповнення тих чи інших нормативно-правових актів, що регулюють відповідний правовий режим та уможливають здійснення заходів забезпечення, як його правореалізації у вузькому розумінні, так і інформаційної безпеки в суспільстві загалом.

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 [75]. На нашу думку, слід погодитись із запропонованою автором позицією та взяти за основу визначену класифікацію напрямів дослідження поняття інформаційної безпеки та врахувати їх у контексті дії адміністративно-правового механізму її забезпечення в діяльності Національної поліції України. При

цьому, необхідно також підкреслити, що всі зазначені структурні елементи категорії інформаційна безпека тісно взаємопов'язані між собою та зумовлюють стійкий соціально-правовий зв'язок, що зумовлює потребу надання їм характеристики, крізь призму принципу відділення загального від його структурних компонентів.

Поняття «безпека інформації» та «інформаційна безпека» безумовно пов'язані між собою. Оскільки зміст поняття «безпека» визначається вибором об'єкта захисту, то якщо цим об'єктом виступає власне інформація, тоді поняття «інформаційна безпека» і «безпека інформації» синонімічні. Але якщо в якості об'єкта /суб'єкта захисту розглядається деякий учасник інформаційних відносин, то слово «інформаційна» в даному терміні вказує на напрямок діяльності, яка може заподіяти шкоду об'єкту / суб'єкту захисту. У цьому випадку поняття «інформаційна безпека» слід трактувати як стан захищеності деякого об'єкта / суб'єкта від загроз інформаційного характеру. Таким чином, поняття «інформаційна безпека» слід вважати родовим по відношенню до поняття «безпека інформації», а їх взаємозамінність є неприпустимою. На жаль, в Україні коло питань інформаційної безпеки практично звужено до проблем безпеки інформації, і основна увага громадськості сконцентрована переважно на проблемі захисту інформації [10]. Зазначене, крім усього іншого додатково підкреслює необхідність термінологічної характеристики окреслених понять і категорій, крізь призму дії адміністративно-правового механізму забезпечення відповідного правового режиму.

На погляд науковців, внутрішньоорганізаційні відносини в органах публічної влади слід розглядати як окрему

складову предмета адміністративного права, яка має особливий характер. Специфічна риса цієї групи відносин полягає в тому, що вони існують та регулюються переважно на єдиних базових засадах незалежно від того, до якої підсистеми публічної влади (державна влада або місцеве самоврядування) або до якої складової державної влади (законодавча, виконавча, судова гілка тощо) належить відповідний орган. Основним призначенням адміністративно-правового регулювання внутрішньоорганізаційних відносин необхідно вважати визначення внутрішніх структур та форм і методів взаємодії між ними в органах публічної влади та їх апаратах, які дозволяють реалізувати покладені на них завдання та функції [16; 108].

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. 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 [75].

1.2. Поняття адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України

Зміст і сутність механізмів забезпечення інформаційної безпеки, перш за все розкривається крізь призму дію тих чи інших нормативно-правових інструментів, що й є його складовими та забезпечують окремий, чітко впорядкований і конструктивно визначений алгоритм забезпечення відповідного вектору прав і свобод людини і громадянина. Відповідні права, що безпосередньо пов'язані з інформаційною безпекою суспільства загалом і Національної поліції України, складають основу правової державності та демократичності суспільства, корелюються зі світовими стандартами в указаній сфері та дозволяють забезпечити стає та безперешкодне функціонування суспільства.

Водночас, проблеми функціонування адміністративно-правових механізмів забезпечення інформаційної безпеки Національної поліції України з огляду на складність та важливість завдань, що визначаються перед нею, зокрема й в умовах дії правового режиму воєнного стану на території України, зумовлюють потребу надання розгорнутої характеристики вказаному інституту та врахувати всі, без

виключення обставини, що впливають на гальмування його діяльності та стають перешкодою в процесі становлення інституту прав і свобод людини і громадянина [153].

Крім цього, додатковим аргументом слугує введений у країні правовий режим воєнного стану та залученість Національної поліції України до заходів із відбиття збройної агресії росії проти нашої держави, що суттєво завантажує можливість ефективного виконання нею обов'язків і повноважень та релевантно потребує оптимізації основних управлінських і процедурно-компетенційний аспектів, пов'язаних із виконанням покладених завдань та реалізацією повноважень.

Добре організована праця впливає на моральну атмосферу колективу, розвиток соціальної та естетичної культури, а найголовніше — сприяє організованості, дисциплінованості особового складу, та є запорукою забезпечення особистої безпеки правоохоронців [115; 116; 119, с. 72].

Поширення інформаційного впливу через засоби масової інформації й мережу Інтернет на суспільну і індивідуальну свідомість для регулювання інформаційної, політичної, моральної, загальнокультурної поведінки громадян в кінцевому підсумку може призвести до серйозних наслідків як особистості, так і держави. Тому, рівень поінформованості суспільства є одним з критеріїв оцінки демократії, найважливішим чинником виживання в боротьбі за інформаційний суверенітет. У свою чергу, такі ознаки як конфіденційність, цілісність, доступність, достовірність і повнота інформації визначають якість управлінських рішень, що приймають органи державної та виконавчої влади [28, с. 87]. Таким чином, слід підкреслити, що адміністративно-

правовий механізм забезпечення інформаційної безпеки в Національній поліції України запобігає несанкціонованому та протизаконному поширенню інформації в діяльності відповідного центрального органу виконавчої влади та створює такі правові умови та обставини, що унеможливляють маніпулювання, викривлення та будь-які інші незаконні та протиправні дії пов'язані з інформацією.

Для того, аби розкрити поняття «механізм адміністративно-правового забезпечення кібернетичної безпеки людини», його основні ознаки, а також основні елементи (структуру), застосовуючи метод аналізу, розглянемо первинні базові поняття, зокрема «механізм», яке першопочатково виникло в обігу окремої науки – механіки. Згодом розвиток наукового знання призвів до того, що це поняття було запозичено іншими науками і, зрештою, поширилось на юридичні знання. Так, під механізмом у найбільш загальному значенні розуміють певний спосіб зробити щось у межах певної системи [152]. Аналогічно, застосовуючи визначені конструкції до надання характеристики поняттю адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України слід звернути увагу на те, що вказаний інститут комплексно забезпечує можливість здійснення відповідних обов'язків і повноважень та утворює необхідну адміністративно-правову конструкцію дотримання інформаційної безпеки в діяльності вказаного органу державної влади, що в свою чергу сприяє дотриманню прав і свобод людини і громадянина [134].

Для формування збалансованої державної політики та ефективного проведення комплексу узгоджених заходів щодо захисту національних інтересів в інформаційній сфері,

створення розвиненого і захищеного інформаційного середовища функціонує система інформаційної безпеки, складовими компонентами якої є: національні інтереси в інформаційній сфері, загрози та небезпеки цим інтересам, сама інформаційна безпека як інструмент зі створення сприятливих умов для їх реалізації, які в сукупності є об'єктом управління органами державного управління, система забезпечення інформаційної безпеки, тобто суб'єкт управління, основні напрями політики національної безпеки в інформаційній сфері, а також внутрішнє та зовнішнє середовище. Інформаційна безпека забезпечується комплексом заходів системи забезпечення національної безпеки України, що включає сукупність державних органів, громадських організацій, посадових осіб та окремих громадян [66, с. 108]. Тому, слід підкреслити, що вказані структурні компоненти адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України, перш за все виокремлюють його зміст і сутність, а також окреслюють поняття, як таке, що може застосовуватись не лише для подальших наукових пошуків, а й для розв'язання проблем практичного спрямування та забезпечення основних організаційно-управлінських процесів, пов'язаних із забезпечення інформаційної безпеки в Національній поліції України. Крім цього, зазначений адміністративно-правовий механізм, в свою чергу включає в себе також й інші структурні елементи, що чітко кореспондуються з його змістовним призначенням, що має враховувати, перш за все, завдання визначені для конкретного органу державної влади.

А.А. Дмитрієв зазначає, що побудова України як європейської та демократичної держави можлива за умови

забезпечення національної безпеки, що покладено саме на органи й підрозділи НП України [30], що також корелюється з позицією викладеною в дисертаційному дослідженні М.Ю. Романова, котрий звертає увагу, що неможливо здійснювати захист певних прав і свобод людини виключно окремими підрозділами Національної поліції України. Цей комплексний процес є взаємообумовленою діяльністю всіх структур й утворень, що спрямована на комплексне забезпечення прав і свобод людини та громадянина – усіх без винятку, зокрема громадян й осіб, яких підозрюють чи вже обвинувачено в учиненні кримінальних та адміністративних правопорушень. Такий зміст функціонування та основних напрямів діяльності як їх базових компонентів у кримінальній (адміністративній) процесуальній процедурі визначений змістом і спрямованістю прав людини [111; 118]. Одним із найбільш важливих аспектів є також скрупульозний та виважений підхід до класифікації її видів, що в свою чергу прямопропорційно впливає на змістовне наповнення тих чи інших нормативно-правових актів, що регулюють відповідний правовий режим та уможливають здійснення заходів забезпечення, як його правореалізації у вузькому розумінні, так і інформаційної безпеки в суспільстві загалом.

У правовій доктрині нині використовуються такі юридичні поняття, як-от: «механізм правового забезпечення», «механізм правового регулювання», «механізм адміністративно-правового забезпечення» тощо. Із аналізу наукових праць випливає, що нерідко «механізм правового забезпечення» та «механізм правового регулювання» ототожнюються. Наприклад, С.В. Діденко, розглядаючи поняття та елементи механізму адміністративно-правового забезпечення обігу та застосування зброї в Україні, зазначає,

що у зв'язку з тим, що адміністративно-правове забезпечення обігу та застосування зброї полягає у виявленні й створенні адміністративних засад та інструментарію реалізації адміністративно-правових відносин у цій сфері, а також охороні та гарантуванні прав, свобод і законних інтересів суб'єктів цих відносин на основі правових норм, механізм адміністративно-правового забезпечення потрібно розглядати через призму правового регулювання та брати його за основу під час формування відповідних висновків [29]. Проте, ми вважаємо, що базовим у даному відношенні є питання пов'язане зі змістовним наповненням терміну механізм, що в даному випадку розглядається як унормований у законодавстві України функціонал упорядкування суспільно-політичних відносин у певному сегменті права. Таким чином, характеризуючи поняття адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України слід звертати увагу на те, які саме структурні та змістовні компоненти його наповнюють, характеризують як організаційно-правове та адміністративно-управлінське явище.

Незважаючи на широке використання понять «інформаційна безпека» та «інформаційна безпека держави», на сьогодні відсутній однозначний підхід до визначення їх сутності. Крім того в законодавстві також не визначена норма, яка б містила дефініцію поняття «інформаційна безпека», при цьому інформаційна безпека розглядається лише як одна із сфер національної безпеки держави. Систематизація сучасних підходів до визначення сутності поняття «інформаційна безпека» дозволила зробити такі висновки: для розкриття сутності поняття «інформаційна безпека» використовуються такі поняття як «стан

захищеності», «стан інформації», «вид суспільних інформаційних правовідносин», «одна зі сторін розгляду інформаційних відносин у межах інформаційного законодавства» [32]. Відповідно, слід зауважити, що співвідношення понять інформаційна безпека та всі наукові й нормативно-правові підходи, які застосовуються до нього прямопропорційно впливають на можливість практичного застосування цих теоретичних конструкцій не лише на практиці, а й під час змістовного наповнення понятійно-категоріального апарату адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України. Таким чином, сутність поняття інформаційна безпека, наповнює якісними характеристиками механізм, що слугує для її забезпечення та організації відповідного правового режиму.

Варто розглянути співвідношення понять «інформаційна безпека» і «безпека інформації». Аналіз їх етимології дозволяє дійти висновку, що термін «інформаційна безпека» є ширшим, ніж «безпека інформації». Інформаційну безпеку України можна розглядати з позицій захисту інтересів держави, особистості й суспільства. Загрозами цій безпеці є не тільки «стан захищеності інформації», але й вияви обмеження свободи слова та доступу до публічної інформації, поширення засобами масової інформації культу насильства, жорстокості, порнографії, намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації [77; 103].

Цікавим на наш погляд є підхід Р. В. Ігоніна стосовно розкриття змісту поняття «адміністративно-правового забезпечення». Так, він вважає, що адміністративно-правове забезпечення функціонування системи судів загальної

юрисдикції – це регламентована адміністративно-правовими нормами діяльність суб'єктів державно-владних повноважень, яка спрямована на створення необхідних умов для належного функціонування системи судів загальної юрисдикції та встановлена адміністративно-правовими нормами система гарантій належного функціонування системи судів загальної юрисдикції [46]. Таким чином, можна попередньо обґрунтувати думку про те, що адміністративно-правовим механізмом забезпечення інформаційної безпеки в Національній поліції України є комплекс норм права, що формують зміст компетенції відповідних суб'єктів, щодо недопущення несанкціонованого (незаконного) використання інформації, що не перебуває в публічному просторі чи під дією будь-яких інших режимних обмежень, що можуть поставити під сумнів правомірність таких дій.

Безпека інформації є певним станом, за якого забезпечуються її цілісність, недоторканність при збереженні, використанні чи розповсюдженні. Безпеку інформації можна забезпечити шляхом обмеження доступу (випадкового або несанкціонованого) суб'єктів, які не мають на це права. У такому випадку забезпечення безпеки інформації є складником загальної інформаційної безпеки. Забезпечуючи, наприклад, безпеку інформації про конкретну особу, про діяльність органів влади, ми забезпечуємо політику інформаційної безпеки держави в особі відповідних суб'єктів [77]. Слід погодитись, на нашу думку, адже в указаному випадку, реалізації загальнодержавного вектору інформаційно-безпекової політики проявляється, зокрема в діяльності Національної поліції України, як держателя низки реєстрів, що містять персональні дані громадян на законних засадах, а також органу, посадові особи якого уповноважені

на здійснення адміністративного чи кримінального провадження, реалізацію адміністративно-юрисдикційних й інших повноважень, пов'язаних із роботою з інформацією інших осіб і громадян.

На думку вчених, термін «забезпечення» визначає дію, діяльність. Відповідно, коли мова йде про певне забезпечення (в нашому випадку інформаційне), то слід мати на увазі передусім діяльність певних суб'єктів, або комплекс засобів, дій, які визначають діяльність суб'єктів в інформаційній сфері. Стосовно нашого дослідження об'єктом забезпечення є інформація, інформаційна безпека, тому аналіз праць науковців, які досліджували цю категорію в контексті поняття «інформаційне забезпечення», «правове забезпечення інформаційної діяльності» дозволив зробити узагальнення стосовно того, що інформаційне забезпечення науковцями розглядається як діяльність (сукупність певних дій, управлінських рішень) [141], яка реалізується певними способами та методами, що спрямовані на збирання, реєстрацію, передачу, зберігання, опрацювання, аналіз, поширення та обробку інформації. Така діяльність охоплює надходження, рух та перетворення інформації, методи її зберігання та передавання [32].

Повноваження поліції України в забезпеченні інформаційної безпеки держави (як одного із напрямів державної інформаційної політики) зумовлюються кількома факторами: місцем Національної поліції в системі правоохоронних органів загалом і у системі органів внутрішніх справ зокрема; характером виконуваних завдань; структурою Національної поліції та системою органів і підрозділів Національної поліції, яка є суттєво оновленою порівняно зі структурою міліції та більш пристосованою до

протидії сучасним загрозам інформаційній безпеці людини, суспільства та держави загалом; специфікою форм забезпечення інформаційної безпеки: правова (або законодавча) та технічна; необхідністю дотримання прав і свобод людини та громадянина одночасно із застосуванням заходів щодо забезпечення інформаційної безпеки [77]. Таким чином, враховуючи вказані нормативні конструкції, слід зауважити, що поняття адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України набуває додаткових конструктивних особливостей, в умовах функціонування зазначеного центрального органу виконавчої влади. Перш за все, вказаний механізм має містити забезпечувальні елементи, що спрямовані не лише на теоретико-правову регламентацію тих чи інших повноважень, а й забезпечувати реалізацію вказаних положень та уможливлювати здійснення їх на практиці.

У своїх працях український вчений І. Голосніченко визначає механізм правового регулювання як систему взаємозв'язаних і взаємозумовлених елементів, які поділяються на три групи: засоби впливу, проміжні ланки й об'єкти впливу. До першої з них входять правові принципи, норми, джерела права, правовідносини. До другої – правосвідомість, правова культура; до третьої – акти реалізації норм [23, с. 44].

Третім і найважливішим елементом механізму адміністративно-правового забезпечення інформації з обмеженим доступом у Національній поліції є форми та методи управлінської діяльності уповноважених суб'єктів щодо обігу цієї інформації. Класифікація форм управління в адміністративно-правовій літературі здебільшого

здійснюється за виникненням певних наслідків. Тому їх частіше поділяють на правові та неправові. Правові форми – це видання юридичних актів, застосування примусових заходів, які виступають як юридичні факти і можуть породжувати (змінювати, припиняти) адміністративно-правові відносини. До неправових належать форми, які безпосередньо юридичного значення не мають, тобто не спричиняють виникнення конкретного юридичного результату. Це такі дії як організація та проведення нарад, обговорень, перевірок, розробка проєктів планів, прогнозів, програм, методичних рекомендацій, здійснення заходів щодо підвищення якості та ефективності управлінської праці [3, с. 278]. Відповідно, правові форми, на нашу думку, є одним із найбільш важливих елементів адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України, оскільки у спосіб їх реалізації досягається результативний та змістовний захист відповідного правового режиму. Крім цього, через визначення змісту і сутності правових форм, а також неправових проявів функціонування будь-якого іншого адміністративно-правового механізму можливим є встановлення його поняття, а також змістовного наповнення, що в подальшому пропорційно впливає на можливість забезпечення відповідних прав і свобод людини і громадянина.

Стратегічною метою забезпечення інформаційної безпеки є досягнення такого розвитку економіки, внаслідок якого були би забезпечені оптимальні умови для життя і розвитку особистості, соціально-інформаційної та військово-політичної стабільності суспільства і збереження цілісності держави, успішного протистояння впливу зовнішніх і

внутрішніх загроз. Державна стратегія інформаційної безпеки країни повинна бути орієнтована, перш за все, на підтримку достатнього рівня виробничого, науково-технічного потенціалу; недопущення зниження рівня життя населення до граничних значень, порушення яких спроможне викликати соціальну напруженість; упередження конфліктів між окремими верствами і групами населення, окремими націями [32]. Саме тому, дія адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України має перш за все спиратися на норми і положення законодавства України в загальнодержавному масштабі, щодо забезпечення інформаційної безпеки українського суспільства. Поняття зазначеного адміністративно-правового механізму витікає із доктринальних положень національного законодавства, де визначається зміст і сутність інформаційної безпеки, а також конкретний перелік адміністративних заходів способів методів і форм забезпечення дотримання інформаційної безпеки, як на загальнодержавному так і на інших рівнях, а також окреслюється вичерпне коло суб'єктів його реалізації.

Багато дослідників до елементів механізму адміністративно-правового забезпечення відносить норми адміністративного права, акти реалізації норм адміністративного права, правові відносини або розглядає його як систему заходів у трьох напрямках: регулювання, охорона та захист. Вважаємо, що такий підхід може бути розширений. По-перше, суспільні відносини не є елементом цього механізму, вони – об'єкт впливу, саме ці відносини має впорядковувати відповідний механізм. Такі відносини пов'язані зі здійсненням публічного управління економічною, соціально-культурною та адміністративно-політичною

сферами життя, а також забезпеченням реалізації та захистом прав, свобод і законних інтересів фізичних та юридичних осіб. По-друге, метод адміністративного права базується на відносинах субординації між учасниками суспільних відносин, а це є ознакою так званого імперативного методу регулювання (або методу владних приписів чи влади-підпорядкування) [6, с. 31]. Таким чином, поняття адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України охоплює собою комплекс нормативно визначених структурно-правових компонентів, що уможливорюють здійснення та реалізацію заходів, щодо забезпечення всього, без виключення суспільства від протиправних і неправомірних дій з інформацією різного рівня та масштабу, що впливає, як на інтереси кожного громадянина окремо, так і на загальнодержавний стан дотримання засад і принципів інформаційної безпеки. Тобто, адміністративно-правовий механізм забезпечення інформаційної безпеки в Національній поліції України включає в себе адміністративно-правові інструменти регулювання, охорони та захисту правового режиму обігу інформації.

Щодо структури адміністративно правового механізму, то заслуговує на увагу підхід, запропонований О. Мурашиним, який називає три основних, кілька допоміжних і цементуючий елементи механізму правового регулювання. До основних він відносить: юридичну норму, правовідносини, реалізацію учасниками правовідносин їх суб'єктивних прав і обов'язків. До допоміжних відносить акти застосування права, а нормативною основою вищевказаного механізму називає систему правових норм, при цьому певну роль відводить підзаконним актам,

пояснюючи це тим, що законодавець не може приймати правові норми з таким ступенем деталізації, який гарантував би можливість регулювання всіх суспільних відносин [4, с. 70]. Таким чином, до кола компетенції Національної поліції України у сфері забезпечення реалізації адміністративно-правового механізму інформаційної безпеки відноситься не лише поточна координація загальних внутрішньо інформаційних процесів, а й визначення чіткого кола норм, які врегульовуватимуть зазначені правовідносини, а також участь в їх перебігу, що включає в себе як статичну (формально-юридичну) так і динамічну (процесуальну) адміністративну складові. Тобто, поняття адміністративно-правового механізму забезпечення інформаційної безпеки передбачає, перш за все не лише нормативно-правовим змістом (що і слугує підґрунтям для його реалізації), а й організаційно-правовим, що включає в себе процедурно-управлінський аспект.

Діяльність поліції, пов'язана із захистом і обробкою персональних даних, здійснюється на підставах, визначених Конституцією України, Законом України «Про захист персональних даних». Поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади з обов'язковим дотриманням Закону України «Про захист персональних даних». Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав доступ, та про обсяг даних, доступ до яких було отримано. Кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів фіксується у спеціальному електронному архіві, ведення якого

покладається на службу інформаційних технологій Міністерства внутрішніх справ України [77]. Таким чином, поняття адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України має містити не лише окремі, загальноправові особливості, а й ті, що безпосередньо відносяться й можуть бути застосовані в умовах особливостей компетенції професійної діяльності кожного поліцейського та Національної поліції України загалом. Наявність розширеного доступу кожного працівника поліції до певного виду (типу) інформації, що може складати предмет і об'єкт адміністративно-правового механізму забезпечення інформаційної безпеки в широкому розумінні, а також у контексті діяльності Національної поліції України, на нашу думку, значно розширює зміст і сутність поняття адміністративно-правового механізму інформаційної безпеки в діяльності Національної поліції України.

Нормативно-правовий блок адміністративно-правового механізму забезпечення інформаційної безпеки держави включає сукупність нормативно-правових актів, які створюють правові умови для забезпечення інформаційної безпеки, а саме правові норми, за допомогою яких здійснюється закріплення повноважень, які покликані забезпечувати інформаційну безпеку в державі, зміна чи скасування окремих нормативно-правових актів, визначення сфери їх дії та кола учасників і прийняття індивідуальних рішень на основі загальних правил для вирішення конкретних юридичних ситуацій. Значення нормативно-правового блоку полягає в тому, що саме він дає механізму забезпечення інформаційної безпеки держави юридичну форму та «правове життя» [32]. Відповідно належить підкреслити, що зміст і сутність поняття адміністративно-правового механізму

забезпечення інформаційної безпеки в діяльності Національної поліції України має бути насичена такими юридичними категоріями, як нормативна врегульованість та чіткість юридичної форми, що в умовах дії норм законодавства та режиму правової держави, де всі члени суспільства зобов'язані виконувати визначення законодавства принципи, дозволить забезпечити ефективність сталість та справедливість дії вказаної юридичної інституції та відповідного центрального органу виконавчої влади не порушуючи права і свободи інших людей.

Орієнтуючись на своє авторське поняття механізму адміністративно-правового забезпечення кібернетичної безпеки людини, до його основних елементів М.В. Плєскач відносить: нормативні засади механізму адміністративно-правового забезпечення кібернетичної безпеки людини (принципи права, норми права); об'єкт адміністративно-правового забезпечення кібернетичної безпеки людини (правовідносини, їх зміст, види, структуру та особливості реалізації); суб'єктів адміністративно-правового забезпечення кібернетичної безпеки людини; засоби адміністративно-правового забезпечення кібернетичної безпеки людини [89, с. 202]. Відповідно, слід погодитись із авторитетним дослідником та констатувати, що зміст і сутність поняття будь-якого адміністративно-правового механізму не може обходитись без надання характеристики його ознакам, що власне і складають окремі юридичні аспекти та вектори подальшої реалізації та втілення в життя відповідного адміністративно-управлінського інструменту, котрий слугує для забезпечення регламентованого законодавством України правового режиму та з метою забезпечення прав і свобод

людини і громадянина у конкретному сегменті суспільно-правових відносин.

Як зазначає О. Саєнко, в основі системи зміцнення інформаційної безпеки країни лежить відповідний її механізм, який складається із взаємопов'язаних та взаємодіючих складових: нормативно-правових; інституційно-організаційних; кадрових; інформаційно-аналітичних [5, с. 20]. Зазначену структуру уточнює М.М. Присяжнюк, який пропонує до структури адміністративно-правового механізму забезпечення інформаційної безпеки держави включити такі блоки з наступним змістом: нормативно-правовий (сукупність норм права і нормативно-правових актів, юридичні факти); інституційно-організаційний (система уповноважених органів управління у сфері забезпечення інформаційної безпеки); процедурно-функціональний (принципи і інструменти, методи регулювання, а також процедури і алгоритми реалізації діяльності з забезпечення інформаційної безпеки, включаючи техніки і технології управління); забезпечувальний (кадрове, інформаційне, матеріально-технічне забезпечення); інформаційно-аналітичний (аналіз стану розвитку і існування об'єкта забезпечення) [93, с. 43]. Відповідно, можливо буде підкреслити, що до кола структурних особливостей поняття адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України необхідно віднести такі властиві йому характеристики, як нормативно-правова врегульованість, інституційно-організаційна форма, кадрове (суб'єктне) наповнення та інформаційно-аналітична підтримка. Значення структурні компоненти будучи чітко інтегрованими у механізмі діяльності Національної поліції

України, як одного з центральних органів виконавчої влади до кола компетенції якого віднесене забезпечення правопорядку, а також прав і свобод людини і громадянина уможливають не лише формальне приведення в дію адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України під час виконання нею покладених законодавством України обов'язків, а й фактично забезпечить високоякісне підтримання правового режиму безпеки інформації під час здійснюваної діяльності.

До правоохоронних повноважень поліції щодо забезпечення інформаційної безпеки держави можна віднести здійснення превентивної та профілактичної діяльності, спрямованої на запобігання вчиненню правопорушень у сфері інформації; виявлення причин та умов, які сприяють вчиненню кримінальних та адміністративних правопорушень у сфері інформації, вжиття в межах своєї компетенції заходів для їх усунення; вжиття заходів з метою виявлення кримінальних, адміністративних правопорушень у сфері інформаційної безпеки; вжиття заходів, спрямованих на усунення загроз життю та здоров'ю фізичних осіб і публічній безпеці, які виникли внаслідок вчинення кримінального, адміністративного правопорушення у сфері інформаційної безпеки; здійснення досудового розслідування кримінальних правопорушень у сфері інформації та інформаційної безпеки в межах визначеної підслідності; розшук осіб, які переховуються від органів досудового розслідування, слідчого судді, суду, які вчинили зазначені вище правопорушення; у випадках, визначених законом, здійснення проваджень у справах про адміністративні правопорушення у сфері інформації, приймає рішення про

застосування адміністративних стягнень, забезпечує їх виконання [77]. Таким чином, на нашу думку, поняття адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України слід поділити на декілька структурних компонентів, один з яких відноситься до реалізації вказаного механізму у внутрішньоуправлінських взаєминах Національної поліції України, а другий, в свою чергу, пов'язати зі змістом і сутністю здійснюваної нею правоохоронної діяльності, у сфері захисту прав і свобод людини і громадянина в межах визначеної законодавством України компетенції.

Таким чином, більшість науковців зійшлися на тому, що структурними елементами механізму адміністративно-правового регулювання, у тому числі механізму забезпечення інформаційної безпеки, є: правові норми, правовідносини, акти реалізації норм права та акти тлумачення правових норм. Деякі науковці до вказаної структури додають ще такі явища, як нормативні акти, юридичні факти, суб'єктів та об'єктів впливу, принципи та інструменти, методи регулювання, діяльність, спрямовану на забезпечення інформаційної безпеки та процедури і алгоритми її реалізації, а також техніки і технології управління; організаційні структури і управлінський персонал; відповідне забезпечення (політичне, правове, інформаційне тощо) [32]. Тому, на нашу думку, доцільним, у наступному підрозділі дослідження буде надання вичерпної характеристики структурним елементам адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України. Крім цього, чільно підкреслити, що без належної нормативно-правової регламентації в даному механізмі, унеможлиблюється взагалі його існування та можливість

здійснення повноважень та обов'язків у відповідній сфері, що в свою чергу може потягнути суттєві порушення прав і свобод людини і громадянина інформаційної спрямованості та суттєво погіршити рівень демократичності держави.

З огляду на наведене механізм адміністративно-правового забезпечення інформації з обмеженим доступом в органах поліції – це врегульована нормами адміністративного права діяльність поліції України та інших органів влади щодо обігу інформації, яка перебуває в законному володінні або розпорядженні поліції, відносно доступу до якої встановлюється законодавче обмеження в інтересах забезпечення публічної безпеки та порядку, протидії злочинності, охорони прав і свобод людини, інтересів суспільства і держави, розголошення якої може завдати істотної шкоди цим інтересам, а оприлюднення переважає суспільний інтерес у її отриманні. До елементів механізму адміністративно-правового забезпечення інформації з обмеженим доступом в органах поліції можна віднести адміністративно-правові норми, закріплені у відповідних актах органів влади [77]. Саме тому, на нашу думку слід виокремити розуміння поняття адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України, як цілісного комплексу адміністративно-правових норм, що мають чітко визначену структуру та комплекс компетенційних характеристик і спрямовані на забезпечення дії такого правового становища, в якому неможливим є вчинення будь-яких незаконних (протиправних) дій із інформацією інших осіб, що використовується в діяльності Національної поліції України та в свою чергу сприяє посиленню інституційної спроможності цього органу державної влади до законного та

ефективного забезпечення дотримання прав і свобод людини і громадянина [131].

1.3. Структура адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України

Адміністративно-правове регулювання діяльності Національної поліції України в умовах дії правового режиму воєнного стану суттєво трансформувалось, з урахуванням сучасних безпекових вимог та обставин, що висувують нові соціально-правові реалії у відносинах всередині суспільства. В свою чергу, зазначені особливості та законодавчі й організаційно-управлінські новели мають, свої переваги та недоліки котрі можуть позитивно чи негативно впливати на основні аспекти функціонування як всієї національної поліції України так і діяльності за окремими напрямками. Стрімкість законодавчих змін, що відбуваються в колі нормативно-правового забезпечення функціонування Національної поліції України, як одного з центральних органів виконавчої влади, що забезпечує дотримання прав і свобод людини і громадянина, а також правопорядок у суспільстві, зумовлюється динамікою трансформації суспільно-правових відносин котрі, в свою чергу, безпосередньо залежать від плину та активності бойових дій, що відбуваються на території України, а також інших видів заходів забезпечення відсічі збройної агресії російської федерації.

