

УДК 342.95

DOI <https://doi.org/10.32782/pdu.2023.2.60>**Е. А. Мамедова**

ад'юнкт кафедри адміністративного права, процесу та адміністративної діяльності
Дніпропетровський державний університет внутрішніх справ
ORCID ID: 0000-0001-9199-4431

МЕХАНІЗМ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПАТРУЛЬНОЇ ПОЛІЦІЇ В УКРАЇНІ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ УДОСКОНАЛЕННЯ

У статті висвітлено наукові підходи та нормативно-правове визначення змісту поняття механізм адміністративно-правового забезпечення кібербезпеки патрульної поліції. Виявлено, що захист інформаційних систем Національної поліції, що використовуються патрульною службою, в яких обробляють значну частину офіційної інформації та персональних даних громадян, не повністю відповідають вимогам законодавства, що збільшує ризики втручання у такі системи, загрожує конфіденційності, недоторканності наявної інформації в реєстрах, базах даних, яка покликана задовольнити потреби та забезпечити гарантовані Конституцією інтереси громадян, суспільства та держави. У статті розкриваються проблеми формування сучасної концепції механізму адміністративно-правового забезпечення кібербезпеки патрульної поліції та його засад. З'ясовано, що формування цієї концепції повинно здійснюватися з урахуванням потреб держави та прав громадян, дотримання верховенства права, засобів правового захисту, поваги до основних цінностей, прав людини та особи на свободу вираження поглядів, однаковий захист загально визнаних основних прав. Основними засадами механізму адміністративно-правового забезпечення кібербезпеки патрульної поліції визначено: принцип мінімального необхідного регулювання, принцип забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, послуг із захисту інформації, кіберзахисту, зокрема прав щодо невтручання в приватне життя та захисту персональних даних як поліцейських так і громадян; принцип прозорості рішень та заходів органів Національної поліції щодо забезпечення кібербезпеки; принцип об'єктивності і правової визначеності. Механізм адміністративно-правового забезпечення кібербезпеки патрульної поліції визначено як систему юридичних, організаційних, ідеологічних, технічних та інших заходів впливу з використанням інформаційних ресурсів, мереж, програмного забезпечення, носіїв інформації, засобів фото- та відеозйомки в роботі патрульних поліцейських, що здійснюється уповноваженими суб'єктами на суспільні відносини, які виникають при використанні кіберпростору для ефективного інформаційного забезпечення функціонування патрульної поліції, своєчасного виявлення, запобігання і нейтралізації реальних і потенційних кіберзагроз. У статті визначено елементи механізму адміністративно-правового забезпечення кібербезпеки патрульної поліції. Виявлено недоліки поточного функціонування механізму адміністративно-правового забезпечення кібербезпеки патрульної поліції та запропоновано напрями удосконалення правового та організаційного характеру.

Ключові слова: Національна поліція України, кібербезпека, патрульна поліція, засади кібербезпеки, механізм забезпечення, адміністративно-правове забезпечення, елементи механізму, недоліки функціонування, напрями удосконалення.

Постановка проблеми. Протягом 2022 року Україна стикнулася з 7000 кібератак на інформаційну інфраструктуру. За минулий рік в Україні було зареєстро-

вано у 2,8 раза більше кіберінцидентів, ніж у 2021 році [1]. 14 січня 2022 року розпочався шквал атак, і першою була масована атака на веб-сайти низки державних органів [2]. Серед інформаційних ресурсів, що піддавались кібератакам були

також ресурси Національної поліції України. Тому в сучасний період МВС України приділяє особливу увагу створенню умов для ефективного захисту прав фізичних та юридичних осіб із використанням передових інформаційних технологій. Пріоритетними напрямками в цій роботі є захист інформаційних прав, запобігання комп'ютерним злочинам, протидія кібертероризму та боротьба з організованою злочинністю в інформаційній сфері. Під час збройної агресії проти України ще більше посилюється питання необхідності кібернетичного захисту інформації в мережах та базах даних МВС.

Патрульна поліція України реалізовує інформаційно-аналітичну діяльність з метою забезпечення ефективності своєї роботи. Ця діяльність включає створення власних баз даних, які є частиною єдиної інформаційної системи Національної поліції України та Міністерства внутрішніх справ України. Патрульна поліція має доступ до баз даних Національної поліції України, Міністерства внутрішніх справ України та інших державних органів. Вона також здійснює інформаційний пошук, аналітичну роботу та обробку персональних даних та іншої інформації з обмеженим доступом в рамках своїх повноважень, які визначені законодавством. Крім того, патрульна поліція забезпечує інформаційну взаємодію з іншими державними органами України, правоохоронними органами іноземних країн та міжнародними організаціями. Це дозволяє патрульній поліції отримувати необхідну інформацію для виконання своїх функцій та забезпечувати безпеку громадян.

З огляду на це існує потреба в дослідженні можливих напрямів удосконалення механізму адміністративно-правового забезпечення кібернетичної безпеки патрульної поліції.

Аналіз останніх досліджень і публікацій. Різні аспекти правового забезпечення кібернетичної безпеки держави, галузей та осіб досліджуються вітчизняними та зарубіжними вченими-правознавцями. Значний внесок у дослідження теоретичних питань, пов'язаних з проблемами адміністративно-правових засад забезпечення кібербезпеки

у сфері публічного управління України, зробили такі науковці: Л. В. Балабанова, Є.Ю. Бараш, Є.Д. Бондаренко, В.В. Годін, І.О. Ієрусалимов, Р.А. Калюжний, В.В. Лушер, С.М. Петренко, А.С. Політова, В.В. Галуцько, О.К. Юдін та інші. Дослідженням питань інформаційного забезпечення, інформаційної безпеки та кібербезпеки правоохоронних органів, опікувались такі вчені як Є.Д. Бондаренко, Г.О. Блінова, В.В. Бухарев, В.А., В.О. Єльцов, Д.П. Кисленко, В.В. Лушер, Г.М. Шорохова та інші. Проте на сьогодні відсутня сучасна узгоджена концепція механізму адміністративно-правового забезпечення кібербезпеки патрульної поліції в Україні.

Останні дослідження і публікації свідчать про пріоритет науковців щодо вивчення проблематики, орієнтованої на правове забезпечення державної кібернетичної безпеки, не приділяючи значної уваги проблемам адміністративно-правового забезпечення кібернетичної безпеки окремих служб та їх підрозділів.

Формулювання мети статті. Метою цього дослідження є формулювання поняття «механізм адміністративно-правового забезпечення кібербезпеки патрульної поліції», визначення його структурних елементів, з'ясування основних засад цього механізму, виявлення недоліків сучасного функціонування, а також виокремлення деяких напрямів удосконалення механізму адміністративно-правового забезпечення кібербезпеки патрульної поліції із наданням відповідних практичних рекомендацій.

Виклад основного матеріалу. У словнику термін «механізм» визначається як внутрішня структура, система чого-небудь або сукупність станів і процесів, що формують певне явище [3]. У загальному розумінні механізм - це система чи сукупність елементів, які спільно працюють для досягнення конкретної мети або виконання певного завдання. Механізми можуть бути фізичними, такими як механічні пристрої або електронні системи, або абстрактними, такими як процедури або алгоритми. У відповідному контексті, коли йдеться про «механізм управління», це вказує на систему чи сукупність процесів

і методів, які використовуються для керування чимось, таким як організація, проєкт або діяльність. Такий механізм може включати в себе структуру, правила, процедури, технології та інші компоненти, які допомагають досягти поставлених цілей та завдань. В залежності від контексту термін «механізм» може мати різні відтінки значень, але в основному вказує на систему або процес, який забезпечує функціонування чого-небудь [4].

У сфері правової доктрини зараз активно використовуються різноманітні юридичні терміни, такі як «механізм правового забезпечення», «механізм правового регулювання», «механізм адміністративно-правового забезпечення» та інші, як вказує М.В. Плєскач [5, с. 202]. Науковці, досліджуючи правові механізми діяльності, явищ, процесів, вказують на різні його ознаки та особливості. Так, Я.В. Греца при дослідженні правового механізму реалізації та захисту прав і законних інтересів суб'єктів податкових відносин робить акцент на суб'єктивних правах та їх захисті через правові засоби [7]. Д.В. Слинко розглядаючи процесуально-правовий механізм формування і прийняття рішень в ОВС, приходять до висновку, що цей механізм передбачає систему правових та процедурних норм і процесів, які регулюють процедури розробки, ухвалення і виконання рішень у цих органах в рамках їх компетенції [8]. Механізм організаційно-правового забезпечення прав і свобод людини на думку О.В. Негодченко це система взаємопов'язаних елементів, які включають в себе правові засоби, організаційні форми та методи діяльності відповідних державних органів [9, с. 39]. К.Г. Волинка у своїх дослідженнях проявляє інші аспекти механізму забезпечення прав і свобод особи. На її погляд він включає в себе комплекс взаємозв'язаних і взаємодіючих юридичних передумов, нормативних засобів та загально-соціальних умов, що створюють необхідні умови для повноцінного здійснення кожною особою своїх прав і свобод [10]. Зазначене визначення підкреслює важливість взаємодії різних чинників, які допомагають гарантувати права і свободи кожної особи в суспільстві.