Саме тому, надання змістовної та вичерпної оцінки всім перевагам та недолікам адміністративно-правового

регулювання діяльності Національної поліції України в умовах дії правового режиму воєнного стану, зокрема в частині забезпечення дотримання прав і свобод людини і громадянина та створення й підтримання атмосфери правопорядку в суспільстві, є одним із пріоритетних завдань цього дослідження й має бути проаналізовано якомога більш комплексно та структуровано. Крім цього, співвідношення інструментів адміністративно-правового регулювання правового статусу людини і громадянина та його взаємодії із суб'єктами органів державної влади, а також самого органу державної влади, так само складають об'єкт і предмет наукового інтересу, в контексті окресленого дослідження, оскільки вони є взаємозалежними з точки зору виконання поліцією покладених на неї функцій та обов'язків [162].

Сфера діяльності органів внутрішніх справ має складну структуру яка створюється державою для забезпечення прав і свобод людини та громадянина. Вона має в собі ряд груп суспільних відносин, які пов'язані із забезпеченням прав і свобод людини, убезпечення держави і суспільства від злочинів, інших посягань, соціальних загроз та визначає різні напрями діяльності органів внутрішніх справ в сфері реалізації основних прав людини і громадянина. Особливе місце серед завдань правоохоронної діяльності посідає захист прав та свобод людини, її життя, здоров'я, честі, гідності, недоторканності та безпеки [115, с. 178]. Така діяльність базується на загальновизначених європейських стандартах, а тому при виконанні своїх обов'язків поліція повинна дотримуватись індивідуальних прав громадян, включаючи права і свободи людини, та не вчиняти свавільних або протиправних дій. Це є основоположним для розуміння верховенства права щодо значущості і для мети діяльності

поліції в демократичній державі [155, с. 25]. Безперечно позитивним аспектом адміністративно-правового регулювання діяльності Національної поліції України в умовах дії правового режиму воєнного стану є широко застосована практика використання загальних принципів і завдань діяльності, відповідним центральним органом виконавчої влади, в умовах відсутності чіткого законодавчого регулювання окремих напрямів і спектрів діяльності поліції. Водночас, враховуючи практику здійснення поліцейськими окремих видів повноважень за конкретними завданнями, що виникли під час ліквідації наслідків збройної агресії, а також кроки, щодо поновлення порушених прав і свобод людини і громадянина, в результаті дій агресора, мають бути сформовані логічні законодавчі пропозиції, щодо чіткого нормування а також визначення механізму стримування противаг у поліцейській діяльності за вказаним напрямом.

На сучасному етапі функціонування Національної поліції України надзвичайно важливим є питання пов'язане з нормативно-правовим забезпеченням її діяльності в умовах змінюваних соціальних потреб, що зумовлюються, перш за все швидким плином бойових дій.

Питання пов'язані з діяльністю Національної поліції України в межах заходів відсічі збройній агресії росії проти України, мають бути врегульовані на рівні законодавства України, оскільки всі органи державної влади, діють виключно в межах і у спосіб визначені законодавством України, що унеможливує її діяльність за принципом «можна все, що не заборонено» й зобов'язує діяти виключно так, як прямо вказано законодавством України.

Варто відзначити, що в умовах введення воєнного стану особливого значення набуває завдання забезпечення прав і

свобод людини і громадянина. Безумовно, коли нормальне функціонування держави і суспільства стає неможливим, окремі права і свободи людини і громадянина зазнають певних обмежень. При цьому, застосовуючи обмеження прав і свобод людини, кожна країна керується нормами статті 29 Загальної декларації прав людини, якою передбачено, що при здійсненні прав і свобод кожна людина повинна зазнавати тільки таких обмежень, які встановлено законом виключно з метою забезпечення належного визнання і поваги прав і свобод інших та забезпечення справедливих вимог моралі, громадського порядку і загального добробуту в демократичному суспільстві [87]. Відповідно, слід зауважити, що зміст функціонування Національної поліції України безпосередньо полягає в необхідності коригування відповідних функціональних компонентів, релевантно із потребами суспільства та в умовах необхідності закріплення відповідних елементів у структурі правового статусу вказаного органу державної влади в нормативно-правовий (законодавчий) спосіб.

На погляд науковців, внутрішньоорганізаційні відносини в органах публічної влади слід розглядати як окрему складову предмета адміністративного права, яка має особливий характер. Специфічна риса цієї групи відносин полягає в тому, що вони існують та регулюються переважно на єдиних базових засадах незалежно від того, до якої підсистеми публічної влади (державна влада або місцеве самоврядування) або до якої складової державної влади (законодавча, виконавча, судова гілка тощо) належить відповідний орган. Основним призначенням адміністративно-правового регулювання внутрішньоорганізаційних відносин необхідно вважати визначення внутрішніх структур та форм і

методів взаємодії між ними в органах публічної влади та їх апаратах, які дозволяють реалізувати покладені на них завдання та функції [16; 131].

Низка вчених і дослідників, спираючись на норми Закону України «Про правовий режим воєнного стану» надають таке визначення поняттю «воєнний стан» [123]: «це особливий правовий режим, що вводиться в Україні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності та передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень» [149]. Відповідно, підвищення соціальної напруги та потреба забезпечення більш глибокого та змістовного дотримання прав і свобод людини і громадянина не лише в контексті внутрішнього правопорядку, а й у розрізі убезпечення осіб і громадян від негативних наслідків збройної агресії рф потребує внутрішнього перерозподілу функцій і обов'язків органів і підрозділів Національної поліції України, а також додаткового наукового опрацювання проблемних питань функціонування зазначеного центрального органу виконавчої влади. Саме тому, над актуальним питанням є необхідність удосконалення організаційного та структурно-функціонального аспектів діяльності Національної поліції

України крізь призму викликів військової агресії та активних євроінтеграційних намагань, що співмірно впливають на внутрішньодержавну безпекову політику.

Адміністративно-правове забезпечення правового режиму воєнного стану в умовах повномасштабного збройного конфлікту в Україні науковці пропонують розглядати у двох варіаціях: 1) як процес встановлення засад його функціональності, що репрезентується нормативним базисом для: відсічі збройній агресії; захисту національних інтересів і цінностей України; 2) як самостійний різновид діяльності органів державної влади, що передбачає втілення в правореалізацію охоронних, захисних, регулятивних та організаційних дій, спрямованих на виконання завдань правового режиму воєнного стану в умовах його введення [9]. Відповідно, належить підкреслити, що сучасний процес діяльності Національної поліції України так само характеризується наявністю двох аспектів: зовнішньоорганізаційного, що має чітке нормативне окреслення, а також внутрішньоуправлінського, що має обмежене організаційно-розпорядче закріплення. Ці інструменти, тією чи іншою мірою забезпечили поточну оптимізацію процесу діяльності відповідного центрального органу виконавчої влади, а також створили підґрунтя для подальшого пошуку шляхів трансформації його функціонування з урахуванням потреб суспільства та внесених у відповідні нормативно-правові акти змін.

Діяльність органів поліції під час дії правового режиму воєнного стану, на відміну від мирного часу, корегується залежно від тих завдань, що ставляться перед ними державою з метою протидії внутрішнім загрозам воєнного стану. Завдання та функції правоохоронних органів, у тому числі і

органів Національної поліції можуть коригуватися відповідно до вимог, що висуваються у конкретний період до цих органів, та з урахуванням загроз та небезпек, які на даний момент стоять на шляху до реального забезпечення законності та правопорядку в державі. Слід звернути увагу, що діяльність органів поліції в умовах правового режиму воєнного стану ускладнюється тим фактом, що поліцейські виконують покладені на них обов'язки в умовах підвищеного ризику, що одночасно супроводжується суттєвим емоційним хвилюванням [2]. Так, покладання обов'язків на поліцію, щодо здійснення досудового розслідування в складі спільних міжвідомчих слідчих груп (спільно зі Службою Безпеки України), а також додаткових обов'язків щодо роботи за напрямом призову на військову службу під час мобілізації (спільно з військовослужбовцями Збройних сил України) суттєво завантажило роботу, як слідчого апарату та патрульної поліції так і всіх інших структурних підрозділів загалом. Так, для більш якісного опрацювання цього питання та винесення низки пропозицій до законодавства України в сфері поліцейської діяльності слід виокремити окремі особливості, що були інтегровані в нормативно-правове забезпечення в період дії воєнного стану на території України.

До прикладу, статтю 8 Закону України «Про Національну поліцію» доповнено частиною четвертою, яка передбачає, що під час дії воєнного стану поліція діє згідно з призначенням та специфікою діяльності з урахуванням тих обмежень прав і свобод громадян, а також прав і законних інтересів юридичних осіб, що визначаються відповідно до Конституції України та Закону України «Про правовий режим воєнного стану» [122], що екзистенційного розширило

межі повноважень Національної поліції та уможливило внесення подальших змін до відповідного нормативно-правового комплексу в частині розширення кількості й різноманіття способів, методів і засобів у поліцейській діяльності з метою забезпечення правопорядку та дотримання прав і свобод людини і громадянина.

Крім цього, належить також зауважити на тому, що внесені до Законів України «Про Національну поліцію» та «Про Дисциплінарний статут Національної поліції України» зміни, що спрямовані на оптимізацію діяльності поліції під час дії воєнного стану діють тимчасово, на зазначений період введення в Україні воєнного стану, здійснення заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії РФ та/або інших держав проти України та 60 днів після цього. Аналогічними є конструкції, щодо застосування заохочень в поліції та можливість присвоєння чергового спеціального звання без встановлення термінів, достроково та на один ступінь вище від звання, передбаченого займаною штатною посадою, що позитивно впливає на адміністративно-управлінські спроможності керівництва Національної поліції України та відповідних органів і підрозділів поліції.

Загострення політичної ситуації, в останні роки, призвело до виведення даної проблеми на перші щаблі. У зв'язку з переходом країни на європейський шлях розвитку і зміни пріоритетів в діяльності з колишньої «міліції» в органи Національної поліції, переорієнтація їх на виконання функцій соціально-правового обслуговування населення. В даний час вирішити ці завдання можливо за умови пильної уваги керівництва Національної поліції до кадрової політики. З точки зору системного підходу до управління вона

розглядається в двох значеннях — зовнішньому і внутрішньому. Зовнішній аспект управлінської діяльності пов'язаний із здійсненням широкого комплексу функцій органу управління виходячи з його соціального призначення. Внутрішній характеризує її як власне управлінську працю, що виражається в реалізації функцій органу шляхом законодавчо визначеного впливу у внутрішньому функціонуванні середовища [136; 181].

О.С. Юнін, посилаючись на законодавство слушно зауважує, що серед завдань таких формувань у взаємодії з Національною поліцією: брати участь у здійсненні заходів щодо тимчасової заборони або обмеження руху транспортних засобів і пішоходів поблизу та в межах зон/районів надзвичайних ситуацій та/або ведення воєнних (бойових) дій разом з Національною поліцією; брати участь у забезпеченні заходів громадської безпеки і порядку в населених пунктах разом з Національною поліцією [112; 182]. На цьому прикладі дослідники вказують на особливості у взаємодії Національної поліції в питаннях забезпечення громадської безпеки і порядку, роботи на блокпостах тощо разом з воєнізованими підрозділами за умов національного спротиву, руху опору і воєнного стану. Так, в умовах запровадження воєнного стану поліцейські беруть участь у забезпеченні громадської безпеки і порядку в особливих умовах несення служби — це діяльність під час комендантського часу, коли відбуваються активні бойові дії (в рамках процесу деокупації територій); пошук зазначених вже диверсійних груп тощо. І все це відбувається у взаємодії з підрозділами, наприклад, Національної гвардії України, добровольчими формуваннями територіальних громад тощо [8, с. 226]. Крім зазначеного слід зауважити на тому, що не лише поліцією забезпечується дотримання

належного правового режиму на прилеглий до лінії бойового зіткнення території, а надання дозволу на перетин блокпостів, наближених до зазначеної території відноситься до компетенції Збройних сил України, тому необхідність налагодження ефективної взаємодії поліцейських, що виконують правоохоронні функції у вказаних районах є безперечною. При цьому, та значна частина поліцейських, що беруть безпосередню участь у забезпеченні відсічі збройної агресії росії проти України також потребують, в даному контексті, належного правового захисту та відлагодження системи взаємодії з підрозділами, силами та засобами військовослужбовців Збройних сил України, Національної гвардії України, Державної прикордонної служби України тощо.

За твердженням Т. Гоббса, цінність збереження держави перевищує її недоліки, оскільки «скасування істотних прав верховної влади спричинило б розпад держави й повернення кожної людини до стану й нещастя війни всіх проти всіх (що було б найбільшим з усіх нещастя, які можуть статися в її житті), тому обов'язок суверена – утримати за собою ці права в повному обсязі. Отже, суверен чинить проти обов'язку, коли поступається іншому або зрікається будь-якого з цих прав... І хоча люди можуть уявляти, що така необмежена влада повинна вести до багатьох нерозумних наслідків, однак відсутність такої влади, а саме невпинна війна всіх проти всіх, веде до значно гірших наслідків. Стан людини в такому житті ніколи не буде вільним від негод, але найбільші негоди, які існують у будь-якій державі, завжди виникають через непокору підданих і через порушення договорів, від яких держави беруть свій початок. А якщо будь-хто, гадаючи, що верховна влада занадто велика, побажає обмежити її, то він

повинен буде підкоритися владі, що може її обмежити, тобто визнати над собою більшу владу» [43, с. 105–106]. Наведена ідея взаємної відповідальності держави і особи в європейський політико-правовій думці за авторства О.Р. Дашковської чітко демонструє, що перевагою чіткого адміністративно-правового регулювання діяльності органів правопорядку, зокрема в умовах, коли можуть бути введені тимчасові обґрунтовані обмеження прав і свобод людини і громадянина, на період особливого часу, що об'єктивно спричиненим широкомасштабною збройною агресією, є об'єктивна та чітко визначена обмеженість повноважень та меж компетенції силових структур у взаєминах із представниками суспільства.

Враховуючи вищезазначене можна дійти висновку, що поліція не є воєнізованим формуванням, і виконує лише виключно сервісні функції щодо надання населенню відповідних послуг, які належать до сфери її діяльності. Таким чином, поліція здійснюючі покладені на неї державою функціональні обов'язки, відіграє ключову роль у підтриманні високого рівня правопорядку і законності в державі, що в свою чергу є важливою гарантією забезпечення прав і свобод людини та громадянина [65]. При цьому, слід підкреслити, що міра застосування принципу верховенства права під час здійснення правоохоронної діяльності, в залежності від конкретного напрямку такої діяльності та відповідного структурного підрозділу різниця, що перш за все, може стати предметом адміністративно-правового регулювання у внутрішньо-організаційних управлінських відносинах, а також під час конкретного здійснення визначених поліцейських функцій. З позитивної точки зору слід характеризувати застосування принципу, за яким

поліцейський зобов'язаний діяти виключно так, як прямо передбачено у законодавстві України, що в свою чергу убезпечує суспільство та конкретно взятих осіб від свавілля та необґрунтованого застосування державного примусу представника органу державної влади.

Захист прав і свобод людини та громадянина, інтересів суспільства та держави є пріоритетним у діяльності цього правоохоронного органу. З огляду на це гарантування прав людини має переважати у відносинах держави і громадянина, всі функції, які здійснює країна, мають бути направлені на охорону інтересів людини, на забезпечення та захист її прав, свобод та законних інтересів. Так, діяльність поліції має забезпечувати на відповідному рівні: законність та правопорядок, гарантувати права, свободи людини, інтереси суспільства та держави загалом [178, с. 14]. В разі використанні працівниками поліції певних заходів, передбачених їхніми повноваженнями, важливо розуміти, що права людини представляють собою імперативний формат, оскільки, отримуючи закріплення у правових нормах, які прописують можливі варіанти поведінки поліцейських, права людини стають правилом, формально визначеним, обов'язковим для всіх, гарантованим відповідними механізмами забезпечення і процедурами захисту [34, с. 49]. Водночас, на нашу думку, необхідно деталізувати позицію автора в тій частині, що кожна особа визначає для себе міру можливої та належної поведінки, з урахуванням тих обмежень, що прямо зазначаються в законодавстві України, у той час як суб'єкти органів державної влади зобов'язані діяти виключно так, як прямо передбачає вказане нормативно-правове коло, що в свою чергу може характеризуватися, як позитив, з точки зору забезпечення дотримання прав і свобод

людини і громадянина та неможливості необґрунтованого обмеження прав, навіть в умовах дії правового режиму воєнного стану, так і як негатив, крізь призму обмеженості адміністративно-правового інструментарію забезпечення прав і свобод людини і громадянина від протиправних посягань та незаконних прецедентів [167].

Здійснюючи свою діяльність поліція повинна застосовувати принцип поваги до гідності, а також недопущення катування або іншого поводження чи покарання, що принижує людську гідність. Жоден службовець органів правопорядку не повинен чинити, підбурювати або терпимо ставитися до будь-якої форми катування або іншого жорстокого, нелюдського або такого, що принижує гідність, поводження чи покарання, а також жоден службовець органів правопорядку не повинен посилалися на розпорядження керівництва або такі виняткові обставини, як військовий стан чи загроза війни, загроза національній безпеці, внутрішня політична нестабільність чи будь-яке інше надзвичайне становище, для виправдання катувань або іншого жорстокого, нелюдського або такого, що принижує гідність, поводження чи покарання. Згідно п. 3 Резолюції Парламентської Асамблеї Ради Європи «Про Декларацію про поліцію» № 690 зазначено, що масові страти, катування та інші форми нелюдського або такого, що принижує гідність, поводження чи покарання заборонені за будь-яких обставин. Офіцер поліції зобов'язаний не підкорятися чи ігнорувати будь-який наказ або розпорядження, який (яке) передбачає такі заходи [129, с. 15]. Вказаний елемент адміністративно-правового регулювання, а також чітка норма законодавства, що визнається на території України, прямо підтверджує

позитивний ефект від принципу законності в діяльності поліції, котрий прямо регулює будь-які організаційно-управлінські та кримінально-процесуальні дії пов'язані з можливим притягненням до будь-якого виду відповідальності представників суспільства за ймовірне чи фактичне вчинення тих чи інших протиправних посягань та правопорушень. Крім цього, важливо зауважити, що дана норма захищає також і поліцейського, котрому було віддано незаконний наказ або розпорядження, в частині неможливості притягнення його до дисциплінарної відповідальності за невиконання відповідного наказу, що фактично порушував чи мав високу ймовірність порушення прав і свобод людини і громадянина.

У діяльності Національної поліції України як центрального органу виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку [122], допускається обмеження прав і свобод людини виключно на підставах та в порядку, визначених Конституцією України і законами України, за нагальної потреби і в обсязі, необхідному для виконання завдань поліції. А здійснення поліцією заходів, що обмежують права і свободи людини, має бути негайно припинено, якщо мета застосування таких заходів досягнута або немає потреби в подальшому їх застосуванні [29, с. 74–79]. Дана позиція дослідника чітко демонструє принцип пропорційності в діяльності поліції, оскільки відповідним посадовим особам забороняється, навіть з урахуванням дії правового режиму воєнного стану, застосовувати ті чи інші поліцейські заходи та будь-які інші заходи примусу до особи, в разі якщо вона не чинить супротиву. Неможливість такого порушення прав і свобод людини і громадянина захищає, як

конкретну особу так і відповідного поліцейського, що зобов'язаний застосовувати та приводити в дію ті чи інші нормативно-правові конструкції, що надають йому право та можливість на здійснення відповідної діяльності в межах своєї компетенції та визначених законодавством України повноважень.

Національна поліція України є органом, на який покладено завдання служити суспільству шляхом забезпечення охорони законних прав та свобод людини і громадянина, підтримувати публічну безпеку та правопорядок, а також протидіяти злочинності. У процесі виконання даних завдань проявляється компетенція Національної поліції щодо реалізації міжнародних стандартів прав людини. Ці завдання утворюють специфіку та особливий характер діяльності поліцейського, підготовка якого повинна бути зосереджена на набутті ним практичних знань, умінь та навичок, виховання у нього поваги до природних прав людини, а виконання його професійних службових обов'язків повинно відбуватися відповідно до вимог нормативно – правових актів, посадових (функціональних) обов'язків та наказів керівництва [31]. Відповідно, коло нормативно-правового регулювання адміністративно-правового статусу національної поліції України, зокрема в умовах дії правового режиму воєнного стану, має охоплювати також і процеси підготовки поліцейських котрі під час здобуття освіти зобов'язані вивчати ті чи інші норми пов'язані з дією правового режиму воєнного стану на території України та ймовірними правовими наслідками його введення, а також мати виключну компетенцію у сфері подальшого (післявоєнного) прогнозування тих чи інших криміногенних факторів у

суспільстві, що власне входить до структури здобуття юридичної професії чи професії у сфері правоохоронної діяльності.

О. К. Соколенко наголошує, що захист прав та свобод людини і громадянина, є не просто окремим завданням правової держави, а її цільовою метою, генеральним напрямом діяльності, який має втілюватись в усіх сферах державного управління, зокрема щодо розширення кола прав і свобод людини і громадянина, вдосконалення змісту й характеру їх гарантій, у тому числі правових гарантій захисту [152, с. 118]. Сьогодення вимагає від працівників органів поліції високого морального і культурного рівня, належного освітнього рівня, досконалого знання не тільки національних нормативно-правових актів та їх правильного застосування на внутрішньодержавному рівні, а й міжнародно-правових документів, що стосуються діяльності правоохоронних органів і забезпечення прав і свобод людини і громадянина в Україні. Саме стан справ в сфері забезпечення прав і свобод людини та їх практичної реалізації є тим критерієм, за яким оцінюється рівень демократичного розвитку держави на світовій арені [104, с. 96]. Можливо слід також зауважити, що стрімка інтеграція України до Європейського Союзу, а також поверхневий аналіз міжнародного законодавства у сфері правоохоронної діяльності, а також законодавство окремих європейських країн прямопропорційно впливають на процеси адміністративно-правового регулювання діяльності Національної поліції України під час дії правового режиму воєнного стану, хоч такий правовий режим для країн європейського простору і є новим та практично нереалізовуваним. При цьому, важливість чіткого дотримання норм і меж законодавства України та

європейського союзу (чи міжнародного законодавства), що в установленому законодавством України порядку ратифіковані та використовуються на нашій території, є беззаперечно необхідною, в контексті подальшої інтеграції української держави до кола світового співтовариства.

Убачається, що обмеження поліцією прав і свобод людини можливе, поперше, виключно на законних підставах, тобто за наявності відповідних юридичних фактів, передбачених Конституцією України і законами України, що обумовлює форму поліцейської діяльності (наприклад, правозастосовну (отримання вмотивованого рішення суду для проведення огляду чи обшуку житла чи іншого володіння особи), адміністративно-правову, організаційну [101, с. 128–129]), по-друге, порядок застосування заходів, які спрямовані на таке обмеження, має бути нормативно визначеним, що, на нашу думку, вказує на потребу чіткої реалізації норм процесуального характеру та на спосіб (метод) відповідної правоохоронної діяльності (наприклад, спосіб проникнення до житла чи до іншого володіння особи, методи обстеження (збору даних), методи формування рішень, методи обґрунтування рішень, методи впровадження, примусу та ін. [41]). Чітке коло форм і методів адміністративно-правового впливу поліцейського на суспільно-правові відносини, перш за все, позитивно впливають на дотримання принципів демократичності та правової державності в суспільному устрої та дозволяють дати вичерпну характеристику основним суспільно-політичним процесам та власне визначити рівень життя суспільства. З протилежної точки зору, вичерпність адміністративно-правового інструментарію, що застосовується поліцейськими в умовах тимчасового обмеження прав і свобод людини і громадянина під час дії

правового режиму воєнного стану, забезпечує встановлення чіткої межі подальшої неможливості обмеження поліцейським певного виду права, оскільки це вже прямо передбачено структурним компонентом законодавства.

Під час виконання обов'язків, поліція користуватися достатньою незалежністю від інших державних органів у процесі виконання доручених їй завдань, за які вона має бути повністю відповідальна. Поліція повинна бути організована в такий спосіб, що сприяє хорошим зв'язкам поліції з громадськістю й за необхідності ефективній співпраці з іншими органами, місцевими громадами, неурядовими організаціями та іншими представниками громадськості, в тому числі етнічними меншинами. Слід зазначити, що в Україні на сьогодні достатньо актуальним є питання щодо діяльності поліції в умовах окупації територій іноземною державою. З цього приводу в Резолюції Парламентської Асамблеї Ради Європи «Про Декларацію про поліцію» вказано, що офіцер поліції повинен продовжувати виконувати свої завдання із захисту людей і майна під час війни й ворожої окупації в інтересах мирного населення [129, с. 17]. Водночас, зазначена позиція так само корелюється із національним законодавством України, що на нашу думку потребує подальшого вдосконалення, оскільки в умовах системного вчинення військами агресора жорстоких, нелюдських та таких, що принижують гідність людини діянь, у тому числі конкретних кримінальних правопорушень, пов'язаних із геноцидом української нації, можливість забезпечення прав і свобод людини і громадянина, а також правопорядку на тимчасово окупованих територіях України взагалі відсутня, у зв'язку з чим, найбільш ефективним виходом із цієї ситуації є евакуація населення.

Вбачається, що поліцейська діяльність у правоохоронній сфері має ґрунтуватися лише на юридичних нормах, систематизованих та об'єктивованих у відповідних нормативноправових актах відмінної юридичної сили як національного, так і міжнародноправового характеру [30, с. 118–127]. Як указують В. Черней і С. Чернявський – неодмінним доповненням переліку проблемних аспектів юридичного, організаційного та прикладного спрямування є актуалізація наукових пошуків у сфері правоохорони, що сприятиме визначенню шляхів удосконалення законодавства та практики його застосування [173, с. 11]. На нашу думку, відсутність обов'язкового наукового забезпечення діяльності Національної поліції, зокрема в умовах правового режиму воєнного стану, а також швидкоплинності законодавства України та стрімкості появи відповідних нормативно-правових новел, негативно впливає на адміністративно-правове регулювання діяльності Національної поліції України в особливий період та потребує врегулювання на нормативно-правовому рівні.

За твердженням М. П. Гурковського, С. С. Єсімова, зміст форм і методів діяльності поліції щодо забезпечення прав і свобод зумовлені конкретно історичними обставинами. Поява інноваційних технологій породила кіберзлочинність, боротьба з якою потребує використання нових ефективних методів діяльності поліції. Це вимагає постійного наукового аналізу з урахуванням закономірностей і тенденцій розвитку суспільства та держави, що у свою чергу неодмінно буде сприяти реалізації конституційного завдання держави щодо визнання, дотримання та захисту прав і свобод людини і громадянина в суспільстві [41, с. 184]. Саме тому, на нашу думку, одним із найбільш позитивних аспектів сучасної

тенденції, щодо внесення змін до законодавства України у сфері правового регулювання поліцейської діяльності та функціонування Національної поліції України необхідно виділити оперативність внесення змін до законодавчого забезпечення окреслених питань, з урахуванням сучасних соціально-правових тенденцій та заходів із відсічі збройної агресії російської федерації.

В юридичній літературі минулого та сучасності немає єдиної точки щодо визначення поняття принципів права, що у свою чергу, дає можливість стверджувати про актуальність цієї проблеми. Незважаючи на відмінність у поглядах на проблему принципів права, юридична наука у відповідні історичні епохи була єдиною у проголошенні певних положень та ідей як принципів права. Іншими словами, принципи права — це такі правові явища, які безпосередньо пов'язують зміст права з тими закономірностями суспільного життя, на яких ця правова система побудована і які вона закріплює. Сама ця залежність зумовлює характер правотворчості, зміст правових норм, способи і методи реалізації права [75, с. 20–21]. Таким чином, позитивний аспект принципу правової врегульованості функціонування Національної поліції України в умовах та обставинах за яких права і свободи людини і громадянина можуть зазнавати суттєвих обмежень полягає в тому, що для всіх учасників зазначених соціально-правових відносин були, є і залишаються в майбутньому зрозумілими, конкретні нормативно-правові умови комунікації в суспільстві між його членами та суспільства із державою, в контексті дотримання правопорядку, а також забезпечення прав і свобод людини і громадянина, зокрема в умовах дії правового режиму воєнного стану в Україні.

Як доречно зазначають українські вчені, попри те, що кожна людина володіє правами й основоположними свободами за фактом народження, трапляються випадки, коли здійснення певного права однією людиною може бути загрозою для прав і свобод іншої людини. Таку ситуацію ще називають конфліктом прав. Більшість прав людини не мають абсолютного характеру. Це означає, що вони можуть бути обмежені за певних конкретних обставин. Свобода слова може бути обмежена заради приватності іншої людини. Приватність пасажирів літака під час реєстрації на рейс і проходження контролю обмежується заради безпеки інших пасажирів. У правовій державі межі прав людини встановлює суд або міжнародні органи із захисту прав людини. До абсолютних прав, які не можна порушувати за будь-яких умов чи обставин, належать лише: заборона катування та такого, що принижує гідність, поводження чи покарання; заборона рабства й примусової праці. Людство вже давно зрозуміло, що користування правами пов'язане з відповідальністю перед суспільством. І саме ця відповідальність диктує необхідність обмежень [114, с. 21]. Таким чином, проаналізовані нормативно-правові та теоретико-правові підґрунтя, що формують інститут адміністративно-правового регулювання функціонування Національної поліції України в умовах дії правового режиму воєнного стану, свідчать про переважну кількість позитивних рис і аспектів даного інституту права, що якісно впливають на основні процеси утвердження зазначеного інституту, а також його подальшого розвитку, крізь призму визначених у суспільстві пріоритетних напрямів трансформації та оптимізації.

Процес формування та форми вираження принципів права (як і їх термінологічні позначення) у різних правових сім'ях і цивілізаціях істотно розрізняються. Як свідчить світовий досвід, вони далеко не завжди фіксуються у якомусь конкретному юридичному документі, зокрема в конституції, що помітно навіть у межах європейської цивілізації. В англійському праві, наприклад, принципи права потрібно відшукувати не в конституції, оскільки як єдиний кодифікований акт у Великій Британії вона відсутня, і навіть не в законах, незважаючи на зростання їхньої питомої ваги в англійській правовій системі, а у відповідних інститутах і звичаях, що часто мають багатовікову історію, судових рішеннях тощо [185, с.154]. Водночас основні канони пов'язані із становленням та функціонуванням інституту адміністративно-правового регулювання функціонування національної поліції України загалом та в умовах дії правового режиму воєнного стану в Україні зокрема з урахуванням особливостей української правової системи мають бути чітко визначені в конкретних кодифікованих чи некодифікованих нормативно-правових актах. Переважна більшість таких змін, пов'язаних із суттєвими корективами в діяльності Національної поліції України, перш за все взаємопов'язуються із унесенням змін до відповідного профільного Закону України, що регулює власне її діяльність, а також нормативно-правових актів, що прямопропорційно впливають на визначення змісту і сутності основних операційних процесів, що відбуваються в Національній поліції України на всіх рівнях управління та за всіма напрямками.