Аналіз наукових праць свідчить про те, що часто терміни «механізм правового забезпечення» та «механізм правового регулювання» використовуються взаємозамінно. Наприклад, у своєму дослідженні С.В. Діденко вказує, що оскільки адміністративно-правове забезпечення включає в себе виявлення та створення адміністративних засад та інструментарію для реалізації адміністративно-правових відносин у даній сфері, а також захист та гарантування прав, свобод і законних інтересів суб'єктів цих відносин згідно з правовими нормами, механізм адміністративно-правового забезпечення слід сприймати через призму правового регулювання та використовувати його як основу при формуванні відповідних висновків [6, с. 646].

Підтримуємо позицію М.В. Плєскач, що подібне ототожнення призводить до надмірного звуження змісту поняття «правове забезпечення», а відтак і його механізму, оскільки між цими поняттями є відмінності, які виражаються у змісті, обсязі та структурних елементах. Так, правове регулювання – це передусім здійснюваний за допомогою права і всієї сукупності правових засобів юридичний вплив на суспільні відносини, а правове забезпечення – це складна диференційована єдність багатьох складників: суб'єктів, цілей, результатів, дій та операцій, засобів та способів здійснення такого забезпечення, які не лише функціонально взаємодіють, а й органічно поєднані між собою за допомогою мережі структурних, вертикальних, горизонтальних, координаційних, субординаційних, просторових, часових тощо відносин [5, с. 202; 11, с. 41].

Правове забезпечення та правове регулювання мають відмінні структурні компоненти. У механізмі правового регулювання визначаються такі обов'язкові елементи на окремих його етапах: принципи права, норми права, спеціалізовані норми права, що втілюються в нормативно-правових актах; правовідносини, індивідуалізовані суб'єктивні юридичні права та обов'язки; акти безпосередньої реалізації прав та обов'язків; акти застосування норм права [5, с. 202; 12, с. 499]. У контексті адміністративного права до складової бази механізму правового забезпечення вклю-

чаються такі елементи: об'єкт адміністративно-правового забезпечення; суб'єкти адміністративно-правового забезпечення; принципи права, норми права, правовідносини з їхнім змістом, видами, структурою та особливостями реалізації; гарантії, заходи, засоби, форми, принципи та методи правового забезпечення [13, с. 50].

Враховуючи зазначене, на наш погляд сформульоване М.В. Плєскач визначення механізму адміністративно-правового забезпечення кібернетичної безпеки людини враховує зазначені вище особливості механізму забезпечення. Так М.В. Плєскач визначає механізм адміністративно-правового забезпечення кібернетичної безпеки людини як узятую в єдності складну систему юридичних, організаційних, ідеологічних, технічних та інших заходів впливу, що здійснюється уповноваженими суб'єктами публічної адміністрації на суспільні відносини, які виникають під час використання кібернетичного простору, з метою їх упорядкування, а також для забезпечення охорони й захисту життєво важливих інтересів, прав та свобод людини в цій сфері [5, с. 202]. 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 [5, с. 202].

У попередніх наукових роботах ми визначили поняття кібербезпеки патрульної поліції як стан захищеності службових інтересів патрульної поліції у кіберпросторі, що досягається шляхом дотримання правових, організаційних, технічних вимог з використання інформаційних ресурсів, мереж, програмного забезпечення, носіїв інформації, засобів фото- та

відеозйомки в роботі патрульних поліцейських для ефективного інформаційного забезпечення функціонування патрульної поліції, своєчасного виявлення, запобігання і нейтралізації реальних і потенційних кіберзагроз. На наш погляд, кібербезпеку патрульної поліції можна розглядати як безпеку служби, кібербезпеку Департаменту патрульної поліції – як кібербезпеку установи, а кібербезпеку патрульного поліцейського – як вид кібербезпеки людини, що виконує службові обов'язки [14, с. 21].