Основним завданням поліції, як стверджує Л. І. Каленіченко, є захист і дотримання прав людини, їх

забезпечення та відновлення. З метою виконання цього завдання поліцейські на практиці часто зіштовхуються з необхідністю обмеження прав і свобод конкретних осіб. Так, наприклад, для захисту прав, порушених протиправними діями певного громадянина, поліцейські повинні притягнути до юридичної відповідальності особу, винну у скоєнні правопорушення. Процес притягнення до того чи іншого виду юридичної відповідальності суб'єкта відповідальності тісно пов'язаний із обмеженням його прав і свобод (наприклад, привід, доставлення, особистий огляд тощо). Працівник Національної поліції України має право обмежувати громадянина (людину) виключно у законному порядку. Слід окремо звернути увагу на те, що питання допустимості у тому чи іншому випадку обмежень прав і свобод людини врегульовано як на рівні національного законодавства, так і на рівні міжнародних правових актів-документів [61, с. 35–39], що у свою чергу потребує також певної нашої уваги, по-перше, до питання щодо допустимості у тому чи іншому випадку обмежень прав і свобод людини, по-друге, до міжнародно-правових документів у сфері регламентації такого обмеження [27]. Таким чином, необхідно зробити проміжний висновок проте, що чим більш якісно механізм адміністративно-правового регулювання функціонування Національної поліції України в умовах дії правового режиму воєнного стану відображений у нормативно-правовому забезпеченні, тим більш ефективно нею буде здійснюватись діяльність у сфері забезпечення дотримання прав і свобод людини і громадянина, а також охорони та захисту правопорядку в державі, з урахуванням сучасних безпекових викликів.

Про це також указують й інші дослідники, зокрема підкреслюється, що для забезпечення правопорядку в суспільстві органи поліції наділені повноваженнями здійснювати поліцейські заходи. Національне законодавство визначає поліцейський захід як дію або комплекс дій превентивного або примусового характеру, що обмежує певні права і свободи людини й застосовується поліцейськими відповідно до закону для забезпечення виконання покладених на поліцію повноважень (ч. 1 ст. 29 Закону). Уважаємо, що ключовим словосполученням у цьому визначенні є «обмеження прав». Саме поняття «обмеження прав» потрібно чітко відмежовувати від поняття «порушення прав людини». Якщо на теоретичному рівні ця межа добре простежується, то на практичному часто виникають проблеми (будь-яке незаконне обмеження прав людини автоматично стає їх порушенням). Тому сьогодні проблема практичного застосування поліцейських заходів набирає все більшої актуальності [153]. Тож, позитивний аспект чіткості нормативно-правового регулювання та належного обґрунтування логіки всіх термінів і понять, що складають інститут адміністративно-правового регулювання функціонування Національної поліції України в умовах дії правового режиму воєнного стану, полягає в тому, що зазначені нормативно-правові компоненти вказаного механізму таким чином формують його зміст, що основні напрями діяльності Національної поліції України забезпечується та реалізуються в найбільш ефективний спосіб із залученням найменшого трудового ресурсу та з найвищою якістю виконання поліцейських функцій.

Висновки до розділу 1

Забезпечення дії адміністративно-правового механізму інформаційної безпеки, на нашу думку має включати низку факторів, серед яких зокрема наявні також й інструменти впливу як на внутрішньоорганізаційної процеси забезпечення інформаційної безпеки так і зовнішню взаємодію, що в свою чергу прямопропорційно корелюється з можливістю та спроможністю забезпечення комплексного дотримання режиму інформаційної безпеки в державі та Національній поліції України, зокрема.

Поняття інформаційної безпеки, як категорії, що прямопропорційно впливає на реалізацію та алгоритм дії адміністративно-правового механізму має бути всебічно досліджено та якісно насичено відповідними структурними характеристиками, що в свою чергу формуються на підставі наукового бачення. Крізь такий підхід, питання пов'язані з науково-теоретичним опрацюванням поняття адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України не можуть бути розглянуті без детального опису самого предмету цього інституту.

Сутність адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України полягає в цілісному та комплексному підході до організації вказаного процесу, оскільки він хоч і може складатись з різних структурних компонентів, проте його єдиний зміст має бути дотриманий з метою забезпечення комплексного підходу до утвердження

прав і свобод людини і громадянина в інформаційному просторі та загальнодержавному контексті.

Поняття суб'єктів адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України складається, перш за все, з поділу їх на декілька категорій, що включають в себе: суб'єктів, що відповідають за забезпечення правового режиму інформаційної безпеки та не допускають витоку відповідної інформації маючи в структурі кола своєї компетенції відповідні завдання та повноваження; суб'єктів, що мають право на ознайомлення та володіння певними видами та типами інформації й отримують можливість його реалізації за дозволом зазначених вище; суб'єктів, що формують загальнодержавну та відомчу політику у сфері захисту та формування архітектури безпеки інформації зокрема в діяльності Національної поліції України; суб'єктів до кола компетенції яких прямо віднесено здійснення адміністративно-юрисдикційних чи будь-яких інших юридичних правочинів, пов'язаних із притягненням до різного виду юридичної відповідальності відповідних осіб, що порушили законодавство України.

РОЗДІЛ 2. ЗМІСТ ОКРЕМИХ ЕЛЕМЕНТІВ АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ

2.1. Нормативно-правове регулювання інформаційної безпеки в Національній поліції України

Основи правового регулювання інформаційної безпеки в Національній поліції України закладені глибоко в законодавстві й прямопропорційно визначають його зміст і сутність. Слід підкреслити, що без належного правового регулювання вказаної інституції забезпечення інформаційної безпеки в Національній поліції України є неможливим, оскільки вона, як центральний орган виконавчої влади зобов'язана діяти виключно в межах і у спосіб прямо передбачені нормами законодавства України, перш за все її Конституції, а також, в свою чергу, підзаконними нормативно-правовими актами.

Саме тому, від змістовності наповнення зазначеного кола нормативно-правового забезпечення залежить не лише ефективність правового регулювання зазначеного адміністративно-правового механізму а й міра та зміст дотримання принципових засад інформаційної безпеки, як в діяльності Національної поліції України так і у повсякденній діяльності суспільства. Саме тому, на нашу думку, основи правового регулювання адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції

України мають постати одним із завдань даного дослідження та бути розглянутими в межах окремого підрозділу.

Недостатність правового регулювання правової бази щодо інформаційних правовідносин значно ускладнює настання якісних змін у цій сфері суспільних відносин. На сьогодні у зв'язку з відсутністю взаємопов'язаних, чітко розроблених заходів та теоретичних розробок із забезпечення інформаційної безпеки держави маємо цілу низку перешкод на шляху повноцінної реалізації державою свого обов'язку щодо забезпечення інформаційної безпеки, яка, у свою чергу, є невід'ємною частиною національної безпеки. Лише реалізація науково обґрунтованої державної інформаційної політики може створити ефективну систему протидії правопорушенням у цій сфері [81, с. 136–137]. Неможливість діяльності органів державної влади та інших владних інституцій у контексті забезпечення інформаційної безпеки в тому числі в діяльності Національної поліції України, перш за все пов'язується із проблематикою недостатнього правового регулювання та нечіткості зазначення в тих чи інших актах законодавства та підзаконних нормативно-правових актах, окремих організаційно-управлінських та нормативно-правових опцій, що не чітко чи ефемерно описують ті чи інші явища, чим унеможливлюють їх правореалізацію та втілення в життя на практиці [136].

Правові питання забезпечення інформаційної безпеки особи безпосередньо пов'язані із визначенням загроз інформаційній безпеці особи. Правовий вакуум у більшості питань забезпечення інформаційної безпеки особи, тобто відсутність єдиного нормативного акта, який би регламентував поняття інформаційної безпеки, її основні ознаки, засоби захисту, суб'єктів, на яких покладається

обов'язок здійснювати захист тощо – є серйозною загрозою. Ще одним викликом є системне порушення законодавства з питань інформаційної безпеки, зокрема порушення норм Кримінального кодексу України, Кодексу України про адміністративні правопорушення тощо. При цьому проблеми неправового характеру, як от технічні помилки інформаційних систем (засобів), а також природні процеси, що впливають на передачу, прийом і зберігання інформації також ставлять під загрозу інформаційну безпеку. Способом протидії в цьому випадку можуть бути використання перевіреної техніки, заборона її використання сторонніми особами, очікування налагодження систем передачі інформації її володільцями. Четвертою загрозою є зовнішні чинники. Подолати таку загрозу можна через захист українського суспільства від агресивного інформаційного впливу, розвиток публічної дипломатії тощо [143].

М.Ю. Романов і О.Ф. Кобзар, посилаючись на Закон України «Про Національну поліцію», зауважують, що законодавство України чітко регламентує охорону прав і свобод людини, а також інтересів суспільства та держави, протидію злочинності й надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги [51; 52; 101], з-поміж пріоритетних завдань поліції, що дає підстави укріплювати нормативно-правове регулювання інформаційної безпеки в Національній поліції України є обов'язок поліцейського (зберігати інформацію з обмеженим доступом, яка стала йому відома у зв'язку з виконанням службових обов'язків), а також відповідне повноваження, покладене статтею 25

(Повноваження поліції у сфері інформаційно-аналітичного забезпечення) [109; 110].

Зважаючи на подвійну природу предмета інформаційного права (що вченими трактується як інформаційна, кібернетична та інша безпека у цифровому просторі) нормативні засади механізму правового забезпечення варто розглядати комплексно, але при цьому враховувати, що застосування того чи іншого нормативно-правового акта залежатиме від характеру правовідносин (приватні чи публічні), які потребують врегулювання, а також від того, які інтереси ним забезпечуються (колективні або індивідуальні) [89]. Слід погодитися з тим, що нормативно-правові засади забезпечені інформаційної безпеки особи та держави в особі Національної поліції України розпорошені по різних актах законодавства, в тому числі тих, що не мають відношення до регулювання зазначеної сфери, як такої. Крім цього, належать звернути увагу на термінологічно неточність, що допускається в видах нормативно-правового забезпечення вказаного адміністративно-правового механізму в частині поділу одних і тих самих понять на декілька явищ, як от кібернетична безпека та інформаційна безпека людини, що на сьогоднішній день є на стільки тісно взаємопов'язаними, що визначити кола їх відмінностей майже неможливо. Сутність відмінності даних понять з нормативно-правової точки зору, що власне є вихідною у даному контексті полягає в формі подачі інформації, оскільки станом на сьогодні більшість інформаційних ресурсів доступні онлайн, що в свою чергу ускладнює реалізацію засад інформаційної безпеки крізь призму дії відповідного адміністративно-правового механізму [133].

На нашу думку, слід покроково проаналізувати окреслені проблемні питання, що пов'язані з нормативно-правовим регулюванням інформаційної безпеки в Національній поліції України.

1. Під правовим вакуумом ми розуміємо відсутність єдиного нормативного акта, який би регламентував поняття інформаційної безпеки, її основні ознаки, засоби захисту, суб'єктів, на яких покладається обов'язок здійснювати захист тощо. Хоча законопроектна робота в цьому напрямі ведеться, наразі не має можливості говорити про стадію прийняття Кодексу про інформацію. Способом протидії зазначеній загрозі, на наш погляд, є прийняття Кодексу України «Про інформацію» [143].

2. Порушення законодавства з питань інформаційної безпеки. Хоча консолідований нормативний акт на сьогодні відсутній, існують правові норми, які фрагментарно регулюють питання забезпечення інформаційної безпеки. До таких нормативних актів слід віднести: Кримінальний кодекс України (ст. 182 «Порушення недоторканності приватного життя», ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку», ст. 361-1 «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут», ст. 361-2 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації», ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно обчислювальних машинах

(комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї», ст. 363 «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється» тощо [61]; Кодекс України про адміністративні правопорушення (ст. 188-31 «Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України», ст. 188-39 «Порушення законодавства у сфері захисту персональних даних» [55] тощо) [143].

Існування значних недоліків та суперечностей у законодавчій регламентації основних параметрів інформаційної безпеки, протиріччя та прогалини у правозастосовній практиці в цій сфері ускладнюють процес впровадження у життєдіяльність нашого суспільства правових норм та інституцій, притаманних сучасному цивілізованому світу [80, с. 66]. Сфері кібернетичної безпеки як інституту інформаційного права також притаманна наявність як норм публічного права, так норм і приватного права. А специфіка предмета правового регулювання потребує суміщення кількох методів правового регулювання – як диспозитивного, так і імперативного. Норми як публічного, так і приватного матеріального права закріплюють, створюють, регулюють, охороняють, а також захищають відповідні права, свободи та інтереси людини у кібернетичному просторі. Загалом, не виокремлюючи публічну чи приватноправову складову, нормативні засади механізму правового забезпечення кібернетичної безпеки людини можна подати через: відповідну систему нормативно-

правових актів; правових принципів; міжнародних та національних стандартів, що регулюють цю сферу [89]. Диспозитивний та імперативний методи правового регулювання в свою чергу, широко використовуються в діяльності Національної поліції України, в умовах необхідності забезпечення дотримання засад інформаційної безпеки й дії відповідного адміністративно-правового механізму.

Розробляючи позицію О. Баранова щодо двох блоків інформаційного законодавства, вважаємо, що можна розмежувати дві складові в структурі законодавства про інформаційну безпеку. По-перше, саме законодавство про інформацію, в якому суб'єкт і інститути права на інформацію проявляються в своїй сукупності. По-друге, «блокування» міжсекторальної інформації («об'єднуючі» блоки інформації, які неминуче присутні або повинні бути в кожній галузі законодавства). Інформаційне законодавство виконує своєрідну універсальну зв'язну функцію для забезпечення системності законодавства, оскільки прагне уніфікувати і об'єднати регулювання інформаційних процесів у всіх сферах державного і суспільного життя. Слід зазначити, що міжгалузевий блок значно перевищує власне інформаційне законодавство. По відношенню до сфери інформаційної безпеки елементами є: нормативна характеристика інформаційної складової компетенції (інформаційно-правової ситуації) кожного суб'єкта інформаційних звітів; інформаційна складова відносин у системі централізації, децентралізації та деконцентрації функцій управління, що дозволяє гнучко регулювати інформаційні потоки; правове регулювання інформаційних систем та інформаційних механізмів [11]. Слід зауважити, що ми так само, як і авторка

поділяємо позицію про те, що всі аспекти інформаційної діяльності будь-якого органу державної влади мають бути належно врегульовані з метою забезпечення правового режиму інформаційної безпеки та дотримання прав і свобод людини і громадянина в даному контексті, що в свою чергу прямопропорційно співвідноситься з рівнем демократії та дотримання принципів правової державності в конкретній країні.

Характерною рисою національного інформаційного законодавства є декларативність значного масиву норм без указівок на шляхи їх реалізації, внаслідок чого спостерігається низький рівень правореалізації норм права, що регулюють суспільні відносини у сфері забезпечення інформаційної безпеки. Крім того, наявність численних бланкетних чи відсильних норм права, багатьох абстрактних, суб'єктивних понять, що потребують офіційного тлумачення чи чіткого визначення, а також відсутність закріплення фундаментальних, базових дефініцій (наприклад, інформаційна безпека) є джерелами загроз інформаційній безпеці України [81, с. 133]. Рівень та ефективність правореалізації тих чи інших норм законодавства України прямопропорційно співвідносяться з ефективністю функціонування адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України. Проте, чіткість та реальність цих норм є тими критеріями, що безпосередньо співвідносяться з можливістю ефективного функціонування та здійснення відповідних повноважень, у тому числі виконання обов'язків конкретними суб'єктами на які їх покладено.

Сфера інформації потребує удосконалення чинних нормативних актів, оскільки регулювання інформаційної безпеки змінюється і завершується настільки швидко, що законодавче і навіть нормативне регулювання не встигає цього зробити [87]. Так, окремими аспектами та інструментами забезпечення правового режиму безпеки інформації та втілення в життя відповідного адміністративно-правового механізму є необхідність дотримання норм загального законодавства України у сфері безпеки інформації, в тому числі щодо звернення громадян.

Зазначимо, що правове регулювання сфери інформаційної безпеки характеризується відсутністю чіткої структурованості, однак до основних нормативно-правових актів, що регулюють правовідносини, які виникають під час використання відповідного простору задля створення умов безпечного його використання, а також охорони, захисту життєво важливих інтересів, прав і свобод людини, можна віднести: 1) чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, адже значна частина кіберпростору є де-факто міжнародною, і лише в окремих випадках його функціонування знаходиться під контролем і суверенітетом відповідної держави. Тому можна стверджувати, що значна частина відносин в кіберпросторі може бути врегульована засобами міжнародного права, до яких варто віднести зокрема: Загальну декларацію прав людини; Конвенцію про кіберзлочинність 2001 р.; Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних та інші. Окремої уваги заслуговує Загальний регламент про захист даних (General Data Protection Regulation, GDPR; Regulation (EU) 2016/679). Загальний регламент про захист даних хоча і

не може вважатися повноцінним джерелом права в Україні, однак положення цього нормативно-правового акта поширюються на тих суб'єктів, які здійснюють свою діяльність, зокрема і у всесвітній мережі Інтернет, на території Європейського Союзу або прямо чи опосередковано мають доступ до персональних даних осіб, які знаходяться на території Європейського Союзу; 2) нормативно-правові акти України, зокрема: Конституцію України; Кримінальний кодекс України; Кодекс України про адміністративні правопорушення; Цивільний кодекс України; галузеві нормативно-правові акти України (закони України), які містять норми, що регулюють правовідносини, що виникають під час використання кіберпростору, і спрямовані на охорону й захист прав, свобод, інтересів людини у цій сфері: Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. за № 2163-VIII¹⁹; Закон України «Про захист персональних даних» та інші [89].

Поділяємо зазначену автором позицію, оскільки диференціація нормативно-правових актів, що забезпечують дію адміністративно-правового механізму інформаційної безпеки в державі загалом та Національній поліції України зокрема та доцільно полягає в їх розподілі на міжнародне та національне законодавство. Водночас, станом на сьогодні, з огляду на стрімкі євроінтеграційні процеси, на нашу думку, потреба порівняння актів права Європейського Союзу із актами національного законодавства зростає кратно, що в свою чергу потребує адаптації національних правових засад у сфері безпеки інформації до міждержавних канонів, що в подальшому дозволить більш ефективно реалізовувати засади інформаційної безпеки та не допускати порушення прав і свобод людини і громадянина, як на національному так і

міжнародному рівні, що є основою та основним завданням діяльності Національної поліції України.

Загрозами інформаційній безпеці особи, крім окреслених, можуть бути відмови, збої, технічні помилки інформаційних систем (засобів), а також природні процеси, що впливають на передачу, прийом і зберігання інформації. Способом протидії в цьому випадку може бути використання перевіреної техніки, заборона її використання сторонніми особами, очікування налагодження систем передачі інформації її володільцями. Також, загрозами можуть бути зовнішні чинники. В умовах збройного конфлікту все частіше трапляються випадки порушення інформаційної безпеки особи з боку російської федерації, зокрема розповсюдження антиукраїнських закликів, спам-повідомлення сепаратистського характеру тощо. Вчені зазначають, що подолати таку загрозу можна через захист українського суспільства від «агресивного інформаційного впливу російської федерації», розвиток публічної дипломатії, у тому числі культурної та цифрової, видалення шкідливої інформації з українського сегменту Інтернету та квотування національного аудіовізуального контенту, захист права на вільний доступ до інформації, створення механізмів захисту від пропаганди тощо [31, с. 98]. Слід зауважити, що правове забезпечення адміністративно-правового механізму інформаційної безпеки в діяльності Національної поліції України в даному контексті потребує удосконалення, оскільки із настанням та введенням в дію правового режиму воєнного стану низка видів та типів інформації, що використовуються в службовій діяльності Національної поліції України стала недоступна публічно та може бути висвітлена лише точково та фрагментарно, з огляду на

потреби національної та державної безпеки, а також безпеки суспільства в широкому її розумінні.

Слід також підкреслити, що в умовах ведення інформаційної війни проти нашої держави будь-яка інформація, що використовується під час здійснення своїх службових обов'язків та реалізації відповідних повноважень, може бути використана агресором проти суспільства, що і зумовлює необхідність обмеження тих чи інших видів інформації з метою недопущення їх неоднозначного трактування чи використання проти суспільства загалом чи окремих взятих його членів.

Проблема забезпечення регулювання в інформаційній сфері поки перебуває на стадії становлення. Інформаційна безпека забезпечується проведенням єдиної державної політики національної безпеки в інформаційній сфері, системою заходів економічного, політичного й організаційного характеру, адекватних загрозам та небезпекам національних інтересів особи, суспільства та держави в інформаційній сфері [81, с. 133–134]. На нашу думку, слід погодитися з позицією автора, оскільки за більш як два роки ведення та реалізації заходів із відсічі широкомасштабної збройної агресії російської федерації система національного законодавства у сфері безпеки інформації, в тому числі в діяльності Національної поліції України, була не достатньо вдосконалена, зокрема в частині недопущення витоку персональних даних осіб, що зберігалися в інформаційно-аналітичних базах відповідного центрального органу виконавчої влади та унеможливлення використання будь-якої іншої інформації агресором в своїх інтересах.

Протягом останніх років в Україні ведеться робота над розробкою якісної електронних систем урядування, наприклад інформаційна взаємодія Державного реєстру актів цивільного стану громадян з інформаційно-телекомунікаційними системами органів державної влади (у тому числі, Національної поліції України), здійснюється в режимі реального часу інформаційно-телекомунікаційними засобами із застосуванням засобів технічного та криптографічного захисту інформації відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах». Для того, щоб якісно надавати електронні адміністративні послуги необхідно зробити доступним швидкісний інтернет для всього населення. Для цього вже прийнято Закон України №3014 «Про електронні комунікації», від 16 грудня 2020 року, який дозволить реформувати сферу електронних комунікацій відповідно до найновіших європейських норм та дозволить надати рівний доступ усім громадянам до зв'язку та Інтернету [147]. Слід зазначити також на тому, що інформаційно-технічні ресурси Міністерства внутрішніх справ України та Національної поліції України також удосконалюються та цифровізуються, що використовується в службовій діяльності. Так, автоматизація процесу видачі довідок про несудимість громадянам України, а також запуск єдиного реєстру зброї, що містить в собі значну кількість інформації пов'язаної з персональною ідентифікацією осіб громадян, потребувала розширення кола способів, методів і засобів забезпечення безпеки інформації в кібернетичному просторі. Саме тому нами попередньо зазначалось там взаємопов'язаності вказаних сфер і наполягається на потребі

суттєвого вдосконалення правового регулювання дії зазначеного адміністративно-правового інституту.

Адміністративно-правові норми (акти) у будь-якій сфері суспільних відносин сьогодні класифікують використовуючи різні підходи. Однак найважливішою класифікацією нормативно-правових актів у сфері інформаційної та інформаційно-аналітичної діяльності Національної поліції в Україні, безперечно, є їх розподіл за юридичною силою. За основу такої класифікації візьмемо систему, визначену О. Скакун: 1) Конституція, конституційні закони; 2) ратифіковані Верховною Радою України міжнародні договори; 3) кодифіковані та звичайні (поточні) закони; 4) постанови Верховної Ради України; 5) укази Президента України; 6) постанови Кабінету Міністрів України; 7) накази міністерств, інших центральних органів виконавчої влади [122]. Водночас враховуючи те, що окремі Закони України є похідними нормативно-правовими актами інших законів (тобто розроблені на їх основі та деталізують або доповнюють їх), пропонуємо у цю класифікацію внести зміни, виклавши третю групу нормативних документів у представленій вище класифікації у такій редакції «кодекси, основоположні та похідні закони» [7]. На нашу думку, зазначені теоретико-правові позиції прямопропорційно впливають на можливість та ефективність належного нормативно-правового забезпечення інформаційної безпеки в діяльності Національної поліції України, що в свою чергу уможливорює ефективне забезпечення дотримання прав і свобод людини і громадянина. Так, поряд із вказаними необхідно також враховувати положення і засади національних стратегій у сфері захисту прав і свобод людини,

цифрової трансформації та інших пропорційно пов'язаних з забезпеченням інформаційної безпеки суспільства.

Основну роль у адміністративно-правовому регулюванні інформаційної та інформаційно-аналітичної діяльності Національної поліції, насамперед, відіграє Закон України «Про Національну поліцію». Відповідно до конституційних принципів, у ст. 1 цього закону визначено, що «Національна поліція України – це центральний орган виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку» [101]. Важливе значення у цьому законі приділено визначенню повноважень Національної поліції у сфері обігу інформації, інформаційно-аналітичного забезпечення, формуванню та використанню інформаційних ресурсів [120]. Зокрема, у ст. 25 цього Закону зазначено, що в межах інформаційно-аналітичної діяльності поліція: наповнює бази (банки) даних, які є складовими ЄІС МВС України; використовує бази (банки) даних МВС України й інших державних органів; проводить інформаційно-аналітичну та інформаційно-пошукову діяльність; забезпечує інформаційну співпрацю з органами державної та виконавчої влади України, правоохоронними органами зарубіжних держав і міжнародними організаціями. Окрім цього, сказано, що «поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень» (ч. 3. ст. 25) [7]. Адміністративно-правове регулювання будь-яких операцій, що здійснюється із банками

та базами даних, що обліковуються в Національній поліції України і відображає сутність та зміст правових засад інформаційної безпеки, як в даному центральному органі виконавчої влади, так і в суспільстві загалом, оскільки воно охоплює всю його соціально-правову діяльність. Варто підкреслити, що доктринальне значення, в контексті функціонування зазначеного центрального органу виконавчої влади, відіграє саме той пул нормативно-правових актів, що прямо чи опосередковано регулює його діяльність. Перш за все, мова йде про закони України котрі регулюють діяльність центральних органів виконавчої влади загалом, а також Національної поліції України та інших органів правопорядку, зокрема. Крім цього, ми вважаємо, що одну з ключових ролей в даному питанні відіграють підзаконні нормативно-правові акти, до кола яких відноситься постанова Кабінету Міністрів України, а також накази та доручення Міністерства внутрішніх справ України (зокрема наказ Міністерства внутрішніх справ України та Міністерства оборони України від 18.05.2023 № 290/411 «Про затвердження Порядку електронної інформаційної взаємодії Міністерства оборони України, Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України»).

Розглядаючи адміністративно-правове регулювання у сфері інформаційної та інформаційно-аналітичної діяльності Національної поліції України, потрібно проаналізувати такі його складові, як галузь адміністративно-правового регулювання діяльності Національної поліції України, мета адміністративно-правового регулювання, а також адміністративно-правові засади у сфері інформаційної та

інформаційно-аналітичної діяльності Національної поліції України. Тому, зокрема, адміністративно-правове регулювання відносин у сфері інформаційної та інформаційно-аналітичної діяльності Національної поліції України можна обумовити такими аспектами: об'єктом адміністративно-правового регулювання постають відносини у сфері інформаційної та інформаційно-аналітичної діяльності підрозділів Національної поліції України; ця діяльність охоплює як публічні, так і непублічні відносини; застосуванням, в основному, імперативних способів здійснення впливу на суб'єкти суспільних відносин і спеціального дозвільного методу адміністративно-правового регулювання; ця діяльність Національної поліції України багато в чому визначається завданнями її діяльності (згідно зі ст. 2 Закону України «Про Національну поліцію» завданнями поліції є «надання поліцейських послуг у сферах забезпечення публічної безпеки і порядку; охорони прав і свобод людини, а також інтересів суспільства і держави; протидії злочинності; надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги») [7]. Вказану позицію необхідно підкреслити та акцентувати взаємопов'язаність завдань, що поставлені перед Національною поліцією України у сфері забезпечення правопорядку в суспільстві та прав і свобод людини і громадянина із тими формами, методами та інструментами, що застосовуються нею для їх досягнення. Безперечно неможливим є забезпечення дотримання прав і свобод людини і громадянина в кібернетичному просторі без введення тих чи інших інформаційно-аналітичних обліків, що в свою чергу зумовлює необхідність забезпечення безпеки їх

функціонування та недопущення витоку тієї чи іншої персональної чи службової інформації пов'язаної із відповідними процесами.

Гармонізація національної правової бази сприятиме зміцненню інформаційної безпеки України та підвищенню її міжнародного авторитету як демократичної і правової держави. Чинне національне законодавство України у частині адміністративно-правового регулювання сфери інформаційної безпеки України потребує вдосконалення. Насамперед, вбачається за необхідне:

доповнити Закон України «Про інформацію» визначенням поняття «інформаційної безпеки;

привести у відповідність нормативно-правові акти України різної юридичної сили, що стосуються сфери інформаційної безпеки;

унести комплекс змін, доповнень та уточнень до законодавчої бази з різних питань адміністративно-правового регулювання забезпечення інформаційної безпеки України, що наразі не знайшли належного врегулювання;

привести у відповідність до міжнародних та європейських норм та стандартів вітчизняне законодавство у сфері забезпечення інформаційної безпеки; розробити належне правове забезпечення міжнародного співробітництва з питань інформаційної безпеки. Слід зауважити, що адміністративно-правове регулювання сфери інформаційної безпеки України потребує подальшого наукового дослідження у напрямку пошуку шляхів вдосконалення національного законодавства у даній сфері [21].

Організаційно-управлінські аспекти, пов'язані з забезпеченням реалізації адміністративно-правового механізму інформаційної безпеки в діяльності Національної

поліції України, що в свою чергу безпосередньо пов’язується з необхідністю створення покладання обов’язків на відповідні підрозділи, що опікуватимуться дотриманням засад інформаційної безпеки не лише на рівні центрального органу управління, а й територіальних підрозділів, у тому числі найменших. Крім цього, окреме питання постає наявність належної кваліфікації суб’єктів забезпечення дотримання засад інформаційної безпеки в діяльності Національної поліції України, оскільки на сьогоднішній день кваліфікаційні вимоги до посад, у відповідних підрозділах інформаційної безпеки, не потребують наявності спеціальних знань (відповідної освіти), проте зміст і сутність їх роботи неминуче призводить до необхідності їх наявності, а їх відсутність унеможливорює виконання покладених завдань.

В Україні створена система забезпечення інформаційної безпеки. Функції та повноваження державних органів, що відповідають за формування та реалізацію державної політики в цій сфері закріплені в нормативно-правових актах різного рівня, як то Конституції України, законах України, указах Президента України, постановах Кабінету Міністрів тощо. Проте недосконалість деяких нормативно-правових актів, їх невідповідність стрімким цифровізаційним процесам, унеможливорює стійке функціонування центральних органів виконавчої влади, які визначають і реалізують політику в інформаційній сфері. Організаційні зміни в системі органів виконавчої влади, що проводяться в рамках адміністративної реформи, мають несистемний характер. Розподіл функцій між окремими суб’єктами системи та схема їх взаємодії потребують вдосконалення. Відсутність цілісної системи інформаційно-аналітичного забезпечення органів державної влади значно ускладнює прийняття ними виважених рішень,

породжує конфліктні ситуації у владних структурах і суспільстві [34].

2.2. Суб'єкти забезпечення інформаційної безпеки в Національній поліції України

Дія адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України реалізується у спосіб втілення в життя повноважень, прав і обов'язків окремих суб'єктів, що прямо відносяться до кола відповідної компетенції. Так, питання аналізу кола суб'єктів забезпечення інформаційної безпеки в Національній поліції України, а також окреслення змісту їх компетенції на нашу думку, безпосередньо відноситься до об'єкта та предмета цього дослідження й у свою чергу, потребує суттєвого та змістовного аналізу.

Крім цього, слід урахувати, що поняття суб'єкта забезпечення інформаційної безпеки в Національній поліції України пропорційно пов'язано з тим, що він безпосередньо може здійснювати та які функції на нього покладаються, щодо застосування інформаційно-безпекових стандартів у діяльності Національної поліції України, як у внутрішньо-службовій діяльності так і під час взаємодії з інститутами громадянського суспільства.