Загалом погоджуючись із концепцією М.В. Плєскач щодо структури механізму адміністративно-правового забезпечення кібернетичної безпеки людини, вважаємо, що ключову роль у ефективності функціонування цього механізму відіграють принципи кібербезпеки. Загалом такі принципи визначені у ст. 2 Закону України «Про основні засади забезпечення кібербезпеки України» [15].

Відповідно до ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII Національна поліція є одним із суб'єктів забезпечення кібербезпеки в Україні, водночас слід визначити особливості застосування цих принципів при захисті кіберпростору у сфері функціонування Національної поліції загалом та патрульної поліції зокрема. Таким чином функціонування адміністративно-правового механізму забезпечення кібербезпеки патрульної поліції повинно відповідати зазначеним вище принципам.

На думку В.О. Демиденко згідно із принципом мінімального необхідного регулювання, рішення (заходи) суб'єктів владних повноважень мають бути необхідними та мінімально достатніми для досягнення мети й завдань із забезпечення кібербезпеки України. Цей принцип передбачає, що правозастосовна діяльність суб'єктів владних повноважень повинна органічно поєднувати два аспекти. Так, з одного боку, регулювання суспільних відносин щодо забезпечення кібербезпеки в Україні суб'єктами владних повноважень передбачає мінімальне втручання в цю сферу. Воно не повинно бути бюрократизованим, надмірно регульованим. Адже активне

втручання органів публічної влади, їх посадових і службових осіб у цю сферу призведе до певного обмеження прав і свобод людей щодо вільної комунікації через функціонування сумісних (з'єднаних) комунікаційних систем і забезпечення електронних комунікацій із використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Це негативно позначиться на можливостях громадянського суспільства щодо протидії корупції, громадянського контролю за законністю й ефективністю діяльності органів публічної влади. Таким чином, може виникнути ситуація, за якої елементарні відносини не витримують тиску нагромаджених зверху норм і приписів, що, зрештою, призведе до збоїв у роботі – від ігнорування до цілковитого заперечення [16, с. 144]. З іншого боку суб'єкти з державно-владними повноваженнями, у тому числі органи Національної поліції мають здійснювати регулювання суспільних відносин щодо забезпечення кібербезпеки в діяльності патрульної поліції тією мірою, яка однозначно забезпечить формування ефективної системи кібербезпеки цієї служби, її підрозділів та працівників.

Наступним принципом застосування законодавства у сфері кібербезпеки суб'єктами з державно-владними повноваженнями є забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, послуг із захисту інформації, кіберзахисту, зокрема прав щодо невтручання в приватне життя та захисту персональних даних. Цей принцип стосуються як працівників поліції так і громадян України, інформацію про яких обробляється в інформаційних системах МВС України. Водночас у межах забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, вважає О.В. Демиденко, законодавець акцентує увагу на невтручанні в приватне життя й захисті персональних даних [16, с. 144]. Особливості захисту персональних даних в роботі патрульної поліції та напрями удосконалення механізму кібербезпеки у цьому напрямі нами було досліджено у попередніх роботах.

Слід зауважити, що одним із важливих принципів застосування законодавства у сфері кібербезпеки патрульної поліції є також принцип прозорості, згідно з яким рішення (заходи) органів Національної поліції мають бути належно обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування). Реалізація цього принципу в правозастосовній діяльності органів поліції є гарантією розробки та прийняття обґрунтованого підзаконного акту, що враховує всі особливості функціонування кеїберпростору в якому функціонують підрозділи патрульної поліції та діють поліцейські.

Водночас прозорість прийняття рішень суб'єктами владних повноважень у сфері електронних комунікацій сприяє досягненню інформаційної стабільності та безпеки, посилює ефективність протидії кібератакам, підвищує рівень довіри громадян до влади. Принцип прозорості в правозастосовній діяльності, наголошує О.В. Демиденко, має бути непорушним не лише на етапі прийняття кінцевого правозастосовного акту, а й на стадії підготовки проекту рішення, вивчення об'єктивних обставин конкретної життєвої ситуації, що потребує реагування цих органів, їх посадових і службових осіб у сфері забезпечення кібербезпеки. Максимальне залучення громадськості до підготовки та прийняття відповідних соціально орієнтованих управлінських рішень значною мірою впливає на рівень довіри до управлінської діяльності, пов'язаної з електронними комунікаційними системами, поінформованості про цю діяльність органів державної влади [16, с. 148]. На наш погляд, аналогічним впливом на сприйняття та дотримання у майбутньому норм прийнятого підзаконного нормативно-правового акту, що регулює порядок дотримання кібербезпеки в патрульній поліції впливатиме вивчення думки поліцейських про положення проекту відповідного документу при проведенні тренінгів з кібербезпеки та анкетування.