На суб'єкти забезпечення реалізації адміністративно-правового механізму інформаційної безпеки в Національній поліції України покладаються завдання, що прямо чи опосередковано пов'язані із захистом прав і свобод людини і громадянина та мають впливати на рівень демократичності

правоохоронних процесів і сприяти укріпленню правової держави в Україні й оптимізувати основні управлінські та державно-владні процеси на шляху інтеграції до Європейського Союзу [139].

У контексті сучасних викликів та загроз національній безпеці України в інформаційній сфері, особливо важливим стає розробка теоретично обґрунтованої класифікації суб'єктів, що входять до системи суб'єктів адміністративно-правового забезпечення інформаційної безпеки. Хоча класифікація за своєю природою не може бути абсолютно вичерпною через різноманіття інформаційної сфери та постійно мінливі умови, вона має залишатися практичною та функціональною для правозастосування. Вважаємо, що система суб'єктів адміністративно-правового забезпечення інформаційної безпеки містить у собі кілька основних груп суб'єктів, кожна з яких відіграє свою роль у запобіганні загрозам національній безпеці України в інформаційній сфері [63].

Різнманітні органи державної влади, що беруть участь у забезпеченні інформаційної безпеки, можуть поділитися на загальні та спеціальні. Загальні – здійснюють регулювання всіх сфер діяльності держави і є загальнодержавними. Спеціальні суб'єкти здійснюють адміністративно-правове регулювання саме діяльності у певній сфері, тому їх повноваження обмежуються нею. Так, до загальних суб'єктів адміністративно-правового регулювання у сфері інформаційної безпеки: Верховну Раду України – визначає державну політику, законодавчі основи її реалізації, гарантії соціального і правового захисту працівників сфери; Президента України, який є гарантом державного суверенітету, територіальної цілісності України, додержання

Конституції України, прав і свобод людини і громадянина [57; 150].

Тому, до кола вищих органів державної влади, що здійснюють регулювання у сфері дії адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції зокрема та всіх органів державної влади загалом, такі вищі державні інституції, як Верховна Рада України, Кабінет Міністрів України та інституцію Президента України. Крім цього, належить підкреслити, що кожен із зазначених органів державної влади володіє виключною компетенцією у відповідній сфері та забезпечує виконання покладених тільки на нього завдань, що унеможлиблює не ефективне здійснення визначених законодавством України повноважень [137].

Окреслені групи формують багаторівневу структуру адміністративно-правового забезпечення інформаційної безпеки, де кожен рівень робить свій внесок у загальну систему захисту. Держава, в особі своїх органів, відіграє ключову роль в адміністративно-правовому забезпеченні інформаційної безпеки. Володіючи значними ресурсами, вони виконують широкий спектр завдань та функцій, починаючи з розроблення та впровадження правових актів, що стосуються інформаційної сфери, і закінчуючи регулюванням і контролем виконання цих актів. На додачу до цього, держава фінансує освітні програми для підготовки фахівців, співпрацює на міжнародному рівні для захисту від транскордонних інформаційних загроз, стимулює розвиток технологій у сфері інформаційної безпеки тощо. Ефективна державна участь і координація між різними органами та секторами є критично важливою для створення надійної системи із захисту національної безпеки України в

інформаційній сфері. Державна участь є невід’ємною та критично важливою у забезпеченні комплексного захисту інформації на всіх рівнях. Державні ініціативи та дії спрямовані на створення надійної та стійкої системи інформаційної безпеки, здатної протистояти сучасним загрозам і викликам. Щодо суспільства та громадян, то вони доповнюють роботу, яку здійснюють державні органи, вносячи інновації та спеціалізовані знання, що допомагають у розв’язанні специфічних завдань і створенні нових технологічних рішень, які сприяють забезпеченню інформаційної безпеки. Отже, важливість кожної з цих груп не може бути недооцінена, оскільки тільки спільні зусилля всіх суб’єктів, які входять до єдиної системи суб’єктів адміністративно-правового забезпечення інформаційної безпеки дають змогу створити ефективну та стійку систему захисту інформаційного простору. У цьому разі розвиток міжсекторальної взаємодії та посилення співробітництва між усіма зацікавленими сторонами, а також залучення громадськості до процесів ухвалення рішень та контролю за дотриманням інформаційної безпеки, стають ключовими елементами у зміцненні національної безпеки України в інформаційній сфері. Розглядаючи можливі напрями організації спільної діяльності суб’єктів адміністративно-правового забезпечення інформаційної безпеки, необхідно мати на увазі, що взаємодію в широкому плані можна здійснювати у формах взаємного обміну інформацією, спільного планування та проведення заходів, взаємного використання сил і засобів в інтересах вирішення спільних завдань, організації спеціального моніторингу тощо [63].

Національна поліція України, як один із центральних органів виконавчої влади на якого покладено обов’язки, щодо

забезпечення прав і свобод людини і громадянина, а також підтримання правопорядку у суспільстві та запобігання вчиненню правопорушень має більш відповідальне становище та коло обов'язків у сфері забезпечення інформаційної безпеки своєї діяльності відносно всіх осіб і громадян, що перебувають на території України чи поза її межами та потребують її захисту. Національна поліція України в своїй діяльності використовує безмежну кількість, як публічної так і непублічної інформації котра не підлягає розголошенню за умов чітко визначених законодавством України.

До системи суб'єктів адміністративно-правового забезпечення інформаційної безпеки в Україні відносяться: Президент України; Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; Міністерство культури та стратегічних комунікацій України; Міністерство з питань реінтеграції тимчасово окупованих територій України; Національна поліція України; Служба безпеки України; Служба зовнішньої розвідки України, Державна прикордонна служба України; Державна спеціальна служба транспорту; Державна служба України з надзвичайних ситуацій; Державна служба спеціального зв'язку та захисту інформації України; Збройні Сили України та інші органи виконавчої влади та військові формування, які входять до сектору інформаційної безпеки; органи місцевого самоврядування; судові органи; комерційні компанії; недержавні організації та громадяни [63]. На нашу думку, слід цілком і повністю погодитись із позицією автора та виокремити, що дані суб'єкти можуть характеризуватися, як загальнодержавні, так і спеціальні відомчі, що в свою чергу зумовлює необхідність визначення змісту і сутності їх

компетенції та її порівняння з метою науково-теоретичного недопущення взаємопоглинання кіл компетенції та запобігання необґрунтованим державницьким трудовитратам. Водночас, роль і місце Державної служби спеціального зв'язку та захисту інформації України, а також Служби безпеки України чітко визначається національним законодавством та впливає на діяльність всіх без виключення органів державної влади, що апелюють інформацією з обмеженим доступом або мають в своєму розпорядженні чи володінні ті чи інші інформаційні бази даних, що апелюють персональною інформацією інших осіб.

У даному контексті доцільно звернути увагу на підхід О.І. Безпалової щодо класифікації суб'єктів реалізації правоохоронної функції держави, яка у результаті аналізу праць вчених-адміністративістів пропонує виокремити такі види суб'єктів: 1) за походженням (ступенем належності до держави): державні (органи державної влади), недержавні (органи місцевого самоврядування, інституції громадянського суспільства); 2) за характером компетенції: загальні (наприклад, Президент України, Кабінет Міністрів України, Верховна Рада України), спеціальні (правоохоронні органи, суд); 3) за кількісним показником (складом): індивідуальні (наприклад, окремі громадяни, посадові особи, журналісти засобів масової інформації), колективні (наприклад, відповідні органи виконавчої влади, суд, громадські організації правоохоронної спрямованості); 4) за терміном дії (або способом призначення суб'єктів): постійні (наприклад, органи внутрішніх справ, органи прокуратури), виборні (або тимчасові) (наприклад, органи місцевого самоврядування, тимчасова слідча комісія Верховної Ради України) [13, с. 67–68]. Цілком погоджуючись із твердженням авторитетної

науковиці необхідно звернути увагу на те, що вказані класифікаційні критерії повністю відповідають потребам нашого дослідження та потребують уточнення в контексті його предмета і об'єкта, а тому на нашу думку чинним буде виділити низку категорій органів державної влади до кола компетенції, яких віднесено реалізація адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України та проаналізувати їх окремо.

Вищі органи державної влади. Слід зауважити, що вищі органи державної влади України до кола яких відносяться Верховна Рада України, як єдиний законодавчий орган державної влади Кабінет Міністрів України, як вищий орган виконавчої влади в Україні, а також інститут Президента України та вертикаль судової влади безпосередньо впливають на формування та реалізацію державної політики у сфері забезпечення безпеки інформації у всіх без виключення органу державної влади та поширюється і правовий вплив на всі соціально-правові відносини у суспільстві.

У контексті мети цього дослідження нас передусім цікавитимуть державні органи, на які чинним законодавством покладаються специфічні завдання щодо забезпечення інформаційної безпеки під час виконання їх основних функцій. До таких органів можуть бути віднесені, по-перше (окрім визначених Доктриною інформаційної безпеки Ради національної безпеки й оборони України та Кабінету Міністрів України), також Президент України та Верховна Рада України які здійснюють заходи у сфері безпеки держави загалом, зокрема інформаційної, безпеки, а по-друге - державні органи, на які безпосередньо покладається виконання заходів у сфері забезпечення інформаційної

безпеки. Рада національної безпеки й оборони України як координаційний і консультативно-дорадчий орган при Президентові України здійснює оцінку потенційних і реальних загроз національним інтересам, розробляє й доповідає Президентові України, вносить пропозиції щодо їх попередження й нейтралізації; розглядає на своїх засіданнях і приймає рішення з найбільш актуальних проблем забезпечення інформаційної безпеки; здійснює координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері [128]. Слід погодитися з позицією автора та доповнити попередньо зазначений перелік в частині того, що Рада національної безпеки і оборони України, зокрема в умовах дії правового режиму воєнного стану та реалізації широкомасштабних заходів із відбиття збройної агресії російської федерації проти України відіграє чи не найважливішу роль у забезпеченні інформаційної безпеки та виділяє які саме види інформації є прийнятними для публічного використання, а які мають бути тимчасово утаємничені чи доступ до яких має бути обмежено. Водночас, доцільно буде зауважити, що всі рішення Ради національної безпеки і оборони вводяться дії указами Президента України, а тому, хоч формування державної політики у сфері безпеки інформації відноситься частково до компетенції Ради національної безпеки і оборони, проте його право реалізація безпосередньо залежить від інституту Президента України та видання ним відповідного нормативно-правового акту.

Верховна Рада України та Кабінет Міністрів України як суб'єкти системи визначають пріоритети в захисті життєво важливих інтересів об'єктів інформаційної безпеки, розробляють загальні засади правового регулювання відносин

в інформаційній сфері, встановлюють порядок організації та діяльності органів забезпечення інформаційної безпеки. Так, Верховна Рада України в межах повноважень, визначених Конституцією України, формує державну політику і законодавчу базу в інформаційній сфері та здійснює контроль за практикою застосування законодавчих актів у діяльності суб'єктів забезпечення інформаційної безпеки та їх посадових осіб; здійснює парламентський контроль та приймає закони України, які визначають і регулюють діяльність органів сектору інформаційної безпеки та їхні повноваження, а також затверджує відповідні бюджетні асигнування та приймає рішення щодо звіту про їх використання; створює комітети, до повноважень яких належить, зокрема, забезпечення контрольних функцій Верховної Ради України за діяльністю органів сектору інформаційної безпеки; для вивчення, підготовки і попереднього розгляду окремих питань у сфері інформаційної безпеки створює тимчасові спеціальні комісії, а для проведення розслідування з питань, що становлять суспільний інтерес, – тимчасові слідчі комісії; проводить парламентські слухання з питань інформаційної безпеки, що становлять суспільний інтерес і потребують законодавчого врегулювання. Кабінет Міністрів України забезпечує формування та реалізацію інформаційної політики держави, забезпечує інформаційний суверенітет, фінансування програм, пов'язаних з інформаційною безпекою, розробляє та затверджує план заходів з реалізації Стратегії інформаційної безпеки, на основі якого відповідні органи виконавчої влади реалізують заходи щодо забезпечення інформаційної безпеки [63; 124]. На нашу думку, характеризуючи інститут Верховної Ради України необхідно, перш за все, зазначити, що це єдиний законодавчий орган державної влади в Україні,

а відповідно до кола його компетенції віднесено унормування на найвищому законодавчому рівні у законах України відповідних правил, а також мір можливої та належної поведінки у сфері правового режиму безпеки інформації, а також діяльності відповідних органів державної влади. З огляду на функціонування в Україні режиму правової держави неможливим є здійснення будь-яких повноважень обов'язків чи завдань органом державної влади, якщо це прямо не передбачено нормативно-правовими актами зокрема законами України, а тому Верховна Рада України має виключне коло компетенції, щодо формування державної політики у сфері інформаційної безпеки в діяльності Національної поліції України.

Характеризуючи зміст і сутність компетенції Кабінету Міністрів України, як вищого органу державної влади у виконавській вертикалі необхідно зазначити, що він має своє виключне коло компетенції, що не перетинається із діяльністю відповідних профільних міністерств та прямо передбачається положенням про Кабінет Міністрів України. Зазначений вищий орган виконавчої влади, перш за все має, обов'язки та повноваження, щодо здійснення координації інших центральних органів виконавчої влади відповідає за злагодженість їх діяльності за окремим напрямом державної політики, а також контролює механізм їх реалізації. Буквально, крізь призму дії адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України – Кабінет Міністрів України виступає основним контролем суб'єктом.

Від ефективності діяльності зазначеної групи суб'єктів щодо формування державної інформаційної політики безпосередньо залежить охорона та захист основних прав і

свобод громадян, інтересів суспільства та держави в інформаційній сфері, недопущення настання зовнішній та внутрішніх загроз у цій сфері та мінімізація їх негативного впливу, що у результаті має призвести до стабільного розвитку національного інформаційного простору. Слід підкреслити, що під час формування державної інформаційної політики шляхом вироблення відповідної нормативно-правової бази суб'єкти, що належать до першої групи, повинні особливу увагу приділяти питанням запровадження постійного моніторингу впливу на національну безпеку процесів, що відбуваються в інформаційній сфері, за результатами якого повинні прийматися рішення про вжиття відповідних заходів реагування [76]. На нашу думку слід, перш за все, зауважити на тому, що злагодженість механізмів формування державної та відомчої політики у сфері безпеки інформації, в тому числі в діяльності Національної поліції України, а також ефективність її планування з метою подальшої реалізації та контролю за відповідним процесом, прямопропорційно впливають на ефективність функціонування конкретного органу державної влади, зокрема в контексті нашого дослідження Національної поліції України. При цьому враховуючи, що Національна поліція України не може здійснювати компетенційні повноваження реалізовувати права та виконувати обов'язки без прямого передбачення цього в нормативно-правовому забезпеченні, ключовим у даному питанні виступає все ж Верховна Рада України, як єдиний законодавчий орган державної влади.

Центральні органи виконавчої влади, що мають повноваження у сфері забезпечення інформаційної безпеки загалом і в Національній поліції України, зокрема. Належить

зауважити, що кожен окремо взятий центральний орган виконавчої влади, що входить до структури Кабінету Міністрів, що координуються ним через певне Міністерство чи конкретного міністра, має своє виключне коло компетенції, проте всі вони синергетично впливають на адміністративно-правовий механізм забезпечення інформаційної безпеки держави загалом та Національної поліції зокрема, як одного із основних і найбільших органів правопорядку в суспільстві. Нами пропонується охарактеризувати зміст і сутність компетенції окремих суб'єктів забезпечення інформаційної безпеки в діяльності органів державної влади загалом та національної поліції зокрема, з метою обґрунтування подальших кроків, щодо оптимізації відповідного процесу у внутрішню відомчий діяльності Національної поліції України.

Міністерство культури та інформаційної політики України (МКІП), основним завданням якого є забезпечення формування та реалізація державної політики у сферах інформаційного суверенітету (у частині повноважень з управління цілісними майновими комплексами державного підприємства «Мультимедійна платформа іномовлення України» та Українського національного інформаційного агентства «Укрінформ»), інформаційної безпеки України. у сфері інформаційної безпеки МКІП реалізує наступні заходи: розробляє заходи щодо запобігання внутрішньому і зовнішньому інформаційному впливу, який загрожує інформаційній безпеці держави, суспільства, особи; розробляє плани заходів щодо сприяння незалежності засобів масової інформації, захисту прав журналістів та споживачів інформаційної продукції; організовує проведення досліджень впливу результатів діяльності засобів масової інформації на

суспільну свідомість; сприяє дотриманню в Україні свободи слова; розробляє та вносить на розгляд Кабінету Міністрів України програмні документи у сфері захисту інформаційного простору України від зовнішнього інформаційного впливу; забезпечує моніторинг інформації у вітчизняних та іноземних засобах масової інформації; забезпечує організацію та проведення мистецьких конкурсів з метою реалізації культурно-мистецьких проєктів, спрямованих на здійснення заходів у сфері захисту національного інформаційного простору; вживає заходів до захисту прав громадян на вільний збір, зберігання, використання і поширення інформації, зокрема на тимчасово окупованих територіях, відповідно до покладених на МКІП завдань; вживає разом з іншими органами державної влади заходів до захисту неповнолітніх від негативного впливу інформаційної продукції, зокрема аудіо- і відеопродукції, яка становить загрозу суспільній моралі або може зашкодити фізичному, психічному чи моральному розвитку неповнолітніх; надає методичну та практичну допомогу засобам масової інформації у сфері інформаційного суверенітету України (у частині повноважень з управління цілісним майновим комплексом Українського національного інформаційного агентства «Укрінформ») та інформаційної безпеки [48; 63; 90]. Коментуючи діяльність та зміст компетенції Міністерства культури та інформаційної політики України необхідно звернути увагу на тому, що на ньому сконцентровані всі політичні та виконавські адміністративно-правові інструменти, що мають безпосередній вплив на реалізацію адміністративно-правового механізму забезпечення інформаційної безпеки загалом та в діяльності Національної поліції України,

зокрема. Зміст повноважень наданих зазначеному центральному органу виконавчої влади, перш за все, прямо корелюється із визначенням загальнодержавного вектору інформаційної безпеки окресленим її сутності механізмів та основних інструментів досягнення, що в умовах системного використання Національної поліції України персональних даних інших осіб, а також роботи в умовах наявності інформації з обмеженими доступами також і проєктується на діяльність цього органу правопорядку. В даному розрізі необхідно зазначити, що в Національній поліції України є, як внутрішньоорганізаційна діяльність, котра пов'язана із плануванням її роботи в декілька річній перспективі, так і зовнішньо правоохоронна діяльність зазначеного центрального органу виконавчої влади, котра пов'язана із реалізацією повноважень та виконанням завдань із захисту прав і свобод людини і громадянина, що потребує постійної роботи з персональними даними інших осіб та, відповідно, вжиття релевантних заходів із недопущення їх несанкціонованого чи незаконного розповсюдження.

Основними суб'єктами, які в рамках даної групи уповноважені вживати заходів щодо формування державної інформаційної політики є Міністерство культури та інформаційної політики України, Державна служба спеціального зв'язку та захисту інформації України, Державне агентство з питань науки, інновацій та інформатизації України, Державна служба України з питань захисту персональних даних. Саме на ці органи на рівні відповідних нормативно-правових актів покладається обов'язок щодо забезпечення інформаційного суверенітету України, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами, забезпечення

функціонування і захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації [76; 88; 95]. При цьому, належить зауважити, що Державна служба спеціального зв'язку та захисту інформації України не відноситься до кола компетенції Міністерства культури та інформаційної політики України, хоча їх повноваження дещо перетинаються. При цьому, Державна служба спеціального зв'язку та захисту інформації України має виключне коло компетенції у сфері захисту держави в цифровому середовищі, що в свою чергу також поглинає собою й інформаційно-безпекові правовідносини з огляду на те, що в сучасних реаліях більшість інформації зберігається в цифровому просторі.

Державна служба спеціального зв'язку та захисту інформації України, яка серед іншого є відповідальною за забезпечення функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA. Зазначимо, що останній відповідальний також за забезпечення кібернетичної безпеки людини. У зв'язку з тим, що станом на 2020 р. досі не прийнято Закону України «Про критичну інфраструктуру та її захист», у якому б було визначено чіткі критерії віднесення того чи іншого суб'єкта діяльності до об'єктів критичної інфраструктури, Державна служба спеціального зв'язку та захисту інформації України має необмежені повноваження щодо виставлення вимог, які стосуються кібернетичної безпеки для як для державних, так і недержавних суб'єктів,

що може спричиняти перешкоди у їх діяльності [89]. Виокремлюючи коло компетенції Державної служби спеціального зв'язку та захисту інформації України необхідно зазначити, що вона є провідною у питанні визначенню основних стандартів захисту будь-якої інформації у тому числі цифрової, а також до кола її повноважень віднесено низку мілітарних функцій, що безпосередньо позитивно впливають на практичну реалізацію основних методів, форм і засобів досягнення належного правового регулювання у сфері інформаційної безпеки, в тому числі в діяльності Національної поліції України.

Державна служба спеціального зв'язку та захисту інформації України, яка є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, активної протидії агресії у кіберпросторі, а також інших завдань відповідно до закону [95]. Служба відіграє ключову роль в адміністративно-правовому забезпеченні інформаційної безпеки, забезпечуючи захист від зовнішніх і внутрішніх інформаційних загроз. Як інтегральна частина сектору безпеки і оборони України, Служба сприяє зміцненню стабільності та безпеки держави шляхом захисту інформаційних ресурсів, забезпечення безпеки зв'язку та контролю за обігом секретної інформації. Її діяльність спрямована на запобігання кіберзагрозам, шпигунству та іншим формам інформаційного впливу, що робить її незамінним елементом у забезпеченні національної безпеки

України загалом [63]. Так до прикладу необхідно підкреслити, що всі наявні в Національній поліції України інформаційно-аналітичні бази даних, що містять, як власні напрацювання поліції так і на законних підставах персональну інформацію пов'язану з іншими особами мають бути сертифіковані державною службою спеціального зв'язку та захисту інформації в Україні, оскільки остання відповідає за такий напрям роботи, як інформаційно-технічне забезпечення інформаційної безпеки, в тому числі в діяльності Національної поліції України та інших центральних органів виконавчої влади до кола компетенції яких віднесено захист прав і свобод людини і громадянина та забезпечення правопорядку.

Суб'єкти забезпечення інформаційної безпеки в Національній поліції України. Слід зазначити, що чисельність Національної поліції України є значною та переважає понад 100 000 осіб, а відповідно коло структурних підрозділів до кола компетенції яких віднесено забезпечення реалізації відомчої політики інформаційної безпеки в Національній поліції України має бути досить широким, що в свою чергу зумовлює необхідність науково-теоретичного опрацювання змісту і сутності компетенції відповідних підрозділів та конкретних посадових осіб.

Національній поліції України, яка служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку у сучасних умовах прогресивного інформаційно-комунікаційного розвитку притаманні наступні напрями адміністративно-правового забезпечення інформаційної безпеки: організація протидії небажаному для інтересів суспільства й держави впливу за допомогою технічних

засобів захисту, причому засоби захисту мають бути адекватними засобам впливу, що означає необхідність застосування належних за кількістю та якістю технічних засобів захисту інформаційних систем (наприклад, створення системи просторового зашумлення для приховування інформації в обмеженому середовищі чи екранування технічних засобів у приміщенні); організація протидії негативному впливу на учасників інформаційних відносин, зокрема протидія кіберзлочинам як таким, що несуть безпосередню суспільну небезпеку; визначення майнових і моральних утрат та їхня мінімізація в разі порушення функціонування інформаційної системи, важливої для належного забезпечення інтересів суспільства та держави, включаючи взаємодію з іншими правоохоронними та судовими органами як України, так і зарубіжних держав для притягнення до відповідальності й відшкодування заподіяних протиправними діями (бездіяльністю) збитків [84, с. 187]. Відповідно, слід зазначити, що на нашу думку, важливим є виокремлення в діяльності Національної поліції України внутрішньоорганізаційного та зовнішньо правоохоронного аспектів, оскільки безпосередньо для своєї діяльності Національна поліція України використовує низку баз даних, що робить зручними організаційно-управлінські процеси. Ці бази та банки даних, перш за все, пов'язуються із узагальненням інформації про кількість поліцейських із можливістю встановлення різних класифікаційних критеріїв та визначення окремих категорій за певними класифікаторами. Водночас, зовнішньо правоохоронний аспект діяльності Національної поліції України та забезпечення інформаційної безпеки в даному напрямі полягає в необхідності недопущення розповсюдження

накопиченої персональної інформації, а також даних з обмеженим доступом, що безпосередньо використовується в процесі службової діяльності поліцейськими з метою захисту прав і свобод людини і громадянина та забезпечення правопорядку у суспільстві, у тому числі протидії злочинності.

Підрозділи кіберполіції. Національна поліція України, яка є відповідальною за забезпечення захисту прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі. Нині в Україні як структурний підрозділ Національної поліції України функціонує Департамент кіберполіції Національної поліції України, завданням якого має бути визначення, розробка та реалізація комплексу заходів, спрямованих на попередження й протидію кримінальним правопорушенням у кібернетичному просторі [89]. При цьому, необхідно звернути увагу на тому, що компетенція Департаменту кіберполіції Національної поліції України більш за все сконцентрована на зовнішньо правоохоронній діяльності, оскільки зазначений підрозділ є оперативним за своїм змістом та призначенням. Крім цього, чи не буде зазначити, що в своїй діяльності зазначений структурний підрозділ використовує значну кількість персональної інформації та даних з обмеженим доступом, що використовується для досягнення конкретно визначених правоохоронних цілей, а тому основні стандарти захисту інформації та канони інформаційної безпеки мають бути дотримані, як ним так і всіма його структурними підрозділами та відповідними суб'єктами, що за своїми

посадовими обов'язками мають доступ до такої інформації та використовують її.

Що стосується повноважень поліції щодо забезпечення інформаційної безпеки держави, то до них насамперед слід віднести: здійснення превентивної та профілактичної діяльності, спрямованої на запобігання вчиненню правопорушень у сфері інформації; виявлення причин та умов, які сприяють вчиненню кримінальних та адміністративних правопорушень у сфері інформації, вжиття в межах своєї компетенції заходів для їх усунення; вжиття заходів з метою виявлення кримінальних, адміністративних правопорушень у сфері інформаційної безпеки; вжиття заходів, спрямованих на усунення загроз життю та здоров'ю фізичних осіб і публічній безпеці, які виникли внаслідок вчинення кримінального, адміністративного правопорушення у сфері інформаційної безпеки; здійснення досудового розслідування кримінальних правопорушень у сфері інформації та інформаційної безпеки в межах визначеної підслідності; розшук осіб, які переховуються від органів досудового розслідування, слідчого судді, суду, які вчинили зазначені вище правопорушення; у випадках, визначених законом, здійснення проваджень у справах про адміністративні правопорушення у сфері інформації, прийняття рішень про застосування адміністративних стягнень, забезпечення їх виконання [77, с. 170–171]. Необхідно підкреслити, що зміст і сутність зовнішнього правоохоронної функції Національної поліції України, у контексті реалізації адміністративно-правового механізму забезпечення інформаційної безпеки в її діяльності та діяльності держави, полягає не лише в запобіганні та недопущенні вчинення відповідних правопорушень

пов'язаних з інформаційно-безпековими режимами, а й безпосередньому розслідуванні та проведенні різноманітних слідчих (розшукових) дій чи реалізації адміністративно-юрисдикційних повноважень у сфері відновлення порушених інформаційно-безпекових прав. При цьому, питання щодо нанесеної шкоди та міри притягнення до відповідальності, а також взагалі наявності такої можливості відноситься безпосередньо до органів судової влади України, котрі уповноважені від імені України відправляти правосуддя.

Законом України «Про Національну поліцію» регламентовано можливість обробки працівниками поліції в інформаційних системах значного обсягу інформації. Однак, зважаючи на значні переваги цих технологій, слід визнати, що при несанкціонованому їх використанні, це може призвести до серйозних наслідків. Серед основних причин порушень інформаційної безпеки обробки інформації варто виділити: відсутність розроблених і затверджених положень (внутрішньовідомчої нормативно-правової бази та практик застосування) щодо інформаційної безпеки, які б відповідали потребам даного відомства/структурного підрозділу, а також національним і міжнародним стандартам у сфері захисту інформації [45]. При цьому, належить зауважити на виключній ролі Державної служби спеціального зв'язку та захисту інформації України, що і визначає стандарти роботи з різноманітними базами та банками даних, що використовуються в діяльності, в тому числі Національної поліції України з метою забезпечення прав і свобод людини і громадянина та запобігання злочинності.

Підрозділи організаційно-аналітичної роботи та контролю. Належить зауважити, що вказані підрозділи, перш за все, мають виключну компетенцію щодо внутрішньої

організаційної діяльності Національної поліції України та забезпечують внутрішньовідомчий контроль за дотриманням стандартів і вимог законодавства України у сфері інформаційної безпеки. Цей аспект є одним з двох основних, в контексті правореалізації механізму адміністративно-правового регулювання забезпечення інформаційної безпеки в діяльності Національної поліції України, а тому, на нашу думку, потребує окремого окреслення.

Слід зазначити, що контрольні завдання та функції, в принципі, притаманні будь-якому суб'єкту управління, зважаючи на те, що контроль є невід'ємною частиною управління. Відповідно завдання щодо здійснення підрозділами ОАЗОР контролю пов'язані з реалізацією органами поліції державної інформаційної політики лише в тій частині, в якій об'єкти контролю пов'язані з інформаційним забезпеченням діяльності органів Національної поліції. Передусім, це стосується завдання щодо здійснення в підрозділах поліції систематичного аналізу та перевірок стану обліково-реєстраційної дисципліни. Неправильна реєстрація інформації про злочини, правопорушення та інші події не лише є грубим порушенням закону, але й призводить до викривлення даних про оперативну обстановку, тенденції розвитку злочинності на території обслуговування та державі в цілому, що, у свою чергу, тягне за собою прийняття управлінських рішень на базі хибних даних [76]. Слід зазначити, що до кола компетенції підрозділів оперативного реагування та контролю відносяться не лише перевірка стану облікової реєстраційних дисципліни. Зазначені підрозділи відповідають, перш за все, за планування в роботі Національної поліції України та всіх її структурних підрозділів і відповідних посадових осіб, що в

свою чергу включає в себе необхідність дотримання стратегії у сфері кібербезпеки в діяльності Національної поліції України, а також врахування відповідних стандартів під час здійснення правоохоронної діяльності та безпосереднього виконання своїх посадових обов'язків, що може бути проконтрольоване підрозділами оперативного реагування та контролю.

Виконання моніторингових завдань більш тісно пов'язано з інформаційним забезпеченням діяльності органів Національної поліції. Моніторинг являє собою безперервне спостереження за станом оточуючого середовища і управління ним шляхом своєчасного інформування про можливості настання несприятливих, критичних або неприпустимих ситуацій [39, с. 60]. До інформаційно-аналітичних завдань ДОАЗОР належать: вивчення, аналіз і узагальнення результатів та ефективності поліцейської діяльності, виявлення причин та умов, що сприяють вчиненню правопорушень, вжиття в межах компетенції заходів щодо їх усунення; підготовка для керівництва МВС, Національної поліції України, інших зацікавлених органів державної влади, громадськості інформаційно-аналітичних та довідкових матеріалів з питань формування та реалізації державної політики у сфері забезпечення публічної безпеки і порядку, охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, надання поліцейських послуг, що мають комплексний характер та охоплюють кілька напрямів діяльності Національної поліції України [76; 99]. Відповідно, зазначена діяльність може характеризуватися двома аспектами, один із яких полягає в необхідності дотримання стандартів у сфері захисту інформації в діяльності самих підрозділів оперативного реагування та

контролю, а інший у тому, що вказані підрозділи наділені компетенцією, щодо здійснення контролю за дотриманням стану інформаційної безпеки в діяльності інших підрозділів Національної поліції України. Явище контролю, як таке, має бути охарактеризовано, оскільки воно реалізується у спосіб втіленням життя декількох форм управлінської діяльності, одним із яких є проведення нарад, розсилання листів-роз'яснень, щодо тих чи інших аспектів правозастосування українського законодавства загалом, а також здійснення контрольних перевірок різного формату. Всі ці адміністративно-управлінські інструменти, перш за все, втілюють ролі місце, а також коло компетенції підрозділів оперативного реагування та контролю, як суб'єкта реалізація адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України.

Підрозділи документального забезпечення. Можна зауважити, що підрозділи документального забезпечення є одним із найбільш розповсюджених серед всього кола органів державної влади, оскільки без належного організаційного супроводу процесів обміну інформацією між суспільством та державою та між окремими органами державної влади неможливим є ні реалізація правоохоронної функції держави, ні будь-яких інших повноважень. Відповідно, системно працюючи з різноманітною документацією, що містить як службову так і особисту інформацію, підрозділи документального забезпечення завдяки включеним до кола їх компетенції повноваженням також здійснюють низку контрольних функцій за реалізацією адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України.

Документальне забезпечення публічного адміністрування в органах Національної поліції являє собою врегульовану нормами чинного законодавства та підзаконних актів діяльність спеціально уповноважених підрозділів та посадових осіб Національної поліції щодо забезпечення процесу публічного адміністрування документальною інформацією з метою вироблення, прийняття та реалізації управлінських рішень, а також досягнення інших цілей публічного адміністрування. До документальної інформації слід включати не тільки нормативні документи та документи організаційно-розпорядчого характеру, що утворюються в процесі діяльності Національної поліції, але й статистичні, аналітичні, довідкові документи та матеріали [19]. Відповідно, слід підкреслити, що вказані матеріали та інформаційно-аналітичні об'єкти містять інформацію різного рівня таємності та характеру й свого спрямування, що може бути також віднесене до кола конфіденційної чи особистої. Таким чином, забезпечуючи документообіг у всій системі Національної поліції України та між всіма структурними підрозділами та відповідними посадовими особами, як увесь підрозділ так і окремі зазначені його працівники зобов'язані дотримуватися стандартів інформаційної безпеки в діяльності Національної поліції України та реалізовувати відповідні функції та завдання вказаного вище адміністративно-правового механізму.

Відповідно до Інструкції з діловодства в системі Міністерства внутрішніх справ України, підрозділами документального забезпечення є Управління документального забезпечення, управління, відділи, сектори документального забезпечення, канцелярії структурних підрозділів апарату Міністерства, ГУМВС, УМВС, науково-

дослідних установ, вищих навчальних закладів МВС, підприємств, установ, організацій, що належать до сфери управління МВС. При цьому, зазначеним наказом, передбачається також функціонування низки автоматизованих систем (АПС «Канцелярія» – автоматизована інформаційно-пошукова система «Канцелярія», що використовується для автоматизації процесів діловодства (облік документів шляхом створення електронних реєстраційних карток та накопичення інформації про рух і виконання документів) за допомогою комп'ютерної техніки) та загалом передбачається використання в діяльності підрозділів електронно-обчислювальної техніки [97]. Можна підкреслити, що використання різноманітних інформаційно-аналітичних систем, у тому числі для забезпечення ефективного документообігу в діяльності Національної поліції України, додатково регулюється державними стандартами у відповідній сфері та координується Державною службою спеціального зв'язку та захисту інформації України, хоч окремі аспекти зазначеного питання та безпосереднє розпорядження вказаними ресурсами здійснюється підрозділами документального забезпечення, а контроль за законністю їх використання в повсякденній службовій діяльності покладається на підрозділи оперативного реагування та контролю, внутрішньої безпеки та інші компетентні підрозділи із числа поліцейських.

Із функціональної точки зору документаційне забезпечення управління є самостійною функцією організації поряд з іншими управлінськими функціями (такими, як забезпечення персоналом, матеріально-технічне забезпечення, забезпечення фінансами тощо). Воно властиве кожній організації незалежно від її організаційно-правової

форми, характеру і напрямів діяльності насамперед тому, що передбачає здійснення діяльності у роботі з документами [146, с. 48–49]. Ключовим суб'єктом у системі документального забезпечення публічного адміністрування виступає Департамент документального забезпечення Національної поліції, крім того, у територіальних та міжтериторіальних органах поліції створюються власні підрозділи документального забезпечення. Основним завданням цього поліцейського підрозділу є встановлення в Національній поліції України єдиного порядку документування управлінської інформації і роботи з документами із застосуванням сучасних автоматизованих систем, методичне керівництво і контроль за дотриманням встановленого порядку роботи з документами в структурних підрозділах апарату поліції [19]. Належить підкреслити, що організаційно-штатна структура Департаменту документального забезпечення Національної поліції України та коло визначених йому завдань, відповідно до зазначеного вище положення, цілком і повністю охоплює діяльність за даним напрямом у всій Національній поліції України, попри інституційну підпорядкованість окремих підрозділів документального забезпечення самостійним міжрегіональним територіальним підрозділам. Крім цього, слід зауважити, що єдність інституційної структури підрозділів документального забезпечення Національної поліції України забезпечує ефективну реалізацію принципів стандартів і засад інформаційної безпеки в діяльності Національної поліції України та дію відповідного адміністративно-правового механізму.

Основними повноваженнями Департаменту документального забезпечення Національної поліції та

відповідних підрозділів на нижчих щаблях системи поліції слід визначити такі: розробка нормативно-правового забезпечення здійснення діловодства та номенклатури справ поліцейських органів та підрозділів; реєстрація та облік документів; організація документообігу, формування справ, їх зберігання та підготовка до передачі на архівне зберігання; контроль за дотриманням структурними підрозділами вимог інструкцій, регламентів та національних стандартів з питань діловодства; перевірка стану діловодства у відокремлених підрозділах; забезпечення дотримання єдиних вимог щодо підготовки документів та організації роботи з ними у тому числі в умовах електронного документообігу; здійснення аналізу інформації про документообіг, необхідної для прийняття управлінських рішень; участь в організації підвищення кваліфікації працівників Національної поліції України з питань діловодства [19; 98]. Слід зазначити, що формування, ведення та зберігання окремих контрольно-наглядових справ щодо діяльності різних підрозділів Національної поліції України, відбувається відповідно до затвердженої номенклатури справ, котра формується, перш за все, підрозділами документального забезпечення та порядок зберігання якої визначається ними ж. Необхідно підкреслити, що зміст і сутність діяльності окремих підрозділів Національної поліції України вимагає дотримання інформаційного режимних обмежень, а збирана в процесі службової діяльності персональна інформація окремих осіб, а також службова інформація, отримана у результаті реалізації окремих поліцейських завдань (функцій) має бути належним чином збережена. Це і відображає сутність ролі і місця підрозділів документального забезпечення Національної поліції України, як суб'єкта реалізації адміністративно-

правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України.

Режимно-секретні підрозділи. На сам кінець слід зауважити на надзвичайно важливі ролі підрозділів режимно-секретної роботи, як одного зі стратегічних напрямів у правоохоронній діяльності загалом та реалізації адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України, зокрема. Діяльність всіх, без виключення, органів про порядку не завжди є гласною до певної пори й передбачає використання, збирання та аналіз інформації із різним режимом таємності. Порядок надання гласності чітко визначається законодавством України, а можливість роботи з нею надається безпосередньо Службою безпеки України. Саме тому режимно-секретні підрозділи, на нашу думку, відіграють чи не найважливішу роль у адміністративно-правовому механізмі забезпечення інформаційної безпеки в діяльності Національної поліції України, як один із компонентів організації механізму правоохоронної діяльності, що в свою чергу уможливорює виконання поліцією покладе на неї завдань із забезпечення прав і свобод людини і громадянина та підтримання правопорядку в суспільстві.

На сучасному етапі реформування правоохоронної системи в Україні в умовах соціально-економічних, політичних зрушень, оновлення законодавства зумовлюють необхідність особливої уваги до проблем забезпечення режиму секретності у проведенні оперативно-технічних заходів і негласних слідчих (розшукових) дій, оскільки у процесі оперативно-службової, слідчої діяльності співробітники органів Національної поліції мають справу з інформацією, яка не підлягає широкому розповсюдженню. Ця

інформація стосується окремих форм, методів, прийомів і результатів діяльності органів Національної поліції щодо вирішення завдань протидії злочинності, зміцнення правопорядку й віднесена законодавством до категорії державної таємниці [79; 96]. Відповідно, правовий режим зазначеної інформації чітко регулюється законодавством України, у тому числі кримінально-процесуальним. Проте, адміністративно-правовий режим поводження з такою інформацією врегульовується окремими підзаконними нормативно-правовими актами, що носять адміністративно-юрисдикційний зміст та безпосередньо складають механізм адміністративно-правового регулювання інформаційної безпеки в діяльності Національної поліції України, оскільки одним із основних її завдань є забезпечення правопорядку в суспільстві та прав і свобод людини і громадянина, зокрема у спосіб використання окремих форм, методів, прийомів і результатів своєї діяльності, що відноситься до категорії державної таємниці України.

Стаття 1 Закону України «Про державну таємницю» визначає державну таємницю (також – секретна інформація) як вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою. Віднесення інформації до державної таємниці – процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди

національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього. Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого включена ця інформація, чи зміни до нього у порядку, встановленому цим Законом [24; 96]. Відповідно, слід підкреслити, що коло компетенції режимно-секретних підрозділів у реалізації адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України, як одного з органів правопорядку, що використовує в своїй діяльності секретну інформацію є надзвичайно важливим та необхідним. При цьому, належить підкреслити, що чи не найважливішу роль у даному аспекті та забезпеченні контролю за цим напрямом роботи та в даному контексті відіграє Служба безпеки України, котра є основним регулятором обігу секретної інформації в державі.

Захист відомостей, що належать до державної таємниці у сфері кримінальної процесуальної та оперативно-розшукової діяльності, також забезпечується чітко визначеним законом порядком допуску та доступу осіб до таких відомостей. У зв'язку з допуском до державної таємниці на працівників органів Національної поліції покладаються певні обов'язки – загальні та спеціальні. Загальні обов'язки поділяються на дві групи: перша передбачає вимоги, для додержання яких працівники мають виконувати активні правові дії із забезпечення режиму секретності і конспірації; друга містить обов'язки у формі правових зобов'язань, спрямованих на необхідність утримання від певних дій, що можуть

спричинити виток секретних відомостей, втрату секретних документів або завдати іншої шкоди охороні державної таємниці [37, с. 16–17]. Оскільки зміст і сутність правоохоронної поліцейської діяльності полягає в необхідності здійснення досудового розслідування у межах визначеної підслідності, а також провадження оперативно-розшукової діяльності в окремих сферах правоохорони, що в свою чергу, у межах протидії тяжкій злочинності неможливо без використання негласних слідчих розшукових дій, питання реалізації основних засад дії у тому числі адміністративно-правового механізму у сфері інформаційної безпеки в діяльності Національної поліції України є надзвичайно важливим, а роль і місце режимно-секретних підрозділів відповідного органу державної влади визначальною.

2.3. Суб'єкти забезпечення інформаційної безпеки в Національній поліції України

Необхідно зазначити, що дія адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України передбачає не лише здійснення правового регулювання у даній сфері, а й зобов'язана та повинна визначати коло відповідальності за порушення вказаних у законодавстві України вимог, щодо інформаційної безпеки в діяльності не лише поліції, а й всіх органів державної влади. Інститут адміністративної відповідальності є одним із основоположних в структурі будь-якого адміністративно-правового механізму, без якого неможливе

його функціонування, оскільки правове регулювання за своїм змістом не може бути досконалим та остаточним без наявності структурованого та змістовно побудованого механізму притягнення до відповідальності осіб, що порушують засади відповідного правового режиму.

Водночас, слід звернути увагу на тому, що хоч реалізація адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України і передбачає чіткість та виваженість адміністративно-правових конструкцій, інструменти притягнення до відповідальності в залежності від міри та змісту вчиненого правопорушення можуть застосовуватись з урахуванням вимог у тому числі кримінального чи цивільного законодавства.

З розвитком всесвітньої мережі Інтернет і збільшенням ступеня комп'ютерної грамотності суспільства проблема забезпечення безпеки локальних мереж і конфіденційності інформації, що у них циркулює, здобуває особливої актуальності. Це обумовлено тим, що будь-який користувач Інтернету може одержати доступ до інформаційних ресурсів будь-якого комп'ютера, підключеного до мережі Інтернет. Крім того, якщо сервер, з'єднаний з Інтернетом, одночасно слугує сервером локальної мережі, то можливе несанкціоноване проникнення в локальну мережу. Необхідність захисту інформації виникає також при пересиланні файлів і програм між Web-вузлами й комп'ютером. Без використання надійної системи захисту комп'ютера існує загроза проникнення (злому) хакерів і, як наслідок, втрати або ушкодження особистих даних, які зберігаються на комп'ютері або ноутбуці [32].

Галузь обігу інформації та відповідно інформаційної безпеки у зазначених правопорушеннях є додатковим об'єктом, на який зазіхає правопорушення. У зв'язку з цим вважаємо, що окремі склади правопорушень необхідно перенести до глави 10 КУпАП, оскільки стан, в якому адміністративно-правові норми знаходяться сьогодні, не може вважатися задовільним. Логіка побудови КУпАП потребує об'єднання цих складів в одному розділі. Знаходження складів адміністративних правопорушень, скоєних у сфері обігу інформації, в єдиному розділі дозволить виключити низку проблем, пов'язаних із кваліфікацією досліджуваних нами деліктів. З урахуванням викладеного можна констатувати, що виникнення адміністративних деліктних правовідносин у сфері обігу інформації контексті забезпечення інформаційної безпеки пов'язані зі скоєнням правопорушень у інформаційному просторі. Сутність адміністративно-деліктних правовідносин проявляється у захисті суспільних відносин, які зазнали негативного впливу внаслідок скоєння адміністративного правопорушення. Відповідно до вироблених теоретичних положень, адміністративно-деліктні правовідносини регулюються матеріальними адміністративно-деліктними нормами, та процесуальними. Адміністративно-деліктне право поєднує інститут матеріальних та процесуальних норм. Матеріальні норми адміністративно-деліктного права спрямовані на регулювання відносин лише між державою в особі уповноважених державних органів і посадовими особами та особою, яка скоїла адміністративне правопорушення. Процесуальні адміністративно-деліктні норми переважно спрямовані на регулювання правовідносин, що виникають під час здійснення провадження у справі про

адміністративне правопорушення. Процесуальні норми дають змогу реалізувати адміністративну відповідальність [54].

Так, потрібно нагадати про те, що КУпАП відносить поліцейських до спеціальних суб'єктів адміністративної відповідальності (стаття 15). Так, військовослужбовці, військовозобов'язані та резервісти під час проходження зборів, а також особи начальницького складу Національного антикорупційного бюро України, Бюро економічної безпеки України, рядового і начальницького складу Державної кримінально-виконавчої служби України, служби цивільного захисту, Державного бюро розслідувань, поліцейські несуть відповідальність за адміністративні правопорушення за дисциплінарними статутами. Водночас, у разі порушення певних правил, норм і стандартів, зазначені особи несуть адміністративну відповідальність на загальних підставах, за винятком застосування до них окремих видів адміністративних стягнень [55; 107].

Адміністративно-правовий зміст інформаційної безпеки серед науковців характеризується різними за пошуками напрямками, що свідчать про їх намагання дослідити і запропонувати розв'язання проблем, які пов'язані з інформацією, інформаційною безпекою, інформаційними технологіями. Серед напрямів протидії тероризму, вчинення якого посягає на національну безпеку України, на думку М. А. Микитюка, повинно стати підвищення ефективності інформаційного забезпечення суб'єктів боротьби з тероризмом, у тому числі, надання їм доступу до інформаційних ресурсів органів державної влади в порядку, встановленому законодавством [72, с. 305]. Водночас, науковець розглядає лише внутрішньоорганізаційне забезпечення режиму інформаційної безпеки, крізь призму дії

відповідного адміністративно-правового механізму в той час, як зовнішньо правоохоронна діяльність Національної поліції України та дотримання режиму інформаційної безпеки, в даному контексті, залишається поза увагою, що на нашу думку не впливає на забезпечення інформаційної безпеки та дію відповідного адміністративно-правового механізму в загальнодержавному та внутрішньовідомчому контексті.

В контексті вищезазначеного, тут варто погодитись з думкою Л. Чистоклетова та О. Хитри про те, що в сучасному суспільстві складається тенденція ускладнення завдань забезпечення безпеки особистості, пов'язаних із застосуванням інформаційно-електронних технологій. При цьому сприяють також численні пробіли в законодавстві, що регулює відносини в інформаційній сфері. Серед інших видів засобів адміністративно-правового примусу не менш важливу роль у сфері інформаційної безпеки відіграє адміністративна відповідальність. Нині інститут юридичної відповідальності посідає особливе місце в юриспруденції, проблемами якої займаються правознавці у різних галузях права, і як свідчить сьогоднішні реалії, є частиною системи інформаційного правопорядку, який закладає правові підвалини для нормального функціонування та розвитку інформаційного суспільства. Разом з тим, практика розгляду справ про адміністративні правопорушення у сфері забезпечення інформаційного законодавства свідчать про наявність певних прогалин в механізмі адміністративно-правового забезпечення прав, свободи і інтересів суб'єктів інформаційного права, що створює перешкоди в правоохоронній та правозастосовній діяльності, а також запобіганні та виявленні вказаного виду правопорушення [142]. Таким чином можна стверджувати, що в даний час

інститут адміністративної відповідальності в інформаційній сфері знаходиться на стадії становлення та удосконалення, він є своєрідним специфічним інструментом правового регулювання, що зумовлений природою інформаційних правовідносин [68]. На нашу думку, слід погодитися з позицією автора та зазначити на тому, що інститут адміністративної відповідальності за порушення правових інформаційних режимів є основою функціонування будь-якого правового режиму. Водночас, швидкоплинність взаємин у даній сфері, а також динамічний розвиток цифрових технологій, у тому числі технології з обміну інформацією, зумовлює необхідність системного перегляду складів адміністративних правопорушень, що й визначають власне, що саме є адміністративним правопорушенням.

За вчинення адміністративних проступків на правопорушників накладаються відповідні адміністративні стягнення, що мають для особи негативні наслідки морального або матеріального характеру (попередження; штраф; оплатне вилучення предмета, який став знаряддям вчинення або безпосереднім об'єктом адміністративного правопорушення; конфіскація: а) предмета, який став знаряддям вчинення або безпосереднім об'єктом адміністративного правопорушення; б) грошей, одержаних унаслідок вчинення адміністративного правопорушення; позбавлення спеціального права, наданого громадянину (права керування транспортними засобами, права полювання); громадські роботи; виправні роботи; адміністративний арешт тощо); заходи впливу (зобов'язання публічно або в іншій формі попросити вибачення у потерпілого; попередження; догана або суворі догани; передача неповнолітнього під нагляд батькам або особам, які

їх замінюють, чи під нагляд педагогічному або трудовому колективу за їхньою згодою, а також окремим громадянам на їхнє прохання); адміністративне видворення за межі України іноземних громадян і осіб без громадянства (ст. 24-32 КУпАП) [127].

Охоронювані адміністративно-правовими засобами формально визначеними у Конституції України та інших нормативно-правових актах інформаційні права, свободи і законні інтереси громадян. Ці інтереси можна назвати об'єктами безпеки у сфері адміністративно-правового регулювання, до яких належать: порушення законодавства про державну таємницю (ст. 212-2 КУпАП); порушення права на інформацію та права на звернення (ст. 212-3 КУпАП); порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію (ст. 212-5 КУпАП); здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем (ст. 212-6 КУпАП) [56; 83]. Слід зауважити, що всі окреслені юридичні склади, що чітко встановлюється кодексом України про адміністративні правопорушення прямо чи опосередковано забезпечують реалізація інституту притягнення до юридичної відповідальності осіб, що порушили правові інформаційні режими, проте, здійснення провадження в дисциплінарному порядку ними не передбачається, хоча поліцейський, як посадова особа Національної поліції України, має бути притягнутий і до неї також. При цьому, необхідно звернути увагу на чіткому розмежуванні адміністративної та кримінальної відповідальності за порушення режиму

інформаційної безпеки в діяльності Національної поліції України, оскільки в залежності від того наскільки тяжким є діяння тієї чи іншої особи релевантною може бути і юридична кваліфікація та відповідно покарання.

До числа адміністративних правопорушень також слід віднести порушення права на об'єкти права інтелектуальної власності, передбаченого ст. 512 КУпАП (глава 6 «Адміністративні правопорушення, що посягають на власність»). Поняття інтелектуальної власності розуміють у значенні, проголошеному в Конвенції «Про заснування Всесвітньої організації інтелектуальної власності», що була підписана в Стокгольмі 14 липня 1967 р. У ст. 2 Конвенції закріплено положення, що «інтелектуальна власність» містить права, які стосуються: літературних, художніх і наукових творів; виконавчої діяльності артистів, звукозапису, радіо- і телевізійних передач; винаходів у всіх сферах діяльності людини; наукових відкриттів; промислових зразків; товарних знаків, знаків обслуговування, фірмових найменувань і комерційних позначень; захисту від недобросовісної конкуренції; всі інші права, що стосуються інтелектуальної діяльності у виробничій, науковій, літературній та художній сферах [127]. Належить підкреслити, що цей приклад може бути своєчасним та корисним у контексті використання в процесі службової діяльності поліцейськими тих чи інших літературних, художніх і наукових творів, право власності на які мають інші особи чи громадяни. Водночас, правові інформаційні режими пов'язані з віднесенням інформації, що стала доказом у кримінальному провадженні чи під час провадження у справах про адміністративні правопорушення, чітко регулюють зазначені позиції та унеможливають незаконне

поводження з нею, а також встановлює чітку відповідальність за порушення відповідних приписів і вимог.

Суб'єктами правопорушень у сфері інформаційних відносин, за якими настає адміністративна відповідальність, є посадові та службові особи, що мають доступ до відповідної інформації; громадяни, які займаються підприємницькою діяльністю; працівники торгівлі, громадського харчування, сфери послуг; посадові особи підприємств, установ, організацій; суб'єкти первинного фінансового моніторингу тощо. Слід зазначити, що досить важливим у реалізації права на інформацію є її повнота та достовірність, а у разі надання інформації ще й своєчасність. Відсутність цих факторів є в багатьох випадках підставою вчинення адміністративних правопорушень посадовими особами, в тому числі і шляхом зловживання свого посадового становища. Аналіз законодавства дає зробити висновок, що адміністративна відповідальність за правопорушення у сфері інформаційного права має наслідки у вигляді штрафу, який встановлюється для кожного окремого випадку і в тих межах, що визначені відповідною нормою. Адміністративне стягнення накладається лише на фізичних осіб [145]. Пов'язуючи даний аспект з дотриманням режиму інформаційної безпеки в діяльності Національної поліції України, належить зауважити, що всі без виключення звернення громадян, а також відповідні інформаційні запити, у тому числі звернення і запити народних депутатів України, чи будь-які інші інформаційні звернення, що прямо передбачені законодавством України, мають бути розглянуті у встановлений законодавством України строк із дотриманням вимог принципу своєчасності повноти та об'єктивності. В свою чергу, українське законодавство безпосередньо

передбачає відповідальність за недотримання вимог відповідних положень, що в свою чергу і приводить в дію інститут юридичної відповідальності в межах адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України.

Особливість порядку правового регулювання, встановленого державою у вигляді правових норм, забезпечується силою державного примусу за допомогою контролю будь-яких дій з інформацією, включаючи збирання, систематизацію, накопичення, зберігання, уточнення, оновлення, зміну, використання, поширення, передачу, блокування, знищення. У сфері обігу інформації зміст адміністративно-деліктних правовідносин безпосередньо пов'язаний із вчиненням делікту, відповідальність за який передбачено нормою Кодексу України про адміністративні правопорушення [17]. Логічним є підкреслити, що інститут юридичної відповідальності за порушення відповідного інформаційно-правового режиму, зокрема в діяльності Національної поліції України, потребує пильної уваги та здійснення оцінки всіх без виключення суттєвих обставин, в тому числі тих, що формують специфіку поліцейської діяльності та адміністративно-правового статусу поліцейського.

Як зазначено в аналітичній записці Національного інституту стратегічних досліджень при Президентові України «Проблеми інформаційного законодавства України у сфері створення, поширення й використання інформації й шляхи їхнього рішення» [105] в Україні правову основу діяльності у сфері телекомунікації складають Конституція України, Закон України «Про телекомунікацію» та інші нормативно-правові

акти, що регулюють відносини в цій сфері [33]. Проте, підкреслюючи зміст і сутність відповідних юридичних документів належать зауважити, що не всі з них прямо визначають конкретні форми та види юридичної відповідальності, що настає за порушення режимних та безпекових обмежень обігу інформації в загальнодержавному розумінні, а також діяльності окремих центральних органів державної влади в Україні, зокрема і Національній поліції України. Доктринальним, з точки зору приведення в дію інституту відповідальності є Кодекс України про адміністративні правопорушення, що визначає зміст і сутність протиправних діянь, а також окреслює міру відповідальності до якої буде притягнута особу, що їх вчинить.

У випадках, за яких порушуються встановлені правила, виникають деліктні адміністративні правовідносини у сфері обігу інформації. Адміністративно-деліктні відносини у сфері обігу інформації є різновидом правовідносин у сфері державного управління; виникають у односторонньому порядку з ініціативи уповноваженого органу чи посадової особи як реакція порушення норми права, що передбачає адміністративну відповідальність; пов'язані з виявленням та фіксацією факту вчинення адміністративного делікту, розглядом справи про адміністративне правопорушення та рішення, виконання прийнятого у справі рішення на основі матеріальних та процесуальних адміністративно-правових норм. Законодавець розкриває поняття адміністративного правопорушення шляхом визначення його основних характеристик [2, с. 487]. Проведення диференціації деліктів у сфері інформації дозволило визначити групи деліктів у сфері обігу інформації щодо інформаційної безпеки: делікти у

сфері обігу інформації, пов'язані з порушенням встановлених термінів виконання операцій з інформацією; делікти, пов'язані з порушенням встановленого порядку надання даних; делікти, що виникли через неналежне виконання обов'язків особами з поводження з інформацією, на яких покладені у зв'язку з професійною діяльністю. Адміністративні деліктні правовідносини у сфері обігу інформації, які впливають на стан інформаційної безпеки мають матеріальну та процесуальну складову. Матеріальні норми дозволяють визначити, що є правопорушенням у сфері інформаційної безпеки [54]. На вашу думку, слід повністю погодитись із запропонованою диференціацією правопорушень у сфері обігу інформації то додатково окреслити, що всі вони застосовані до діяльності Національної поліції України, оскільки вона є центральним органом державної виконавчої влади в Україні, до кола компетенції якої відноситься, як обов'язок надання будь-якої інформації за запитом чи зверненням в установленому законодавством України порядку, так і забезпечення законного та безпечного обігу всіх персональних даних та будь-якої іншої службової інформації, що використовується в її діяльності, відповідно до норм і положень законодавства України у сфері інформації.

Слід звернути увагу також на те, що деякі вчені відносять до кола інформаційних адміністративних правопорушень набагато ширший перелік, ніж було зазначено попередньо, а саме тому, на нашу думку, посилаючись на позицію авторитетних дослідників необхідно чітко вказати, про які саме статті Кодексу України про адміністративні правопорушення йдеться.

До правопорушень, які скоєні у сфері обігу інформації інформаційної безпеки, належать: ст. 41-3 «Ненадання інформації для ведення колективних переговорів і здійснення контролю за виконанням колективних договорів, угод»; ст. 82-3 «Приховування, перекручення або відмова від надання повної та достовірної інформації за запитами посадових осіб і зверненнями громадян та їх об'єднань щодо безпеки утворення відходів та поводження з ними»; ст. 163-5 «Приховування інформації про діяльність емітента»; ст. 163-9 «Незаконне використання інсайдерської інформації»; ст. 163-11 «Порушення порядку розкриття інформації на фондовому ринку»; ст. 166-4 «Порушення порядку подання інформації та виконання рішень Антимонопольного комітету України та його територіальних відділень»; ст. 172-8 «Незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових повноважень»; ст. 184-2 «Порушення порядку або строків подання інформації про дітей-сиріт і дітей, які залишилися без опіки (піклування) батьків»; ст. 186-6 «Порушення законодавства про друковані засоби масової інформації»; ст. 188-31 «Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України»; ст. 188-47 «Порушення встановленого законом порядку отримання інформації з Єдиного державного реєстру, держателем якого є Державтоінспекція Міністерства внутрішніх справ України, Державного реєстру речових прав на нерухоме майно, Державного земельного кадастру»; ст. 195-5 «Незаконне зберігання спеціальних технічних засобів негласного отримання інформації»; ст. 212-3 «Порушення права на інформацію та права на звернення»; ст. 212-5 «Порушення порядку обліку, зберігання і використання документів та

інших матеріальних носіїв інформації, що містять службову інформацію», ст. 212-6 «Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем»; ст. 212-9 «Порушення порядку ведення передвиборної агітації, агітації під час підготовки і проведення референдуму з використанням засобів масової інформації та порядку участі в інформаційному забезпеченні виборів»; ст. 212-11 «Ненадання можливості оприлюднити відповідь щодо інформації, поширеної стосовно суб'єкта виборчого процесу»; ст. 212-13 «Виготовлення або розповсюдження друкованих матеріалів передвиборної агітації, які не містять відомостей про установу, що здійснила друк, їх тираж, інформацію про осіб, відповідальних за випуск» [54]. Таким чином Кодекс України про адміністративні правопорушення регулює юридичну відповідальність за порушення правових інформаційних режимів, зокрема в діяльності Національної поліції України та поширює свою юридичну силу не лише на відповідних суб'єктів із числа поліцейських, а й на цивільних осіб, що так само можуть вчинити зазначені правопорушення чи взяти участь в їх учиненні. Водночас, на нашу думку, вказані норми все ще потребують доопрацювання, з урахуванням сучасних викликів.

Зовнішня експертиза, що неодноразово проводилася в Україні, зокрема представниками Організації з безпеки й співробітництва в Європі, підтверджує, що законодавча й нормативно-правова база функціонування інформаційної сфери України в цілому відповідає європейським нормам і стандартам. Виходячи із цього, можна затверджувати, що сьогодні в Україні вже створені основи такої галузі

законодавства як інформаційне право. Проте, важливою проблемою залишається деяка несистемність вітчизняної правової політики в інформаційній сфері, зокрема зважаючи на те, що законодавчі акти приймаються з метою рішення тактичних задач, без обліку стратегічних орієнтирів і об'єктивних українських умов [86, с. 24]. Водночас, належить зауважити, що дискусія щодо встановлення інформаційно-правової відповідальності в українському суспільстві та правовому просторі триває не один рік й не знаходить належної аргументації необхідності її введення.

Процесуальні норми необхідні для регламентації провадження у справах про адміністративні правопорушення у галузі обігу інформації, найбільш важливим є процес доведення вини у скоєнні правопорушення в інформаційному просторі. За характером впливу (наявності обмежень прав) розглянута група процесуальних заходів підрозділяється на примусові та заходи не примусового характеру [36]. Вчені пропонували розмежувати адміністративні правопорушення, об'єднані у главі 10 Кодексу, на групи правопорушень: у сфері електронних комунікацій; у сфері свободи масової інформації; що посягають на встановлений законом порядок збирання, зберігання, використання, розповсюдження чи захисту інформації; що зазіхають загальні відносини у сфері інформації [42, с. 433]. Ця класифікація має позитивні сторони, зокрема, розмежовує правопорушення у сфері комунікацій та інформації, підкреслюючи необхідність правового захисту цієї групи суспільних відносин. Але класифікації властиві окремі недоліки. Виділяти в окрему групу загальні відносини у сфері інформації недоцільно, оскільки відсутній коментар, що дозволяє усвідомити, які саме правовідносини слід відносити до цієї групи [54].

Належить цілком і повністю погодитись із запропонованим, оскільки виважена та аргументована диференціація тих чи інших складів адміністративних правопорушень пов'язаних із недотриманням інформаційна безпекових режимів діяльності Національної поліції України зокрема, та відповідного інституту в загальнодержавному значенні загалом, дозволить більш ефективно здійснювати заходи, щодо притягнення до адміністративної відповідальності винних у вчиненні указаних діянь осіб, а також убезпечить дію вказаного механізму від необґрунтованого затягування необ'єктивності оцінки отриманих доказів та необґрунтованого та неправомірного притягнення до зазначеного виду відповідальності невинних осіб.

Необхідно зазначити, що об'єктом адміністративно-правового захисту є охоронювані і порушені права, свободи та інтереси фізичних осіб, права та інтереси юридичних осіб. Адміністративно-правовий захист здійснюється адміністративно-правовими засобами у випадку порушення охоронюваного права. Найчастіше застосовуваним адміністративно-правовим засобом є притягнення винної особи до адміністративної відповідальності, яка настає за посягання на об'єкт адміністративно-правового захисту. Тобто об'єкт адміністративно-правового захисту та об'єкт адміністративного правопорушення часто можуть співпадати. Об'єктом адміністративного правопорушення є суспільні відносини, які охороняються нормами законодавства про адміністративні правопорушення. Таким чином, об'єктом адміністративно-правового захисту також є суспільні відносини, які охороняються нормами законодавства про адміністративні правопорушення, а авторське право як об'єкт адміністративно-правового захисту – це суспільні відносини,

які охороняються нормами законодавства про адміністративні правопорушення [5, с. 159]. Слід зауважити на чіткому розмежуванні об'єктів адміністративно-правового захисту, у контексті дії відповідного адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України, оскільки до зазначеної категорії відноситься не вся інформація. Відповідно, враховуючи поліваріативність трактування поняття об'єкту адміністративно-правового захисту, в даному контексті, корелюється також зміст і сутність інституту юридичної та зокрема адміністративної відповідальності, а також міра та зміст покарання, що може бути застосоване до конкретної особи.

Слушною, на нашу думку, є позиція Л.І. Каленіченко, яка вважає, що «особливості юридичної відповідальності працівників Національної поліції України полягають у такому: 1) працівники Національної поліції України, як особи, що перебувають на державній службі й виконують відповідні функції та завдання держави, мають вищий рівень юридичної відповідальності, ніж інші громадяни; при цьому показово, що до працівників Національної поліції України можуть застосовуватися всі види юридичної відповідальності, що й до загальних суб'єктів права; 2) працівники Національної поліції України, як особи, що перебувають на державній службі та покликані служити суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки й порядку, мають специфічний набір підстав юридичної відповідальності; 3) обсяг підстав юридичної відповідальності працівників Національної поліції України є ширшим, ніж обсяг підстав юридичної відповідальності

загальних суб'єктів права; 4) склад правопорушення працівника Національної поліції України є специфічним, тісно пов'язаним з його державно-владними повноваженнями» [50, с. 28]. Належать цілком і повністю погодитися із зазначеними особливостями юридичної, зокрема і адміністративної відповідальності працівників Національної поліції України в контексті дотримання адміністративно-правового режиму інформаційної безпеки в діяльності відповідного центрального органу виконавчої влади та підкреслити, що він потребує удосконалення, зокрема в частині чіткого структурування складів адміністративних правопорушень, а також їх розширення, зокрема через стрімкі євроінтеграційні процеси та необхідність адаптації українського законодавства до актів права Європейського союзу, а також цифровізації суспільства, що невпинно відкриває нові сфери обігу інформації та відповідно потребує нових заходів і засобів її захисту зокрема і правового.

Висновки до розділу 2

Зміст і сутність нормативно-правового регулювання адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України, перш за все, базується на необхідності уточнення інформаційної складової, що полягає у визначенні змісту та сутності цього соціально-правового явища та за результатами окреслення відповідних характеристик формування загального уявлення про ті методи та способи адміністративно-правового

регулювання, що найбільш ефективно можуть забезпечити його безпеку.

Так, імперативний метод крізь призму нормативного його забезпечення розглядається, як можливість Національної поліції України не допустити витоку тієї чи іншої інформації пов'язаної з персональними даними особами чи будь-якою іншою, що використовується нею в службовій діяльності, а також у наявності можливості притягнути до юридичної відповідальності конкретну особу за необережності чи умислу якої виник такий виток і особу, яка незаконно заволоділа зазначеною інформацією. Правове регулювання із використанням диспозитивного методу, в свою чергу, полягає в створенні таких нормативно-правових та організаційно-управлінських підвалин, що превентивно діють на інститут інформаційної безпеки та створюють всі необхідні умови і засади для недопущення незаконних дій з інформацією чи тих, що можуть потягнути протиправні наслідки для суспільства та держави загалом.

Чіткий розподіл суб'єктів, що здійснюють реалізацію адміністративно-правового механізму забезпечення інформаційної безпеки в тому числі в діяльності Національної поліції України запобігає неефективному здійсненню своїх повноважень та необґрунтованим витратам трудових ресурсів органів державної влади. При цьому слід підкреслити, що поділ вказаних суб'єктів може здійснюватися, як за горизонтальним так і вертикальним принципом, при цьому, враховувати компетенцію відповідних органів державної влади, щодо здійснення правового регулювання того чи іншого аспекту сфери інформаційної безпеки, в тому числі в діяльності Національної поліції України. Так, до одного з найбільш

важливих критеріїв також слід віднести, як зовнішньо так і внутрішню організаційну структуру суб'єктів забезпечення інформаційної безпеки в Національній поліції України, як одному з центральних органів виконавчої влади та безпосередньо в ній самій, як самостійному органі правопорядку.

До кола суб'єктів реалізації адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України належать: вищі органи державної влади України (Верховна Рада України, Кабінет Міністрів України, а також інститут Президента України та вертикаль судової влади); центральні органи виконавчої влади, що мають повноваження у сфері забезпечення інформаційної безпеки загалом і в Національній поліції України зокрема (кожен окремо взятий центральний орган виконавчої влади, що входить до структури Кабінету Міністрів України, що координуються ним через певне Міністерство чи конкретного міністра; суб'єкти забезпечення інформаційної безпеки в Національній поліції України (до кола яких належать підрозділи кіберполіції, підрозділи організаційно-аналітичної роботи й контролю, підрозділи документального забезпечення, режимно-секретні підрозділи.

Умови та обставини зокрема в службовій діяльності Національної поліції України зумовлюють ще більші ризики, що в свою чергу потребує удосконалення адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України, зокрема і в спосіб удосконалення інституту відповідальності за неправомірні чи незаконні дії з будь-якою інформацією, що була отримана відповідними особами в результаті провадження та реалізації своїх службових повноважень чи виконання обов'язків.

Неминучість притягнення до певного виду юридичної відповідальності, в залежності від тяжкості вчиненого правопорушення прямо передбачається Конституцією України та втілюється в інших нормах і актах законодавства.

Крім цього, інститут притягнення до юридичної відповідальності осіб, що порушили такі інформаційно-правові режими, так само прямо визначається як Законом України «Про Національну поліцію», щодо здійснення дисциплінарного провадження відносно такої особи так і Кодексом України про адміністративні правопорушення, де прямо передбачається низка форм і видів відповідальностей, до яких може бути притягнуто інших осіб, що вчинили неправомірні чи незаконні дії. Крім цього, Кодекс України про адміністративні правопорушення чітко та змістовно регулює інститут юридичної відповідальності за порушення правових інформаційних режимів, зокрема в діяльності Національної поліції України та поширює свою юридичну силу не лише на відповідних суб'єктів із числа поліцейських, а й на цивільних осіб, що так само можуть вчинити зазначені правопорушення чи взяти участь в їх учиненні.

РОЗДІЛ 3. УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ

3.1. Зарубіжний досвід забезпечення інформаційної безпеки в поліцейських підрозділах та шляхи його запровадження в Україні

Нами підкреслюється, що необхідність використання зарубіжного досвіду забезпечення інформаційної безпеки в поліцейських підрозділах, а також аналіз шляхів його запровадження в Україні є необхідною умовою оптимізації будь-якого державницького процесу, оскільки лише завдяки залученню позитивних міжнародних практик, на основі конкретних зарубіжних прикладів можливим є оптимізація системи адміністративно-правового забезпечення всіх без виключення процесів в Україні.

Надзвичайної важливості та актуальності вказане питання набуває з огляду на те, що Україна обравши своїм шляхом інтеграцію до Європейського Союзу, а також розпочавши перемовини, щодо цього процесу взяла на себе зобов'язання адаптувати національне законодавство до актів права Європейського Союзу, що потребує значних зусиль, зокрема і науково-дослідницьких, у частині вивчення вказаних актів права Європейського Союзу та позитивного досвіду забезпечення інформаційної безпеки зокрема в поліцейських підрозділах інших країн.

Слід звернути увагу на той факт, що на початку ХХІ століття глобалізаційні процеси по всьому світі, суттєві зміни в інформаційних системах розвинутих і перехідних країнах спричинили підвищення наукового інтересу до вивчення проблем безпеки та переосмислення місця інформаційної безпеки в ієрархії потреб людини і суспільства. Необхідність забезпечення інформаційної складової національної безпеки є вихідною соціально-правовою потребою суспільства і держави. Саме через призму безпековості і необхідності захисту від різних інформаційних загроз забезпечується рівень цивілізації й державності [32].

Становлення правового регулювання сфери інформаційної безпеки розпочалось наприкінці ХХ століття. Насамперед, усвідомлення загроз, що виникають у зв'язку з розвитком інформаційних технологій, соціально-економічними, військовими та політичними наслідками останньої інформаційної революції, мало місце в країнах, що перші розпочали активну трансформацію у напрямку побудови інформаційного суспільства. Одними з перших держав, які розпочали розробку національної інформаційної політики та політики у сфері інформаційної безпеки стали Сполучені Штати Америки та Японія, а слідом за ними – переважна більшість розвинених країн світу [44].

Інформація, яка вільно розповсюджується в інформаційному просторі країни і її регіонах, може бути суттєвим чинником впливу на соціальну, економічну, політичну і виховну сфери життя регіону. Будь-які «матеріальні» рішення до їх реалізації апробовуються в інформаційній сфері, яка, нажаль, ще не настільки ефективно захищена на законодавчому рівні. Результати такої апробації стають вирішальними [48, с. 253]. В умовах сьогодення

засоби масової комунікації власно є новими «природними ресурсами», що збільшують багатства суспільства. Тобто, боротьба за капітал, ринки збуту відходять на другий план, а головним стає доступ до інформаційних ресурсів, що призводить до того, що війни ведуться вже більше в інформаційному просторі за допомогою інформаційних видів озброєнь. Як вірно зазначає Г. Почепцов: «сучасні інформаційні війни – це квазі-агресивний інструментарій мирного життя, а не лише збройного конфлікту між державами [91, с. 21]».

Питання інформаційної безпеки в політичній сфері охоплюють інформаційно-аналітичну діяльність дипломатичних представництв і зовнішньо-економічних відомств, в економічній галузі – стосуються захисту інформації у банківських системах та мережах зв'язку, у сфері правоохоронної діяльності – захисту таємної інформації і документів службового користування від несанкціонованого доступу і подальшого неправомірного використання [32]. Безперечно, це питання набуває широкої актуальності та гостроти, у випадку коли застосовується до діяльності конкретних органів правопорядку, що апелюють під час здійснення своїх повноважень значною кількістю персональних даних інших осіб, а також інформацією, пов'язаною з результатами власної гласної та негласної оперативно-розшукової діяльності.

Генеральний секретар ООН для створення міжнародного механізму протидії використанню інформаційних озброєнь та розпалюванню інформаційних війн запропонував державам-членам ООН розглянути конкретну типологію інформаційних загроз, визначити критерії проблеми, включаючи розробку міжнародних принципів безпеки глобальних інформаційних

систем, внести відповідні пропозиції [9]. Внаслідок визнання складової глобального процесу інформатизації, постійно акцентується увага на ймовірності застосування інформаційної зброї. Суспільна сфера виступає найбільш вразливою для інформаційних впливів, оскільки включає систему формування громадської думки, структуру засобів масової комунікації, інформаційно-організаційну структуру політичних партій, громадських рухів, національно-культурних та релігійних інституцій, структуру забезпечення основних прав і свобод людини, плюралізму і незалежності виявлення поглядів, вільного обміну ідеями та інформацією [22]. Безперечно, належить сконцентруватися на тому, що зміст і сутність поняття інформаційної безпеки та відповідний адміністративно-правовий механізм забезпечення, як загальнодержавному розумінні так і вузькому відомчому значенні має бути всіляке укріплений, як внутрішньодержавними нормативно-правовими інструментами так і міжнародними стандартами та вимогами, що в свою чергу формуватиме стійкий, як законодавчий так і організаційно-управлінський фундамент для убезпечення від несанкціонованого розповсюдження персональних даних осіб, а також інформації, що використовується в правоохоронній діяльності.

Правоохоронні органи зарубіжних країн широко використовують автоматизовані інформаційно-пошукові системи, які дозволяють значно оптимізувати розкриття та розслідування злочинів, вчинених членами організованих угруповань. З огляду на іноземний досвід національна інформаційна система ідентифікації має будуватися на базі єдиної технології, яка дає змогу обробляти найрізноманітнішу інформацію. Система має охоплювати усі

вузлові точки роботи з населенням, паспортно-візові служби, відділення поліції, поліклініки, каси продажу білетів, системи соціального страхування тощо. Принцип «краще запобігти, ніж карати» має зберігатися і у справі протидії організованих злочинності. Запобігання організованих злочинності здійснюється головним чином оперативно-розшуковими засобами за допомогою громадськості, ЗМІ та інших соціальних інститутів [43]. Відповідно, належить підкреслити, що використання інформаційно-телекомунікаційних систем в діяльності Національної поліції України також широко застосовується, зокрема в частині синхронізації всіх без виключення державних баз та реєстрів, в межах єдиного інформаційно-пошукового простору, а також залучення до його наповнення інформаційно-комунікаційної системи, що пов'язана з роботою інформаційного порталу Національної поліції.

Створена в США система державного регулювання в інформаційній сфері, має на меті ефективне використання сучасних інформаційних технологій для прискорення розвитку економіки, водночас, враховує питання інформаційної безпеки у складі національної безпеки. В США вже на початок XX сторіччя сформувалась система забезпечення інформаційної безпеки, яка спрямована насамперед на убезпечення єдиного інформаційного простору США, проте лише частково відповідає на питання щодо інформаційної безпеки людини. Американська модель покладена в основу багатьох моделей формування інформаційного суспільства. Американська модель, або модель Кремнієвої долини, побудови інформаційного суспільства була заснована на індивідуалізмі, розвиненості ринку ідей, ризикованому підприємництві при

задекларованих мінімальних функціях держави, що обмежуються створенням умов для розвитку ринкових сил [44].

Дослідниками, зокрема О.І. Бугерою, О.Е. Радутним, звертається увага на застосування «великих даних» як ключових інструментів роботи у США (Агентство національної безпеки), Великій Британії (в Сучасній стратегії запобігання злочинності – Modern Crime Prevention Strategy – окремий розділ Using Data and Technology to Prevent Crime), Австралії (впровадження технологій Big Data для кримінологічного прогнозування злочинності комісією зі злочинності – Australian Crime Commission), Японії, де на державному рівні розглядається створення системи запобігання злочинності та протидії екстремістським організаціям із використанням технології великих даних (Big Data Technologies) та штучного інтелекту (artificial intelligence, AI) [20, с. 25–29].

У 1974 році був прийнятий Акт про охорону персональних даних, що визначав категорію «право на приватність» як особисте і фундаментальне право, яке охороняється Конституцією США. Також було встановлено заборону на збір і збереження інформації про те, як індивід здійснює свої права, передбачені першою поправкою до конституції (свободу слова і друку, свободу віросповідання, свободу зборів і подачі петицій), за винятком випадків, коли це прямо передбачено законом або дозволене самим індивідом, або коли це має безпосереднє відношення до правоохоронної діяльності. У 1986 році було прийнято Акт про комп'ютерну безпеку (Computer Security Act), яким визначено значимість безпеки інформаційних систем для всього суспільства. Створено Національний інститут

стандартів і технологій, на який покладались обов'язки щодо моніторингу можливих загроз, та напрацювання шляхів захисту, як у державних інформаційних системах, так і в приватному секторі [44].

Крім ООН, питанням правового забезпечення інформаційної безпеки займаються й інші міжнародні організації. Так, за ініціативою так званої «Групи восьми» у 2000 році ухвалено Окінавську хартію глобального інформаційного суспільства, в якій наголошувалося, що солідарна основа політики і дій в інформаційній сфері спроможна змінити методи взаємодії держав щодо сприяння глобальному соціальному і економічному розвитку. Підкреслено, що формування глобального інформаційного суспільства має супроводжуватися заходами, спрямованими на створення безпечного і вільного від злочинності кіберпростору [32].

4 грудня 2009 року у Києві підписано Угоду між Україною та Європейським поліцейським офісом про стратегічну співпрацю, яка була ратифікована 5 жовтня 2010 року. Метою цієї угоди є посилення співпраці держав-членів Європейського Союзу, що діють через Європол, з Україною у запобіганні міжнародній злочинності, їх виявленні, припиненні та розслідуванні таких злочинів у рамках мандату Європолу, зокрема, шляхом обміну стратегічною та технічною інформацією. Так, стратегічна інформація включає заходи правоохоронного характеру, які можуть бути корисними для запобігання злочинам; нові засоби скоєння злочинів; спостереження та дані, отримані в результаті успішного застосування нових правоохоронних методів та засобів; маршрути, які використовуються контрабандистами або особами, причетними до злочинів, пов'язаних із

торгівлею людьми та змінами цих маршрутів тощо. Однак ця угода не дає повноважень на передачу даних, що належать до встановлення осіб, які вчинили злочин [123]. Відповідно, для забезпечення ефективної співпраці у межах обміну інформацією між всіма учасниками Європейського Союзу та відповідними державними державами, що діють через Європол та забезпечують створення єдиного безпекового європейського середовища, необхідним є унесення змін до законодавства України в частині гармонізації його і за актами права ЄС, щодо дієвої роботи адміністративно-правового механізму забезпечення інформаційної безпеки, перш за все, в діяльності Національної поліції України, як одного з найбільших правоохоронних органів в державі. Разом із цим, належить зауважити, що наскільки неминучим є розширення кола інформаційних банків та баз даних, а також різновидів інформації, що в подальшому може використовуватись для аналізу криміногенних факторів та детермінантів злочинності на загальнодержавному та міжнародному рівні, необхідним є розроблення нових правових форм, методів і засобів регулювання зазначених соціально-правових відносин в контексті втілення життя теоретико-правових норм адміністративно-правового механізму забезпечення інформаційної безпеки в суспільстві загалом, та діяльності Національної поліції України зокрема.

Державами, що входять до Європейського Союзу, у рамках Європолу організовано єдину автоматизовану систему обліку кримінальних відомостей, що діє з 2002 року. До складових комплексної інформаційно-аналітичної системи TECS (The Europol Computer System), крім власне AIC, також належать аналітичний центр та індексна підсистема. Комп'ютерна система TECS дозволяє одночасно обробити та

проаналізувати майже мільйон записів. Вся інформація до системи надається безпосередньо державами-членами ЄС. Кожна країна має власну організацію-представника в Гаазі, так звану ELOS. Тільки ці організації мають доступ до національних баз даних. Формування AIC TECS здійснюється централізовано під контролем керівництва Європолу [59]. Відповідно, слід зазначити, що з огляду на критичну кількість єдиних автоматизованих систем обліку, що містять в собі персональну інформацію, а також службові дані, щодо правоохоронної діяльності та використовується, як Національною поліцією України так і іншими органами правопорядку на території України та в міждержавному контексті, необхідним є виокремлення ще одного рівня чи напряму застосування адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України, а саме – міжнародного.

На саміті ОБСЄ, який відбувся у 2010 році, главами держав і урядів 56 держав-членів підкреслено необхідність досягнення «більшої єдності цілей і дій у протидії новітнім транснаціональним загрозам». У декларації, ухваленій за результатами саміту, підкреслено, що загрози інформаційній безпеці входять до числа новітніх транснаціональних загроз. Варто наголосити, що більшість держав розглядає забезпечення інформаційної безпеки, насамперед, з точки зору реалізації та захисту національних інтересів та цінностей. У вирішенні проблем забезпечення безпеки інформаційної сфери як на загальнодержавному, так і регіональному рівнях вони, з урахуванням реальних та потенційних загроз національній безпеці, а також рівня інформаційно-комунікаційного розвитку країни, використовують комплексний підхід, в якому враховується

специфіка розвитку регіонів. Складність законодавчого регулювання суспільних відносин у цій сфері пов'язана, зокрема, з тим, що об'єктами такого забезпечення одночасно є особистість, суспільство та держава, інтереси яких збігаються лише частково. Якщо правове забезпечення інформаційної безпеки особистості знаходиться під контролем як державних органів, так і міжнародних правозахисних організацій, то регламентація державної безпеки в інформаційній сфері, в основному, залишається справою самої держави. З одного боку, інформаційна безпека розглядається з точки зору організації убезпечення населення від впливу деструктивної інформації, а також захисту інформації, насамперед таємної, комерційної, з обмеженим доступом; з другого – актуалізуються питання захисту інформаційно-комунікаційних систем, які знаходяться під контролем держави [32]. Оскільки це значить, що в тій площині де правоохоронна діяльність виходить за межі однієї держави та здійснюється у спосіб комунікації різних суб'єктів правопорядку на міждержавному рівні чи в міжнародному контексті, питання нормативно-правового забезпечення реалізації адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності, зокрема Національної поліції України, потребує посилення, оскільки не всі акти права Європейського Союзу та національного законодавства на сьогоднішній день є взаємоузгодженими та внутрішньо відповідними. Це, перш за все, зумовлює низку юридичних колізій та спричиняє неможливість застосування українського законодавства на території інших держав-членів Європейського Союзу, що негативно впливає на інституцію захисту прав і свобод людини і громадянина в широкому розумінні та потребує виважених та обдуманих законодавчих

кроків, на підставі попереднього науково-теоретичного аналізу відповідних соціально-правових відносин.

Країни ЄС демонструють спільну позицію щодо інформаційної безпеки та стандартів прав людини в інформаційній сфері, при чому така позиція є динамічною і постійно зазнає переосмислення. При цьому вона значною мірою базується на передумовах побудови інформаційного суспільства в країнах Європи – розвиненій економіці та соціальній спрямованості політики. Європейці, які мають певний обсяг благ, що гарантований певною мірою, системою соціальної захищеності, значно більше цінують можливість самореалізації, вільний час, можливість спілкування, а також захищеність приватного життєвого простору. Тому в інформаційній політиці ЄС спостерігається пошук деякого балансу між контролем з боку держави і ринковими законами. ЄС намагається віднайти формулу динамічного поєднання державних і суспільних інтересів. Тому основні відмінності між американською і європейською моделями розбудови інформаційного суспільства, а також розумінням інформаційної безпеки лежать в площини соціального спрямування внутрішньої політики ЄС [44]. На нашу думку, забезпечення інформаційної безпеки в діяльності Національної поліції України з огляду на євроінтеграційні процеси нашої держави мають бути чітко збалансовані у спосіб доповнення законодавства України тими нормами і положеннями, що слугуватимуть, перш за все, запобіжниками поширення неправдивої інформації або розповсюдження персональних чи особистих даних приватних осіб та органів державної влади, а також тієї інформації, що безпосередньо складає державну таємницю чи призначена для службового користування.

У розробленні та впровадженні корпоративної об'єднаної інформаційної моделі даних для потреб поліції, на нашу думку, на особливу увагу заслуговує досвід Сполученого Королівства Великої Британії. Як слушно зауважив В.О. Заросило, реалізація цих відносин під час попередження правопорушень та їхнього швидкого розкриття у Великій Британії забезпечується запровадженням новітніх комп'ютерних відеоспостережень, створених завдяки фінансуванню міських адміністрацій та приватних підприємств [38]. Так з 2013 року до National Crime Agency (NCA) (Національне кримінальне агентство) передано інформаційну систему The National Policing Improvement Agency (NPIA). Доступ до неї мають усі територіальні поліцейські сили Великобританії, поліція Північної Ірландії (PSNI), Британська транспортна поліція (BTP), поліцейська служба Шотландії, Національна служба ідентифікації (NIS), Національна агенція зі злочинності (NCA), Служба безпеки (MI-5) та Секретна розвідувальна служба (MI-6), Асоціація начальників поліції (ACPO) та інші [59]. Слід зазначити, що введення системи різноманітних видів доступу до інформаційно-комунікаційних систем, що використовуються в діяльності Національної поліції України потребують релевантних нормативно-правових кроків, щодо забезпечення недопущення зловживання службовим становищем поліцейськими різного рівня та спричинення, як результату, поширення конфіденційної інформації із зазначених баз та банків даних. Також важливим є те, що новітні форми, методи та способи реалізації адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України неминуче обумовлені стрімкою цифровізацією поліцейської діяльності, а також розширенням

кола державних послуг, що надаються онлайн у тому числі Національною поліцією України.

Таким чином, в ЄС спостерігається чітке розмежування особливостей інформаційної безпеки людини і суспільства, інформаційної безпеки держави та міжнародної інформаційної безпеки. При цьому основоположними стали власне інтереси людини і суспільства, що й обумовило інтенсивний розвиток таких напрямів як безпека персональних даних, доступ до інформації, а також забезпечення реалізації демократії в умовах побудови інформаційного суспільства. Окремим рядком слід відзначити правове забезпечення протидії кіберзлочинності, яке обумовлене як обраним напрямом на розбудову інформаційного суспільства, так і традиційно визначальною роллю держави в захисті прав та законних інтересів її громадян [44]. Слід зауважити, що в Європейському Союзі безпека персональних даних конкретної особи є чи не найвищою цінністю в суспільстві, оскільки воно повністю пронизане, як цифровою, так і письмовою чи усною інформацією. Інформація, у розумінні європейських демократичних цінностей виступає інструментом впливу на соціально-правові відносини світового співтовариства та конкретної держави, а тому забезпечення її безпеки у нормативно-правовий спосіб та організаційно-управлінськими заходами є чи не найпріоритетнішим завданням.

До автоматизованих інформаційно-пошукових систем, що використовуються у правоохоронній діяльності, також належать JUDEX – це система для реєстрації кримінальних правопорушників та потерпілих, що містить близько 3 млн записів; Fichier National Automatisé des Empreintes Génétiques

(FNAEG) – автоматизований національний банк даних генетичних відбитків ДНК, створений у 1998 році, який спочатку використовувався для реєстрації сексуальних злочинців, але надалі став містити дані про інші злочини, у тому числі й про осіб, які беруть участь у протестних рухах громадянської непокори 3 2807 профілів у 2003 році FNAEG зросла до 330 000 у 2006 році, і 127 0000 у 2009 році. Автоматизована база даних сексуальних злочинців, що перебуває у віданні Міністерства юстиції, була створена в 2004 році. До неї вносяться ім'я, стать, дата та місце народження, національність, псевдонім, адреса, характер правопорушення, дата та місце скоєння правопорушення, характер та дата рішення та санкції або вжиті заходи. Станом на жовтень 2008 року база даних містила записи щодо 43 408 осіб [106]. Можна зауважити на провідні ролі створення інформаційних баз та банків даних, що містять значну кількість персональної та індивідуальної інформації осіб і громадян, які вчиняли кримінальні чи адміністративні правопорушення та підкреслити, що такий досвід діяльності правоохоронних органів України загалом та Національної поліції України зокрема, може бути корисним та суттєво позитивно повпливати на ефективність здійснення поліцейської діяльності, виконання завдань із забезпечення правопорядку у суспільстві та дотримання прав і свобод людини і громадянина, що є базовими демократичними цінностями та утверджує правову державу в умовах сучасних глобалізаційних викликів, зокрема дії правового режиму воєнного стану а також широкомасштабної збройної агресії росії проти України.

В ЄС у межах Шенгенських домовленостей функціонує Шенгенська інформаційна система (SIS), яка є однією з

найбільших інформаційних систем у сфері публічної безпеки у світі та найбільшою в Європі. Шенгенська інформаційна система (SIS) інтегрує інформацію про осіб, які вчинили серйозні кримінальні правопорушення, та осіб, яким заборонено перебування в ЄС. Система містить дані про осіб, які перебувають у розшуку, а також про втрачені документи, викрадені автомобілі, зброю тощо. Призначена SIS для застосування поліцейськими, прикордонниками, митниками держав-членів ЄС [69, с. 145; 140, с. 408]. Як у розглянутих вище країнах, правоохоронні органи Федеративної Республіки Німеччина активно використовують телекомунікаційні засоби та вводять інноваційні комп'ютерні технології для ефективного та якісного інформаційного забезпечення своєї службової діяльності. Так, наприклад, інформаційно-пошукова система Федеральної кримінальної поліції – Informationssystem der Polizei (INPOL) – включає базу даних усіх осіб, оголошених у розшук, відомості про викрадені автомобілі, документи тощо. Дані щодо осіб, розшукуваних німецькою поліцією чи судовими органами, вже за кілька секунд після внесення до бази стають доступні всім користувачів зазначеної системи, а це все відділення поліції та митні органів ФРН. У базі даних Inpol-Personenfahndungsdatei станом на 1 лютого 2014 року було зареєстровано близько 382 597 запитів на арешт та 181 794 на встановлення місцезнаходження осіб; в базі даних Sachfahndungsdatei перебували станом на цю ж дату відомості щодо близько 10 600 000 об'єктів, що перебувають у розшуку, у тому числі 138 568 автомобілів, 739 426 велосипедів, 5 597 512 документів, що посвідчують 3 особи [59]. Відповідно, зазначений приклад, перш за все, додатково підкреслює необхідність розширення спроможностей

Національній поліції України, щодо використання інформаційно-комунікаційних систем у своїй діяльності, що релевантно впливає на необхідність посилення новими методами та формами забезпечення інформаційної безпеки в діяльності зазначеного центрального органу виконавчої влади, відповідного адміністративно-правового механізму.

3.2. Пріоритетні напрями удосконалення адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України

Процес удосконалення забезпечення інформаційної безпеки в Національній поліції України є невинним та системним процесом пов'язаним із тим, на скільки динамічними є соціально-правові відносини в державі та які безпекові чи будь-які інші фактори впливають на них. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Національній поліції України містить значну кількість структурних компонентів, кожен із яких сприяє недопущенню неправомірних дій з інформацією під час службової діяльності Національної поліції України, а оскільки від взаємної злагодженості всіх зазначених елементів залежить загальна ефективність його функціонування та фактичне забезпечення інформаційних прав і свобод людини і громадянина, а також дотримання стандартів інформаційної безпеки на практиці, виокремлення пріоритетних напрямів його удосконалення є одним із найбільш важливих аспектів нашого дослідження.

При цьому, чітке структурування напрямів удосконалення адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України дозволить якомога більш ефективно впливати на його трансформацію, без шкоди поточним соціально-правовим відносинам у даній сфері, а також дозволить якомога більш влучно та конструктивно визначити ті форми, методи, способи та засоби, що можуть позитивно вплинути на його подальше функціонування, а також забезпечення прав і свобод людини і громадянина, в контексті функціонування одного з найбільших центральних органів виконавчої влади правоохоронного спрямування, зокрема.

З кожним роком все більше і більше країн світу долучається до захисту інформаційного простору. Створення спеціальних підрозділів поліції у сфері забезпечення інформаційної безпеки та протидії кіберзлочинності має місце в багатьох країнах світу, зокрема, в Австралії, Великобританії, Данії, Естонії, Канаді, Малайзії, Нідерландах, Німеччині, Норвегії, Польщі, США, Швейцарії, Швеції і інших. Серед основних функцій цих спецпідрозділів є: моніторинг кіберпростору з метою виявлення кіберзлочинів, вірусів або шкідливого програмного забезпечення; здійснення оперативно-розшукових та розвідувальних заходів з метою фіксування протиправних дій кіберзлочинців; розслідування кіберзлочинів, надання методичної та практичної допомоги іншим галузевим службам і правоохоронним органам у межах своєї компетенції; профілактику кіберзлочинів за допомогою громадськості та засобів масової інформації; навчання працівників поліції [70, с. 110]. Саме тому, на нашу думку, одним із найбільш важливих пріоритетів в забезпеченні

подальшої оптимізації функціонування механізму адміністративно-правового забезпечення інформаційної безпеки є залучення чинного міжнародного досвіду, що показав себе ефективним, як в окремих країнах так і в міждержавному контексті. Додатково, питання в даному аспекті інтенсифікує необхідність подальшої європейської інтеграції України до міжнародного європейського співтовариства та неможливість входження до нього, без внесення змін до законодавства України, що регулює відповідну сферу та всі дотичні до нього аспекти соціально-правового життя українського суспільства й функціонування органів державної влади.

Якщо вести мову за кібербезпеку, то варто зауважити, що не зважаючи на те, що Україна вимушена зіштовхуватися з російською агресією у кіберпросторі з початку гібридної війни в 2014 році, об'єктивно визнання кібероборони (складової оборони держави) відбулося в Україні лише в березні 2016 року після Указу Президента України про введення в дію Стратегію кібербезпеки України. В ній визначено, що «основу національної системи кібербезпеки становлять Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи». В даному документі вперше для Міністерства оборони України і Генерального штабу Збройних Сил України були визначені нові задачі, серед яких підготовка держави до відбиття агресії в кіберпросторі і забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахисту власної інформаційної інфраструктури [104; 155]. Слід зауважити, що

безпековий аспект, як один із напрямів забезпечення подальшої оптимізації функціонування адміністративно-правового механізму інформаційної безпеки в діяльності Національної поліції України є чи не найважливішим. Триваюча широкомасштабна збройна агресія проти України, розв'язана росією в 2022 році, чітко продемонструвала необхідність укріплення адміністративно-правових механізмів всіх без виключення державних інституцій, що пов'язані з безпекою і обороною держави. Відповідно, враховуючи, що інформаційна безпека є одним із фундаментальних чинників держави, оскільки більшість інформації знаходиться у відкритих чи закритих базах даних, а відповідно має цифровий вигляд та може бути досяжною для ворога, питання удосконалення, як правового так і технічного забезпечення реалізації адміністративного механізму інформаційної безпеки в діяльності всіх без виключення суб'єктів сектору безпеки і оборони, у тому числі Національної поліції України є надзвичайно важливим.

В умовах інтернаціоналізації всіх сфер суспільного життя розвиток законодавства не може відбуватись без врахування глобалізаційних процесів. При цьому, законотворчі органи окремих держав вимушені враховувати стандарти міжнародного права, а також тенденції до зближення правових систем. Як правило, такі інтеграційні процеси обумовлені геополітичним становищем держави, економічними чинниками, історичними передумовами, а також національною правовою культурою і традиціями державотворення. Гармонізація і уніфікація відбувається за двома напрямками. По-перше, шляхом утворення міжнародних актів, укладання міждержавних договорів, а також нормотворчої діяльності міжнародних організацій, які

визначають пріоритети, орієнтири, а часом і рамки для розвитку національного законодавства у визначених сферах. Другий напрям стосується національного нормотворення, коли держави самостійно сприймають і закріплюють в національному законодавстві досвід правового регулювання інших держав чи міжнародно-правові тенденції. Інформаційна безпека, як сфера правового регулювання, апіорі не може розвиватись без врахування міжнародного правового поля та досвіду зарубіжних країн. Це обумовлено самою істотою інформаційної сфери, яку складно обмежити національними кордонами в демократичній державі [44]. Пропонована автором позиція, перш за все, підкреслює багаторівневість інституту удосконалення адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України, оскільки окремі нормативно-правові акти можуть бути врегульовані та змінені лише за умови ініціативи відповідного уповноваженого на це органу державної влади чи міждержавної інституції, в залежності від юридичної сили та рівня останнього. Саме тому, архітектура адміністративно-правового механізму забезпечення інформаційної безпеки в державі та Національній поліції зокрема, будучи комплексним та врівноваженим механізмом, що спрямований на впорядкування соціально-правових відносин, як загальнодержавного, так і міжнародного масштабу потребує комплексного підходу до реформування та врахування всіх об'єктивних факторів і обставин, що впливають на нього.

Вчені виділяють ще один напрямок (превентивно-захисний), котрий полягає в обмеженні доступу до інформації про належність особи до сил охорони правопорядку, а якщо приховати таку належність неможливо або недоцільно –

обмеженні доступу до інформації про анкетні дані працівників сил охорони правопорядку та їх близьких осіб, а саме відомостей про їх місце проживання, перебування, місце роботи тощо. Цей напрямок є превентивно-захисним. Його змішана природа полягає в тому, що, з одного боку, унеможлиблюючи доступ до інформації про працівника сил охорони правопорядку, він забезпечує попередження посягання (є превентивним), з іншого боку, попередження посягання відбувається на етапі певних підготовчих дій стосовно збору інформації про особу коли вже розпочалися певні дії щодо підготовки до посягання, тобто превенція в її чистому вигляді виявилась неефективною (в цій частині він є захисним). Збереження в таємниці інформації про належність особи до сил охорони правопорядку є найвищим ступенем превентивно-захисного напрямку і має застосовуватися до таких категорій осіб: 1) особи, які залучаються до конфіденційного співробітництва на платних або безоплатних засадах; 2) особи, які є штатними працівниками сил охорони правопорядку, але виконання ними своїх функціональних обов'язків можливо виключно за умови збереження в таємниці їх професійної належності до органів охорони правопорядку [18]. На нашу думку, виділення превентивно-захисного напрямку реалізації адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України, перш за все, пов'язується з двома аспектами, одним із яких є необхідність формування такого кола законодавчого регулювання, що унеможливило б будь-які протиправні дії з інформацією, а з іншого боку прямо передбачає наявність технічних засобів захисту у відповідному сегменті соціально-правових відносин та

враховує всі безпекові фактори і обставини, що виникли на даному етапі розвитку державних процесів в Україні.

Як зазначає О.А. Заярний, одним із напрямів удосконалення способів захисту інформаційних прав людини в умовах застосування штучного інтелекту (один із аспектів кібернетичної безпеки людини) є впровадження у практичну діяльність етичного напрямку, в основу якого включаються акти м'якого права – етичні норми та принципи, які містять адресовані розробникам або постачальникам вимоги щодо забезпечення дотримання інформаційних прав фізичної особи, заклики до недискримінації за ознаками застосування технологій штучного інтелекту чи відмови від їх застосування [41].

Більш детально необхідно зупинитися на загальній стратегії інформаційної безпеки, система якої формально проголошена в Національній програмі інформатизації. Згідно зі ст. 5 Закону України «Про Національну програму інформатизації», головною метою процесів інформатизації є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави [102]. Зазначений вище Закон є досить важливим елементом системи інформаційної безпеки навіть незважаючи на те, що приписної конструкції про роль та участь органів місцевого самоврядування у ньому немає. Справа в тому, що ст. 17–19 Закону створюють правові підстави та закріплюють за суб'єктами інформаційних відносин у державі (центральною владою, органами виконавчої влади, органами місцевого самоврядування, підприємствами, установами, організаціями) обов'язок розробки та прийняття програм інформатизації, що

за великим рахунком, є сукупністю стратегій та правових інструментів для формування політики інформаційної діяльності відповідно до власних потреб кожного суб'єкта. Питання інформаційної безпеки не є виключенням [126]. Так, Національна поліція України, маючи програму інформатизації вживає заходів, щодо автоматизації основних організаційно-управлінських та сервісних процесів, що відображається в запуску на серверах Міністерства внутрішніх справ України низки інформаційно-аналітичних ресурсів, наприклад, як «Освітній портал Національної поліції України», що сприяє та забезпечує реалізацію системи професійного навчання поліцейських або «Інформаційний портал Міністерства внутрішніх справ України», що містить інформацію надану Національною поліцією України, щодо наявності чи відсутності судимостей в осіб і громадян України.

Важливість використання інструментів післядипломної освіти, наголошується також М.Ю. Романовим, котрий підкреслює, що стажування, перепідготовка та спеціалізація є надважливими опціями, що безпосередньо впливають на професіоналізм поліцейських кадрів [112; 114; 117], а відповідно, цифровізація цих форм здобуття знань, кратно пришвидшує відповідний процес і потребує суттєвої уваги в частині забезпечення інформаційної безпеки.

Інформаційна безпека в системі міжнародної безпеки пройшла різні етапи становлення. В другій половині ХХ сторіччя міжнародні домовленості здебільшого стосувались забезпечення існування та розвиток інформаційного середовища бізнесу. На межі тисячоліть відбулися значні трансформаційні процеси в геополітиці і внаслідок подвійної трансгранично-національної природи кіберпростору

національна політика держав щодо інформаційної безпеки стає значимою у вимірі зовнішньої політики, оскільки пов'язана з розбудовою інфраструктури. Дубов Д.В. наводить як приклад, що цілком внутрішні питання освітньої сфери (наприклад, щодо підготовки фахівців ІТ-сфери) робить це питання частиною зовнішньої політики держави [35, с. 29]. Тим більше значимим в міжнародному аспекті є правове забезпечення інформаційного простору держави, інформаційних прав і свобод людини, режимів доступу до інформації, зокрема в глобальній мережі, гарантування принципу міжнародного нейтралітету, електронної демократії та інші [44; 100; 151].

Слід зауважити, що в контексті функціонування адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України, підготовка фахівців із сфери кіберзахисту прямопропорційно пов'язується із функціонуванням окремих підрозділів Національної поліції України, таких як Департамент кіберполіції та Департамент інформаційно-аналітичної підтримки, працівники яких мають відповідну кваліфікацію та рівень знань у зазначеній сфері й можуть забезпечити не лише належний технічний захист інформації, а й доповнити розробленими нормами відповідний адміністративно-правовий механізм.

На сучасному етапі розбудови системи інформаційної безпеки виняткове значення має зміцнення нормативно-правової бази функціонування інформаційного середовища в цілому та проблеми забезпечення інформаційної безпеки. Динамізм відносин в інформаційній сфері постійно випереджає розвиток суспільної правосвідомості, встановлені регулятори суспільних відносин, ускладнює створення

стабільної правової регламентації. Відставання, недосконалість нормативно-правової бази дозволяє окремим суб'єктам реалізовувати свої протиправні наміри і можливості в інформаційній сфері щодо широкого спектра інтересів інших як суб'єктів, так і об'єктів національної безпеки. Безперечним є необхідність удосконалення нормативно-правової бази забезпечення інформаційної безпеки України, яке б відповідало не лише міжнародним стандартам, а передусім українським національним інтересам в інформаційній сфері. При чому важливою є не стільки статика окремих нормативно-правових актів, скільки динаміка доповнень, яка б містила механізми генерації нових рішень, проектів, що дозволяють діяти в темпі, які диктує інформаційне суспільство [8; 62].

Оцінка сучасного стану адміністративно-правового забезпечення інформаційної безпеки в Україні, в аспекті напрацювання науково обґрунтованих пропозицій з цього питання, актуалізувала необхідність сфокусувати увагу на таких першочергових заходах щодо трансформації інформаційного законодавства України: переглянути понятійно-категоріальну базу, доповнивши Закон України «Про інформацію» поняттям «інформаційна безпека», узгодивши невідповідності щодо переліку суб'єктів інформаційних відносин у Законах України «Про інформацію», «Про доступ до публічної інформації»; прийняти низку змін до Законів України: «Про громадські об'єднання», «Про благодійну діяльність та благодійні організації», «Про очищення влади», «Про інформацію» шляхом законодавчого закріплення поняття «агент впливу», передбачивши чіткі механізми їх ідентифікації та протидії деструктивній діяльності агентів впливу в інформаційній

сфері [155]. На нашу думку, слід цілком і повністю погодитися з такою позицією та доповнити, що зміни до вказаного нормативно-правового поля, що регулює сферу інформаційної безпеки загальнодержавному контексті прямопропорційно вплинуть на рівень та міру ефективного функціонування адміністративно-правового механізму забезпечення інформаційної безпеки безпосередньо в діяльності Національної поліції України та інших правоохоронних органів і суб'єктів сектору безпеки і оборони.

Слід законодавчо встановити затверджені положення: про обов'язковий склад і основну технічну комплектацію виробничих і корпоративних мереж, які впливають на стан інформаційної безпеки; про обов'язкові вимоги по інформаційній безпеці систем, програмного і апаратного забезпечення; про безпечне ведення бізнесу із використанням нових інформаційних технологій і глобальних інформаційних мереж. Потребують подальшого вирішення питання щодо розробки комплексу інформаційних стандартів із урахуванням забезпечення інформаційної безпеки, розвитку системи сертифікації інформаційних продуктів, систем і послуг, створення системи ліцензування діяльності організацій по окремих напрямках формування єдиного інформаційного простору України [8]. На нашу думку, ці інформаційно-технічні кроки, перш за все, потребуватимуть додаткової оцінки в результаті їх імплементації, з метою належної інтеграції до структури адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності всіх без виключення органів державної влади, у тому числі Національної поліції України.

Висновки до розділу 3

Загалом, характеризуючи зарубіжний досвід забезпечення інформаційної безпеки в діяльності поліцейських підрозділів та органів правопорядку загалом необхідно підкреслити, що зазначені теоретико-правові інституції характерні, перш за все, високим рівнем нормативно-правового захисту індивідуальних прав людини і громадянина, щодо інформаційної безпеки кожного члена суспільства. Вказане досягається, перш за все, встановленням жорстких методів, форм та способів адміністративно-правового регулювання відповідної інформаційної сфери, а також потужним інструментарієм, щодо встановлення меж юридичної (адміністративної чи кримінальної в залежності від ступеня вини конкретної особи) відповідальності за протиправні дії чи бездіяльність пов'язані з сферою інформаційної безпеки.

Не лише нормативно-правове забезпечення реалізації адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України є ефективним інструментом забезпечення вказаного правового режиму. Чільне місце слід виділити також інформаційно-технічним інструментам захисту інформації котрі мають гарантувати безпеку та схоронність відповідних даних, що використовуються в службовій діяльності Національної поліції України чи зберігаються нею у відповідних базах та банках даних.

Правові інформаційно-безпекові режими не пов'язуються із механізмами забезпечення прав і свобод людини і громадянина, в тій частині де діють превентивно,

створюючи такий правовий стан речей за умов дії якого унеможлиблюється незаконне поводження з будь-якою інформацією, що в свою чергу забезпечує права і свободи людини і громадянина в даному сегменті.

Без чіткого окреслення діянь за вчинення яких, особа підлягає адміністративній чи будь-якій іншій юридичній відповідальності, неможливо буде законно та виважено застосувати відповідний інститут права, що в свою чергу зумовлює необхідність чіткого та структурованого визначення всіх складників цього правового явища.

ВИСНОВКИ

У дисертації здійснено теоретичне узагальнення та запропоновано вирішення нового наукового завдання, суть якого полягає у формуванні теоретичних положень і практичних рекомендацій щодо питання функціонування адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України. Найбільш суттєвими висновками є такі положення.

1. Оскільки інформація є основним інструментом комунікації суспільства, що в свою чергу дозволяє ефективно розвивати його та забезпечувати такий соціально-правовий стан, за якого окреслені блага (права і свободи людини і громадянина) не перебувають під загрозою, питання забезпечення безпеки поводження з інформацією безперечно є тим аспектом адміністративно-правового його регулювання, що безпосередньо впливає на безпечність знаходження членів соціуму всередині нього, уможливорює сталий соціальний розвиток і убезпечує як увесь соціуму так і окремих його представників від протиправних посягань на визначені, як обов'язкові для них блага.

Правовий режим інформації, що діє в Національній поліції України має режимні обмеження, щодо роботи з нею, що в свою чергу, потребує особливого підходу до забезпечення дії відповідного адміністративно-правового механізму, що спрямовується не лише на внутрішній захист інформації, що використовується в роботі поліції, а й потребує запобігання її витоку назовні, що може порушити права і свободи людини і громадянина.

Розглядаючи інформаційну безпеку, необхідно

зауважити, що її об'єктивний прояв, перш за все, дозволяє сформувати такі соціально-правові умови й втілити відповідне правове становище, що впорядковує обіг тієї чи іншої інформації, а також забезпечує неможливість її неправомірного використання. Суб'єктивна ж сторона адміністративно-правового захисту режиму інформаційної безпеки дозволяє забезпечити вірне правове розуміння учасників обігу інформації, зокрема в діяльності Національної поліції України, щодо основних стандартів і вимог її захисту та охорони.

2. Поняття адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України включає в себе не лише теоретико-правові конструкції втілення в життя самого змісту інформаційної безпеки, а й передбачає, в тому числі, окремі аспекти покладання обов'язків щодо його реалізації на конкретні суб'єкти. При цьому, сукупність дій і прийняття конкретних рішень втілюється в змісті компетенції кожного окремого органу державної влади чи його структурного підрозділу, правореалізація яких можлива лише крізь призму чіткого та унормованого в законодавстві України алгоритму функціонування цих учасників.

3. Елементи адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції в Україні потребують нормативне закріплення та чіткої структури, котра складається з визначення змісту та сутності правовідносин про які йдеться, загальний опис процесів, а також форми реалізації зазначеного механізму та окреслення чіткого кола його суб'єктів. Крім цього, належить звернути увагу на те, що оскільки зазначений механізм призначений для врегулювання, як внутрішньо так і зовнішньо

організаційної діяльності Національної поліції України в аспекті інформаційної безпеки, необхідним є уточнення змісту та сутності неправомірної поведінки всіх можливих суб'єктів, крізь призму дії поліцейського законодавства.

Від чіткості визначення змісту і сутності будь-якого адміністративно-правового механізму, а також окреслення векторів його практичної реалізації залежить ефективність його функціонування в загальнодержавному контексті, а також міра та можливість подальшої оптимізації діяльності, в даному випадку, конкретного органу державної влади в реаліях якого існує відповідна адміністративно-правова опція. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Національній поліції України окреслює відповідні правовідносини не лише всередині її діяльності, а й виходить в зовнішню площину.

Адміністративно-правовий механізм забезпечення інформаційної безпеки в діяльності Національної поліції України складається з низки актів законодавства України до кола яких, перш за все, належать ті норми, що прямо чи опосередковано регулюють дію правового режиму інформації та зміст інформаційної безпеки, що власне і є об'єктом та предметом забезпечення в контексті дії зазначеного адміністративно-правового механізму, у тому числі в контексті функціонування Національної поліції України. Таким чином, логічним видається висновок про те, що коло нормативно-правового забезпечення інформаційної безпеки в діяльності Національної поліції України, перш за все, спирається на базове законодавство у даній сфері та не може йому суперечити, що в свою чергу накладає низку додаткових зобов'язань на вказані центральний орган виконавчої влади та висуває окремі вимоги до підзаконних

нормативно-правових актів, що регулюють його діяльність.

4. Характеристика нормативно-правового регулювання інформаційної безпеки у Національній поліції України базується на галузях законодавства України, що в першу чергу складає, як кримінальне та адміністративне так і цивільне й інформаційне законодавство, котрі можуть бути застосовані в механізмі адміністративно-правового регулювання інформаційної безпеки в Національній поліції України. Зазначена теза обґрунтовується, перш за все тим, що ті чи інші види інформації та неправомірні чи незаконні дії, що були вчинені з нею, спричиняють різні правові наслідки та, відповідно, підлягають варіативній юридичній кваліфікації, що тягне за собою необхідність притягнення до юридичної відповідальності тих чи інших суб'єктів.

5. Чітке окреслення суб'єктів, відповідальних за зазначений напрям роботи, їх класифікація та уточнення в розрізі роботи державницького механізму загалом є важливою складовою дії адміністративно-правового механізму інформаційної безпеки в Національній поліції України.

До кола суб'єктів реалізації адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України належать: Верховна Рада України, як єдиний законодавчий орган державної влади, Кабінет Міністрів України, як вищий орган виконавчої влади в Україні, а також Президент України та вертикаль судової влади, що безпосередньо впливають на формування та реалізацію державної політики у сфері забезпечення безпеки інформації); центральні органи виконавчої влади, що мають повноваження у сфері забезпечення інформаційної безпеки загалом і в Національній поліції України, зокрема

Міністерство культури та стратегічних комунікацій України, Державна служба спеціального зв'язку та захисту інформації України, а також Національна поліція України); суб'єкти забезпечення інформаційної безпеки в Національній поліції України (до кола яких відносяться підрозділи кіберполіції, підрозділи організаційно-аналітичної роботи та контролю, підрозділи документального забезпечення, режимно-секретні підрозділи).

Так, поділ суб'єктів адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України, перш за все, можна здійснити шляхом розподілу їх на зовнішні та внутрішні, що в свою чергу, мають додаткову організаційно-управлінську вертикаль й можуть поділятися за колом компетенції, змістом повноважень, а також масштабом діяльності.

6. Притягнення до відповідальності за вчинення адміністративних правопорушень у сфері правового режиму інформаційної безпеки самими поліцейськими, базується на тому, що предметом таких правопорушень є інформація, власником якої поліцейський не являється, оскільки її правовий режим має безпосередню приналежність до адміністративно-правового статусу поліції чи інших правоохоронних органів, тобто є власністю держави, а поліцейський, в свою чергу, порушує виконання своїх службових обов'язків, щодо забезпечення її збереження та нерозповсюдження.

Кодекс України про адміністративні правопорушення був прийнятий у 1984 році, а тому з урахуванням того, що українське суспільство з тих часів суттєво трансформувалася, а загальнодержавний курс розвитку соціально-правових відносин спрямовується наразі на вступ України до

Європейського Союзу, все адміністративне законодавство пов'язане із притягненням осіб за вчинення відповідних адміністративних правопорушень до юридичної відповідальності потребує оновлення, а саме, оновлення санкцій статей 212-3 «Порушення права на інформацію та права на звернення», 212-5 «Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію», 212-6 «Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем» тощо, Кодексу України про адміністративні правопорушення.

7. Цифровізація та інформатизація загальних процесів, що відбуваються в державі та всьому світі потребує релевантної відповіді від органів державної влади, в частині унормування основних способів, що слугують для втілення в життя адміністративно-правового механізму забезпечення інформаційної безпеки в широкому розумінні та дотримання відповідного режиму в діяльності не лише на території країни, де вони функціонують, а й у міждержавному аспекті.

Досвід Сполучених Штатів Америки може бути одним із найбільш ефективних та застосованих до сучасних правових реалій України, оскільки зазначена держава вже має досвід забезпечення інформаційної безпеки поліцейських підрозділів, що суттєво ускладнює правореалізацію зазначеного механізму та забезпечення прав і свобод людини і громадянина в контексті критичних безпекових загроз. Позитивні практики застосування інформаційно-безпекових гарантій, у тому числі на найвищому конституційному рівні, мають бути запроваджені в діяльності правоохоронних

органів України.

8. Виділення превентивно-захисного напрямку реалізації адміністративно-правового механізму забезпечення інформаційної безпеки в діяльності Національної поліції України, перш за все, пов'язується з двома аспектами, одним із яких є необхідність формування такого кола законодавчого регулювання, що унеможливило б будь-які протиправні дії з інформацією, а з іншого боку прямо передбачає наявність технічних засобів захисту у відповідному сегменті соціально-правових відносин та враховує всі безпекові фактори і обставини, що виникли на даному етапі розвитку державних процесів в Україні.

Гострота та актуальність цієї проблематики зокрема, актуалізується з урахуванням значної кількості баз даних та банків інформації, що знаходяться в розпорядженні Національної поліції України та наповнюється нею в процесі здійснення своїх правоохоронних функцій. Крім цього, окремий міждержавний аспект її діяльності слід враховувати не менш уважно, оскільки в бази та банки даних Національної поліції України, на певному етапі, може потрапити також інформація про осіб і громадян правопорушників інших держав світу, що покладає на зазначені центральний орган виконавчої влади додаткові зобов'язання, щодо захисту і цієї інформації також.

Інформаційно-роз'яснювальна робота, щодо правил поведінки із різними типами та видами інформації в діяльності Національної поліції України, а також системне підвищення навичок і здібностей поведінки з інформаційно-технічними ресурсами є пріоритетними завданнями керівництва Національної поліції України та суб'єктів уповноважених на це підрозділів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адміністративна діяльність органів поліції України : підручник / [В. В. Сокурєнко, О. І. Безпалова, О. В. Джафарова та ін.] ; за заг. ред. В. В. Сокурєнка. Харків : ХНУВС, 2017. 432 с.
2. Адміністративне право України (загальна частина) : навч. посіб. / [О. І. Остапенко, С. С. Єсімов, Л. С. Гулак та ін.] ; Львів : СПОЛОМ, 2021. 616 с.
3. Адміністративне право України. Академічний курс : підручник : у 2 т. / [редкол.: В. Б. Авер'янов (голова) та ін.]. Київ : Юрид. думка, 2004. Т. 1 : Загальна частина. 584 с.
4. Адміністративне право України. Академічний курс : підручник : у 2 т. / [редкол.: В. Б. Авер'янов (голова) та ін.]. Київ : Юрид. думка, 2005. Т. 2 : Особлива частина. 624 с.
5. Адміністративне право України. Академічний курс : підручник : у 2 т. / [редкол.: В. Б. Авер'янов (голова) та ін.]. Київ : Юрид. думка, 2007. Т. 1 : Загальна частина. 592 с.
6. Адміністративне право : підручник / [Ю. П. Битяк, В. М. Гарашук, В. В. Богущкий та ін.] ; за з. ред. Ю. П. Битяка, В. М. Гарашука, В. В. Зуй. Харків : Право, 2010. 624 с.
7. Адміністративно-правове регулювання обігу інформації з обмеженим доступом в інформаційно-телекомунікаційних системах Національної поліції : монографія. Львів : ЛьвДУВС, 2021. 212 с.
8. Антонюк В. В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці. Державне управління: удосконалення та розвиток. 2014. № 8. URL: <http://www.dy.nayka.com.ua/?op=1&z=747>.

9. Арістова І. В. Розбудова правової держави в Україні: правовий механізм забезпечення права на доступ до інформації в суспільстві знань. Правова інформатика. 2010. № 1 (25). С. 3–13.

10. Архіпов О. Є., Архіпова Є. О. Особливості розуміння зрозуміти «інформаційна безпека» та «безпека інформації». Інформаційні технології та безпека: основи забезпечення інформаційної безпеки (ІТБ-2014) : матеріали XIV Міжнар. наук.-практ. конф. (Київ, 28 трав. 2014 р.). Київ : ІПРІ НАН України, 2014. С. 18–30.

11. Баранов О. А. Напрями перспективних досліджень у галузі інформаційного права. Інформація і право. 2016. № 2 (17). С. 15–31.

12. Баранов О. П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України. Вісник Національної академії державного управління при Президентові України. 2014. № 3. С. 60–65.

13. Безпалова О. І. Адміністративно-правовий механізм реалізації правоохоронної функції держави : монографія. Харків : НікаНова, 2014. 544 с.

14. Безпека життєдіяльності та охорона праці : підручник / [В. В. Сокурєнко, О. М. Бандурка, С. М. Бортник та ін.] ; за заг. ред. В. В. Сокурєнка. Харків : ХНУВС, 2021. 308 с.

15. Березовська І. Р. Поняття і характеристика структурних елементів механізму застосування адміністративно-правових засобів забезпечення інформаційної безпеки України. Науковий вісник Національної академії внутрішніх справ. 2013. № 2. С. 31–35. URL:

<https://elar.naiu.kiev.ua/server/api/core/bitstreams/b28463ac-4347-4c43-be5c-4bcc3a348b21/content>.

16. Бедний О. І. Внутрішньо-організаційні відносини в органах публічної влади та їх апаратах як складова предмета адміністративного права. Науковий вісник Ужгородського національного університету. 2016. Вип. 40. Т. 1. С. 131–134. (Серія «Право»).

URL: <https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/33940/1/%D0%92%D0%9D%D0%A3%D0%A2%D0%A0%D0%86%D0%A8%D0%9D%D0%AC%D0%9E-%D0%9E%D0%A0%D0%93%D0%90%D0%9D%D0%86%D0%97%D0%90%D0%A6%D0%86%D0%99%D0%9D%D0%86%20%D0%92%D0%86%D0%94%D0%9D%D0%9E%D0%A1%D0%98%D0%9D%D0%98%20%D0%92%20%D0%9E%D0%A0%D0%93%D0%90%D0%9D%D0%90%D0%A5%20%D0%9F%D0%A3%D0%91%D0%9B%D0%86%D0%A7%D0%9D%D0%9E%D0%87%20%D0%92%D0%9B%D0%90%D0%94%D0%98.pdf>.

17. Бєлєвцева В. В. Правовий режим інформаційних ресурсів. Інформація і право. 2011. № 3 (3). С. 41–46. URL: <http://il.ippi.org.ua/article/view/271636>.

18. Богуславський В. В. Адміністративно-правове регулювання інформаційного забезпечення особистої безпеки працівників сил охорони правопорядку : монографія ; за наук. ред. О. Г. Комісарова. Дніпро : Біла К. О., 2019. 128 с.

19. Бугайчук К. Документальне забезпечення публічного адміністрування в органах Національної поліції. Підприємництво, господарство і право. 2019. № 9. С. 109–115. (Серія «Адміністративне право і процес»). URL: <http://pgp-journal.kiev.ua/archive/2019/9/19.pdf>.

20. Бугера О. І. Використання Інтернет-технологій для запобігання злочинності. *Visegrad Journal on Human Rights*. 2018. № 4 (2). С. 25–29.

21. Візір Т. С. Адміністративно-правове регулювання забезпечення інформаційної безпеки в Україні: сучасний стан та перспективи вдосконалення. *Science Online*. 2019. № 4. URL: <https://nauka-online.com/publications/jurisprudence/2019/4/administrativno-pravove-regulyuvannya-zabezpechennya-informatsijnoyi-bezpeki-v-ukrayini-suchasnij-stan-ta-perspektivi-vdoskonalennya/>.

22. Міжнародна кіберсправа: як правоохоронці України, Європи та США спільно викрили хакерську банду в центральній Україні. Телевізійна служба новин, 28.11.2023. URL: <https://tsn.ua/ukrayina/mizhnarodna-kibersprava-yak-pravoohoronci-ukrayini-yevropi-ta-ssha-spilno-vikrili-hakersku-bandu-v-centralniy-ukrayini-2459725.html>

23. Голосніченко І. П. Адміністративне право України (основні категорії і поняття) : посібник. Ірпінь, 1998. 108 с.

24. Горелік Д. С. Особливості забезпечення режиму секретності на стратегічних об'єктах в Україні. Підготовка поліцейських в умовах реформування системи МВС України : зб. наук. пр. (Харків, 24 трав. 2018 р.). Харків : ХНУВС, 2018. С. 235–238. URL: https://univd.edu.ua/general/publishing/konf/24_05_2018/pdf/65.pdf.

25. Гумін О. М., Пряхін Є. В. Адміністративно-правове забезпечення: поняття та структура. *Наше право*. 2014. № 4. С. 46–50.

26. Гурковський В. І. Інформаційна безпека в Україні як складова національної безпеки. *Збірник наукових праць*

Української академії державного управління при Президентіві України. 2002. Вип. 2. С. 9–18.

27. Детюк А. М. Поняття та структура механізму адміністративно-правового регулювання державного замовлення у сфері освіти. Порівняльно-аналітичне право. 2016. № 5. С. 189–192.

28. Дегтяр А. О. Державно-управлінські рішення: інформаційно-аналітичне та організаційне забезпечення : монографія. Харків : Магістр, 2004. 224 с.

29. Діденко С. В. Поняття та елементи механізму адміністративно-правового забезпечення обігу та застосування зброї в Україні. Наукові праці Національного університету «Одеська юридична академія». 2015. Т. 16. С. 463–469. URL: http://nbuv.gov.ua/UJRN/Npouyua_2015_16_52.

30. Дмитрієв А. А. Принципи та правове регулювання діяльності органів Національної поліції України з протидії організованих злочинності. Вісник Кримінологічної асоціації України. 2016. № 1 (12). С. 164–166.

31. Довгань О. Д., Ткачук Т. Ю. Система інформаційної безпеки України: онтологічні виміри. Інформація і право. 2018. № 1 (24). С. 89–103.

32. Долженко К. І. Адміністративно-правове забезпечення інформаційної безпеки регіону : дис. ... канд. юрид. наук : 12.00.07. Харків, 2016. 221 с.

33. Долженко К. І. Правові аспекти захисту державної інформації у фінансовій сфері. Актуальні питання безпеки фінансової системи держави : зб. наук. пр. Міжнар. наук.-практ. інтернет-конф. (Харків, 21 лют. 2014 р.). Харків : НікаНова, 2014. С. 115–118.

34. Домбровська С. Механізми забезпечення інформаційної безпеки як складової безпеки України. Теорія

та практика державного управління. 2015. № 1 (48). URL: <http://repositsc.nuczu.edu.ua/bitstream/123456789/3052/1/Dombrovska-NADU481.pdf>.

35. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 328 с.

36. Єсімов С. С., Бортник Н. П. Правова регламентація заходів адміністративно-процесуального примусу. Соціально-правові студії. 2021. Вип. 3 (13). С. 28–34.

37. Єфімов В. В., Нізельник О. І. Щодо організаційних заходів забезпечення режиму секретності при проведенні ОТЗ й НСРД Національною поліцією України. Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики : матеріали Всеукр. наук.-практ. конф. (Дніпро, 18 листоп. 2016 р.) : у 2 ч. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2016. Ч. 2. С. 15–18.

38. Заєць О. М. Інститут аналітичного супроводження досудового розслідування кримінального провадження в Україні: сучасний стан і перспективи розвитку. Вісник кримінального судочинства. 2016. № 4. С. 17–25.

39. Захарова В. І., Філіпова В. Я. Основи інформаційно-аналітичної діяльності : навч. посіб. Київ : Центр учб. літ., 2013. 336 с.

40. Захист інформаційної безпеки як функція держави.

41. Мего-Інфо : [сайт]. URL: <http://mego.info/%D0%BC%D0%B0%D1%82%D0%B5%D1%80%D1%96%D0%B0%D0%BB/>.

42. Заярний О. А. Деякі напрями удосконалення способів захисту інформаційних прав фізичних осіб в умовах застосування технологій штучного інтелекту. Актуальні проблеми захисту інформаційних прав особи в умовах

технологічних викликів та цифрової реальності : матеріали Міжнар. наук.-практ. конф. (Херсон, 17–18 верес. 2019 р.). Херсон : Гельветика, 2019. С. 94–98.

43. Заярний О. А. Правове забезпечення розвитку інформаційної сфери України: адміністративно-деліктний аспект : монографія. Київ : Київ. нац. ун-т ім. Т. Шевченка, 2017. 700 с.

44. Злочинна організація та її співвідношення з бандою, організованою групою. KazEdu : [сайт]. URL: <https://www.kazedu.kz/referat/194206>.

45. Золотар О. Інформаційна безпека людини: теорія і практика : монографія. Київ : АртЕк, 2018. 446 с.

46. Іванов І. Є. Актуальні питання інформаційної безпеки у діяльності Національної поліції України. Юридична наука. 2020. № 3 (105). С. 183–190. DOI: 10.32844/2222-5374-2020-105-3.23.

47. Ігонін Р. В., Галунько В. В. Поняття адміністративно-правового забезпечення функціонування системи судів загальної юрисдикції. Адвокат. 2011. № 1 (24). С. 36–40.

48. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Humanitarian vision. 2016. Vol. 2. № 1. С. 27–32. URL: http://nbuv.gov.ua/UJRN/hv_2016_2_1_7.

49. Інформаційна політика та безпека. Основні напрямки діяльності. Міністерство культури та стратегічних комунікацій України : [сайт]. URL: <https://mcip.gov.ua/informatsiyna-polityka-ta-bezpeka/osnovni-napriamky-diialnosti/>.

50. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека : навч. посіб. Харків : ХНЕУ, 2008. 352 с.

51. Каленіченко Л. І. Особливості юридичної відповідальності працівників Національної поліції. Науковий вісник Ужгородського національного університету. 2019. Вип. 55. Т. 1. С. 27–31. (Серія «Право»).

52. Кобзар О. Ф. Правоохоронна діяльність: теоретико-правовий аналіз. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2017. № 3. С. 7–14.

53. Кобзар О., Романов М. Організаційно-правові засади функціонування підрозділів дізнання Національної поліції України. Вісник Університету імені Альфреда Нобеля. 2021. № 1 (2). С. 96–101. (Серія «Право»). URL: <https://law.duan.edu.ua/images/PDF/2021/1/14.pdf>.

54. Кобрусєва Є. А. Структура адміністративно-правового механізму забезпечення права на мирні зібрання в Україні. Право та державне управління. 2020. № 1. Т. 1. С. 262–269. DOI: <https://doi.org/10.32840/pdu.2020.1-1.40>.

55. Ковалів М. В., Сидор М. Я. Обіг інформації в деліктних адміністративних правовідносинах у контексті інформаційної безпеки. Юридичний науковий електронний журнал. 2022. № 8. С. 290–292. URL: http://lsej.org.ua/8_2022/63.pdf.

56. Кодекс України про адміністративні правопорушення : Закон Української РСР від 7 груд. 1984 р. № 8073-X. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text>.

57. Кодекс України про адміністративні правопорушення. Відповідає офіц. тексту. Суми : ВВП НОТІС, 2020. 336 с.

58. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>.

59. Копейчиков В. В. Загальна теорія держави і права : навч. посіб. Київ : Юрінком, 1997. 320 с.

60. Кордонський М. С. Аналіз зарубіжного досвіду використання системи поліцейської інформації та розвідки : магістерська робота. Одеса, 2022 рік. С. 97-99.

61. Корнієнко Д., Павлютін Ю. Сутність механізму адміністративно-правового забезпечення службово-бойової діяльності сил безпеки (на прикладі Національної гвардії України). Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2020. № 4. С. 35–41. URL: http://nbuv.gov.ua/UJRN/Nvdduvs_2020_4_7.

62. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. Відомості Верховної Ради України. 2001. № 25. Ст. 131.

63. Крупнова А. О. Адміністративно-правові форми забезпечення інформаційної безпеки в Україні. Юридичний науковий електронний журнал. 2024. № 6. С. 217–222. DOI: <https://doi.org/10.32782/2524-0374/2024-6/53>.

64. Крупнова А. О. Система суб'єктів адміністративно-правового забезпечення інформаційної безпеки в Україні. Науковий вісник Ужгородського національного університету. 2024. Вип. 83. Ч. 2.

65. С. 277–287. (Серія «Право»). URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/42-1.pdf>.

66. Куракін О. М., Романов М. Ю. Співвідношення верховенства права та закону в розрізі соціологічної концепції праворозуміння. Науковий вісник Херсонського державного університету. 2015. № 2 (1). С. 33–36. (Серія «Юридичні науки»).

67. Ліпкан В. А. Національна безпека України : навч. посіб. Київ : Кондор, 2006. 552 с.

68. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. Київ : КНТ, 2006. 280 с.

69. Лыченко И. Административно-правовой механизм противодействия правонарушениям в сфере собственности. *Leges et Viata*. 2014. Вип. 1/3 (265). С. 68–71.

70. Малашко О. Є. Адміністративно-правові засоби забезпечення інформаційної безпеки в Україні. *Scientific Notes of Lviv University of Business and Law*. 2020. Vol. 24. С. 145–149. DOI: <https://doi.org/10.5281/zenodo.3894507>.

71. Малиновська О. А. Міграційна політика: глобальний контекст та українські реалії : монографія. Київ : НІСД, 2018. 472 с.

72. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і безпека*. 2015. № 2 (57). С. 107–113.

73. Миджин Г. Є. Структура адміністративно-правового механізму захисту прав на об'єкти інтелектуальної власності. *Соціально-правові студії*. 2020. Вип. 2 (8). С. 72–79. URL: https://sls-journal.com.ua/web/uploads/pdf/S&LS_2020_Vol.%203,%20No.%202_72-79.pdf.

74. Микитюк М. А. Державна охорона в Україні – адміністративно-правове регулювання : монографія. Львів : Львів. політехніка, 2018. 472 с.

75. Моргунов О. А. Поняття та механізм адміністративно-правового регулювання публічного адміністрування сфер фізичної культури і спорту. Юридичний науковий електронний журнал. 2019. № 3. С. 274–277. URL: http://www.lsej.org.ua/3_2019/72.pdf.

76. Національна безпека України: сутність, структура та напрямки реалізації : навч. посіб. / [О. Г. Данільян та ін.]. Харків : Фоліо, 2002. 285 с.

77. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Гельветика, 2017. 168 с.

78. Негодченко В. О. Адміністративно-правове забезпечення державної інформаційної політики органами Національної поліції України : дис. ... д-ра юрид. наук : 12.00.07. Харків, 2017. 455 с. URL: <http://info.dgu.edu.ua/jspui/bitstream/123456789/238/1/%D0%B4%D0%B8%D1%81%D1%81%D0%B5%D1%80%20%D0%9D%D0%B5%D0%B3%D0%BE%D0%B4%D1%87%D0%B5%D0%BD%D0%BA%D0%BE.pdf>.

79. Негодченко В. О. Інформаційна безпека в органах Національної поліції України: адміністративно-правове забезпечення. Право і суспільство. 2020. № 6. С. 167–174. URL: http://pravoisuspilstvo.org.ua/archive/2020/6_2020/26.pdf.

80. Нижник Н. Р., Ситник Г. П., Білоус В. Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навч. посіб. Ірпінь : Акад. ДПС України, 2000. 304 с.

81. Нізельник О. До питання визначення поняття режимно-секретного забезпечення оперативно-розшукової й кримінальної процесуальної діяльності Національної поліції України. Національний юридический журнал: теория и практика. 2019. № 2. Т. 1. С. 113–115. URL: http://www.jurnaluljuridic.in.ua/archive/2019/2/part_1/26.pdf.

82. Олійник О. В. Адміністративно-правові засоби забезпечення інформаційної безпеки. Юридичний вісник. 2015. № 1. С. 65–69.

83. Олійник О. В. Нормативно-правове забезпечення інформаційної безпеки в Україні. Право і суспільство. 2012. № 3. С. 132–137.

84. Ордулі Е. До питання про правовий механізм захисту прав інтелектуальної власності в Україні. Теорія та практика інтелектуальної власності. 2019. № 6. С. 55–64.

85. Остапенко О., Баїк О. Адміністративно-правова природа інформаційної безпеки. Вісник Національного університету «Львівська політехніка». 2021. № 3 (31). С. 167–179. (Серія «Юридичні науки»). URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2021/nov/25402/25.pdf>.

86. Пересада О. М. Роль Національної поліції України в забезпеченні інформаційної безпеки держави: теоретико-методологічні аспекти. Правовий часопис Донбасу. 2019. № 4 (69). С. 183–189.

87. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. Юридичний журнал. 2009. С. 122–135.

88. Пилипчук В. Теоретико-правові проблеми подолання глобальних викликів і загроз національній безпеці. Вісник Академії правових наук України. 2008. № 1 (52). С. 22–30.

89. Пиріжок Ю. Організаційно-правовий механізм забезпечення інформаційної безпеки : магістерська робота : 281 «Публічне управління та адміністрування». Хмельницький, 2022. 87 с. URL: <https://irlykhuml.univer.km.ua/server/api/core/bitstreams/fcb93f87-4419-4831-8dca-b78aa98452b7/content>.

90. Питання діяльності Міністерства інформаційної політики України : постанова Кабінету Міністрів України від 14 січ. 2015 р. № 2. URL: <http://zakon.rada.gov.ua/laws/show/2-2015-п>.

91. Плєскач М. В. Сутність поняття та основні елементи механізму адміністративно-правового забезпечення кібернетичної безпеки людини. Часопис Київського університету права. 2020. № 4. С. 201–209. DOI: 10.36695/2219-5521.4.2020.36.

92. Положення про Міністерство культури та інформаційної політики України : постанова Кабінету Міністрів України від 16 жовт. 2019 р. № 885. URL: <https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text>.

93. Почепцов Г. Г. Сучасні інформаційні війни. Вид. 2-ге, доповн. Київ : Києво-Могилянська акад., 2016. 504 с.

94. Присяжнюк А. Й. Адміністративно-правовий механізм забезпечення економічної безпеки держави. Форум права. 2011. № 1. С. 808–813.

95. Присяжнюк М. М., Белошевич Я. С. Інформаційна безпека України в сучасних умовах. Вісник Київського національного університету імені Тараса Шевченка. 2013. Вип. 30. С. 42–46. (Серія «Військово-спеціальні науки»).

96. Пришляк М. І. Механізм адміністративно-правового забезпечення медичного обстеження наречених в Україні:

поняття та загальний аналіз складових елементів. Держава та регіони. 2017. Вип. 3. С. 46–52. (Серія «Право»).

97. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23 лют. 2006 р. № 3475-IV. URL: <http://zakon.rada.gov.ua/laws/show/3475-15>.

98. Про державну таємницю : Закон України від 21 січ. 1994 р. № 3855-XII. Відомості Верховної Ради України. 1994. № 16. Ст. 93.

99. Про затвердження Інструкції з діловодства в системі Міністерства внутрішніх справ України : наказ МВС України від 23 серп. 2012 р. № 747. URL: <https://zakon.rada.gov.ua/rada/show/v0747320-12#Text>.

100. Про затвердження Інструкції з діловодства в системі Національної поліції : наказ Національної поліції України від 20 трав. 2016 р. № 414. URL: <http://tranzit.ltd.ua/nakaz/>.

101. Про затвердження Положення про Департамент організаційно-аналітичного забезпечення та оперативного реагування Національної поліції України : наказ Національної поліції України від 27 серп. 2015 р. № 126. URL: <http://tranzit.ltd.ua/nakaz/>.

102. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481.

103. Про Національну поліцію : Закон України від 2 лип. 2015 р. № 580-VIII. URL: <https://zakon.rada.gov.ua/laws/show/580-19#Text>.

104. Про Національну програму інформатизації : Закон України від 4 лют. 1998 р. № 74/98-ВР. URL: <http://zakon2.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80>.

105. Про основи національної безпеки України : Закон України від 19 черв. 2003 р. № 964-IV. URL: <http://zakon.rada.gov.ua/laws/show/964-15>.

106. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 берез. 2016 р. № 96. Офіційний вісник Президента України. 2016. № 10. Ст. 198.

107. Проблеми інформаційного законодавства України у сфері створення, поширення й використання інформації й шляхи їхнього рішення. Аналітична записка. НІСД : [сайт]. URL: <http://www.niss.gov.ua/articles/1189/>.

108. Протидія злочинам у сфері земельних відносин : навч. посіб. / [С. В. Андрусенко, О. М. Бандурка, М. С. Рябченко та ін.] ; за заг. наук. ред. С. М. Гусарова. Харків : ХНУВС, 2013. 170 с.

109. Розгон О. Г. Адміністративна відповідальність поліцейських у період дії воєнного стану в Україні: роздуми про перспективи удосконалення. Дніпровський науковий часопис публічного управління, психології, права. 2022. Вип. 6. С. 160–163. DOI: <https://doi.org/10.51547/ppp.dp.ua/2022.6.26>.

110. Романов М. Організаційно-правові засади судового контролю, прокурорського нагляду та взаємодії з громадськістю в діяльності підрозділів дізнання Національної поліції України. Право і суспільство. 2021. № 5. С. 224–231. DOI: <https://doi.org/10.32842/2078-3736/2021.5.30>.

111. Романов М. Поняття, сутність і значення діяльності підрозділів дізнання. Науковий вісник Національної академії внутрішніх справ. 2021. № 2 (26). С. 102–106. DOI: <https://doi.org/10.33270/01211192.102>.

112. Романов М. Функціонування підрозділів дізнання Національної поліції України: до питання визначення функцій як елементу організаційних засад. Честь і закон. 2021. № 3 (78). С. 89–93. DOI: <https://doi.org/10.33405/2078-7480/2021/3/78/244558>.

113. Романов М. Ю. Організаційно-правові засади забезпечення функціонування підрозділів дізнання Національної поліції України : дис. ... д-ра філософії : 081 «Право». Київ, 2022. 264 с.

114. Романов М. Ю. До питання визначення місця і ролі перепідготовки як форми післядипломної освіти дізнавачів Національної поліції України. Актуальні проблеми юридичної науки та практики у ХХІ столітті : матеріали Міжнар. наук.-практ. конф. (Рівне, 23–24 верес. 2021 р.). Рівне : Міжнар. екон.-гуманіт. ун-т ім. акад. С. Дем'янчука, 2021. С. 73–76.

115. Романов М. Ю. Забезпечення права на свободу та особисту недоторканість дізнавачами Національної поліції України: адміністративно-правовий аспект. Діяльність органів досудового розслідування в умовах реформування правоохоронних органів : матеріали Всеукр. наук.-практ. конф. (Дніпро, 21 трав. 2021 р.). Дніпро : Дніпроп. держ. ун-т. внутр. справ, 2021. С. 76–79.

116. Романов М. Ю. Зміст і сутність поняття стажування в контексті післядипломної освіти працівників підрозділів дізнання Національної поліції України. Актуальні дослідження правових та економічних процесів у контексті євроінтеграції : матеріали Всеукр. наук.-практ. конф. (Дніпро, 2 черв. 2021 р.). Дніпро : Дніпроп. держ. ун-т. внутр. справ, 2021. С. 185–188.

117. Романов М. Ю. Організаційно-правові основи функціонування підрозділів дізнання Національної поліції України. Механізм функціонування громадянського суспільства : зб. тез Всеукр. наук. конф. (Львів, 18 груд. 2021 р.). Львів : ЛьвДУВС, 2020. С. 282–284.

118. Романов М. Ю. Поняття та сутність функцій підрозділів дізнання Національної поліції України в контексті організаційно-правового забезпечення. Правові засади організації та здійснення публічної влади : матеріали IV Міжнар. наук.-практ. конф. (Хмельницький, 2–6 берез. 2021 р.). Хмельницький : Хмельн. ун-т. упр. та права ім. Л. Юзькова, 2021. С. 449–452.

119. Романов М. Ю. Спеціалізація як форма післядипломної освіти дізнавачів Національної поліції України: проблеми та перспективи. Реформування законодавства та державних інституцій: прогалини, досягнення та перспективи : матеріали Всеукр. наук.-практ. конф. (Рівне, 24–25 трав. 2021 р.). Рівне : Міжнар. екон.-гуманіт. ун-т ім. акад. С. Дем'янчука, 2021. С. 172–175.

120. Романов М. Ю., Кобзар О. Ф. Організаційно-правові, адміністративні та кримінальні процесуальні аспекти діяльності підрозділів дізнання Національної поліції України : монографія. Кропивницький : ДонДУВС, 2022. 498 с.

121. Сахно А. П. Значення законності й дисципліни в діяльності ОВС України та шляхи їх зміцнення. Проблеми правознавства та правоохоронної діяльності. 2010. № 3. С. 71–77.

122. Сенік С. В. Повноваження Національної поліції у сфері інформаційно-аналітичного забезпечення. Сучасний конституціоналізм: проблеми теорії та практики : матеріали

наук. семінару (Львів, 23 черв. 2017 р.). Львів : ЛьВДУВС, 2017. С. 243–247.

123. Ситник Г. П., Олуйко В. М., Вавринчук М. П. Національна безпека України: теорія і практика : навч. посіб. Київ : Кондор, 2007. 616 с.

124. Скакун О. Теорія держави і права (енциклопедичний курс) : підручник. Харків : Еспада, 2006. 776 с.

125. Смелік В. Б. Міжнародно-правові засади інституційної системи Інтерполу : дис. ... канд. юрид. наук : 12.00.11. Ірпінь, 2005. 225 с.

126. Стратегія інформаційної безпеки : Указ Президента України від 28 груд. 2021 р. № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#n5>.

127. Сулацький В. Поняття та структура адміністративно-правового механізму превентивної діяльності Національної поліції України. Підприємництво, господарство і право. 2021. № 3. С. 196–200. (Серія «Адміністративне право і процес»). DOI: <https://doi.org/10.32849/2663-5313/2021.3.31>.

128. Терехов В. Удосконалення адміністративно-правового регулювання реалізації політики інформаційної безпеки в органах місцевого самоврядування. Актуальні проблеми правознавства. 2017. № 1. С. 43–47. DOI: <https://doi.org/10.35774/app2017.01.043>.

129. Тихомиров О. О., Тугарова О. К. Юридична відповідальність за правопорушення в інформаційній сфері : навч. посіб. Київ : Нац. акад. СБУ, 2015. 172 с.

130. Ткачук Т. Суб'єкти забезпечення інформаційної безпеки держави: функціональний аналіз. Национальный юридический журнал: теория и практика. 2017. № 6. Т. 2. С.

- 42–46. URL:
http://jurnaluljuridic.in.ua/archive/2017/6/part_2/9.pdf.
131. Управління органами Національної поліції України : підручник / [О. М. Бандурка, О. І. Безпалова, О. В. Джафарова та ін.] ; за заг. ред. В. В. Сокурєнка. Харків : Стильна тип., 2017. 580 с.
132. Федорова Н. Є., Смієсова В. Л. Інформаційна безпека та шляхи її забезпечення на етапі інформаційно-технологічної революції. Причорноморські економічні студії. 2020. Вип. 57. URL:
http://bses.in.ua/journals/2020/57_2020/4.pdf.
133. Федотов Д.В. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Національній поліції України: до питання змісту. Правові проблеми сучасності та наукові підходи до їх вирішення: матеріали міжнародної науково-практичної конференції, м. Київ, 25–26 січня 2023 р. – Київ: Науково-дослідний інститут публічного права, 2023. С. 139–141.
134. Федотов Д.В. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Національній поліції України: конструктивні особливості. Актуальні проблеми взаємодії правової науки та практики її застосування: матеріали міжнародної науково-практичної конференції, м. Київ, 16–17 березня 2022 р. – Київ: Науково-дослідний інститут публічного права, 2022. С. 118–120.
135. Федотов Д.В. До питання поняття правового регулювання адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України. Проблемні питання юридичної науки в контексті реформування правової системи України: матеріали міжнародної науково-практичної конференції, м. Київ, 19–20

жовтня 2022 р. – Київ: Науково-дослідний інститут публічного права, 2022. С. 221–223.

136. Федотов Д.В. Інформаційна безпека у контексті її адміністративно-правового забезпечення. Науково-практичні засади розвитку юридичної науки на сучасному етапі державотворення: матеріали міжнародної науково-практичної конференції, м. Київ, 15–16 лютого 2023 р. – Київ: Науково-дослідний інститут публічного права, 2023. С. 117–120.

137. Федотов Д.В. Інформаційна безпека як об'єкт адміністративно-правового забезпечення. Держава та регіони. Серія Право. 2022. № 2. С. 287-291. DOI <https://doi.org/10.32782/1813-338X-2022.2.47>

138. Федотов Д.В. Правове регулювання адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України. Науковий вісник публічного та приватного права. 2024. Випуск 4. С. 178-182.

139. Федотов Д.В. Система суб'єктів забезпечення інформаційної безпеки в Національній поліції України та їх характеристика. Інноваційні підходи до реформування сучасного законодавства: матеріали міжнародної науково-практичної конференції, м. Київ, 20–21 квітня 2023 р. – Київ: Науково-дослідний інститут публічного права, 2023. С. 144–146.

140. Федотов Д.В. Структура адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України. Юридичний науковий електронний журнал. 2023. № 6. С. 853-856. DOI <https://doi.org/10.32782/2524-0374/2023-6/207>

141. Федотов Д.В. Суб'єкти забезпечення інформаційної безпеки в Національній поліції України. Право і суспільство.

2024. № 2. С. 624-629. DOI <https://doi.org/10.32842/2078-3736/2024.2.89>

142. Філіппов С. О. Протидія транскордонній злочинності: глобальний контекст і реалії України : монографія. Одеса : Фенікс, 2019. 450 с.

143. Черноіваненко А. В., Галуцько В. В. Інформаційне забезпечення підготовки, прийняття і реалізації управлінських рішень: теоретичний підхід до визначення поняття. Актуальні проблеми розвитку управлінських систем: досвід, тенденції, перспективи : зб. тез IV студент. наук.-практ. конф. (Харків, 23 квіт. 2009 р.). Харків : Магістр, 2009. С. 120-123.

144. Чистоклетов Л. Г., Хитра О. Л. Адміністративно-правові засоби у забезпеченні інформаційної безпеки України. ІТ-право: проблеми та перспективи розвитку в Україні : зб. матеріалів II Міжнар. наук.-практ. конф. (Львів, 17 листоп. 2017 р.). Львів, 2017. С. 212–217.

145. Шабетя С. А., Несін В. В. Правові питання забезпечення інформаційної безпеки особи в Україні. Юридичний науковий електронний журнал. 2021. № 4. С. 293–296 URL: http://www.lsej.org.ua/4_2021/73.pdf.

146. Шай Р. Я. Принципи та форми реалізації функцій держави. Вісник Національного університету «Львівська політехніка». 2014. № 810. С. 116–123. (Серія «Юридичні науки»). URL: http://nbuv.gov.ua/UJRN/vnulpurn_2014_810_21.

147. Шапіро В. С. Адміністративна відповідальність за порушення законодавства України про інформацію. Науково-теоретична конференція викладачів, аспірантів, співробітників та студентів юридичного факультету : тези

доп. (Суми, 20 квіт. 2011 р.) : у 3 ч. Суми : СумДУ, 2011. Ч. 2. С. 171–176.

148. Шведа Н. М. Документаційне забезпечення управління : навч. посіб. для студентів спец. 074 «Публічне управління та адміністрування» та 281 «Публічне управління та адміністрування». Тернопіль : ТНТУ ім. І. Пулюя, 2018. 98 с.

149. Шевчук О., Кузь Т. Правове забезпечення інформаційної безпеки процесу надання електронних адміністративних послуг. Актуальні проблеми правознавства. 2021. № 1 (25). С. 59–65. DOI: 10.35774/app2021.01.059.

150. Штанько Г. Ю. Внутрішньоорганізаційна діяльність у сфері кадрового забезпечення органів Національної поліції України. Актуальні проблеми сучасної науки в дослідженнях молодих учених : тези доп. наук.-практ. конф. (Харків, 17 трав. 2017 р.). Харків : ХНУВС, 2017. С. 185–186. URL: https://univd.edu.ua/general/publishing/konf/17_05_2017_2/pdf/48.pdf.

151. Шумейко Т. А. Поняття та ознаки адміністративно-правового механізму формування та реалізації державної політики у сфері обігу зброї в Україні. Юридична наука. 2020. № 8 (110). С. 169–176. DOI: 10.32844/2222-5374-2020-110-8.21.

152. Шустрова К. В. Адміністративно-правове регулювання діяльності засобів масової інформації в Україні. Сучасні проблеми адміністративного права та процесу : тези доп. Всеукр. наук.-практ. конф. (Харків, 30 черв. 2017 р.). Харків : ХНУВС, 2017. С. 170–172. URL: https://univd.edu.ua/general/publishing/konf/30_06_2017/pdf/59.pdf.

153. Яковлев П. О. Механізм адміністративно-правового регулювання державного управління у сфері забезпечення інформаційної безпеки України. Правова позиція. 2020. № 2 (27). С. 74–77. URL: <https://legalposition.umsf.in.ua/archive/2020/2/14.pdf>.

154. Definition of ‘mechanism’. Collinsdictionary : [site]. URL: <https://www.collinsdictionary.com/dictionary/english/mechanism>.

155. Федотов Д.В. Поняття адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України. KELM (Knowledge, Education, Law, Management). 2023. № 7. С. 386-390. DOI <https://doi.org/10.51647/kelm.2023.7.64>

156. ISO/IEC 17799:2005. Information technology. Security techniques – Code for practicefor information security management. ENISA : [site]. URL: <https://www.enisa.europa.eu/topics/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-17799>.

157. Kaletnik V. Current State of Administrative and Legal Ensuring of Information Security in Ukraine: Theoretical and Legal Analysis. Scientific Works of National Aviation University. 2021. Vol. 2. No. 59. P. 70–77. (Series «Air and Space Law»). DOI: <https://doi.org/10.18372/2307-9061.59.15597>.

Наукове видання

Федотов Данило Вадимович
Романов Максим Юрійович

АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ

Монографія

Підп. до друку 23.09.2025. Формат 60×84/16
Папір офсетний. Друк цифровий.
Ум. друк. арк. 12,09. Зам. № 2409-25.
Наклад 300 прим.

Виготовлювач ТОВ «7БЦ»
03087, м. Київ, вул. Олекси Тихого, 84
e-mail: 7bc@ukr.net, тел: (044) 592-00-80
Свідоцтво суб'єкта видавничої справи ДК №5329 від 11.04.2017