Водночас із 231 опитаного працівника патрульної поліції 70,1% патрульних поліцейських вказали, що заняття з кібербезпеки для них не проводилися.

Подібна ситуація і з методичними розробками щодо дотримання правил кібербезпеки патрульної поліції: 78,8% опитаних вказали, що таких методичних розробок в їх службі немає, відповідно лише 21,2% поліцейським такі методичні розробки надавалися. Що вказує на необхідність приділення більшої уваги реалізації принципу прозорості, згідно з яким рішення (заходи) органів Національної поліції щодо забезпечення кібербезпеки мають бути належно обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності [17].

Важливим принципом застосування законодавства у сфері забезпечення кібербезпеки є об'єктивність і правова визначеність, максимально можливе застосування національного та міжнародного права щодо повноважень й обов'язків державних органів, органів місцевого самоврядування, підприємств, установ, організацій, громадян у сфері кібербезпеки, наголошує О.В. Демиденко [16, с. 144]. Застосовуючи законодавство України у сфері забезпечення кібербезпеки, органи влади повинні максимально точно й усебічно аналізувати події та дії суб'єктів правовідносин щодо електронних комунікацій, захисту галузевих інформаційних ресурсів, інформації тощо, ураховуючи їхню багатогранність і суперечливість, позитивні та негативні аспекти, на підставі цього приймати правове легітимне рішення. Прийняття такого рішення має відповідати положенням національного та міжнародного права. Під час застосування правових норм національного та міжнародного права може постати питання щодо співвідношення юридичної сили вітчизняних і міжнародних нормативно-правових актів із забезпечення кібербезпеки [16, с. 144].

Нормативні засади механізму адміністративно-правового забезпечення кібербезпеки патрульної поліції містяться як у галузях публічного, так і у галузях приватного права, зокрема у конституційному, адміністративному, кримінальному праві. Загалом проведене нами опитування 231 працівника патрульної поліції продемонструвало наступне. Вони вважають, що документи, в яких визначені правила дотримання кібербезпеки в роботі

патрульної поліції це перш за все Закон України «Про захист інформації в інформаційно-комунікаційних системах» - зазначили 71,9% опитаних та Закон України «Про основні засади забезпечення кібербезпеки України» - так вважають 68,8% поліцейських. В Конституції України та в Законі України «Про Національну поліцію» також на думку опитаних зазначені правила - 36,8% та 34,2 % відповідно. Менше опитаних вважають, що ці правила визначені в документі «Стратегія інформаційної безпеки» - 24,2%. В таких документах як «Дисциплінарний статут Національної поліції України» та «Внутрішні правила та інструкції патрульної поліції» менше всього визначені правила дотримання кібербезпеки в роботі патрульної поліції - 7,8% та 5,2% відповідно. Досить суперечливі відповіді патрульних поліцейських щодо положень, які визначають необхідність дотримання правил кібербезпеки в їх посадових інструкціях: у половини є такі положення в посадовій інструкції, у іншій половини таких положень немає в посадовій інструкції [17].

Окресливши основні засади та елементи механізму адміністративно-правового забезпечення кібернетичної безпеки патрульної поліції, слід зазначити, що є певні недоліки в його поточному функціонування. Так результати проведеного опитування працівників поліції свідчать, що під час своєї службової діяльності 62,3% з них стикались з проблемами в роботі технічних засобів при обміні інформацією; 19,5% зустрічались із порушеннями громадян у сфері кібербезпеки; зникла чи блокувалась службова інформація у 17,3% опитаних; мали місце кібератаки, котрі відбувались на МВС та негативно впливали на виконання службових обов'язків - 12,1%; порушення законодавства з інформаційної/ кібербезпеки допускались також серед колег - 8,2% [17].

Основними проблемами у сфері кібербезпеки патрульної поліції були також: постійна некоректна робота технічного засобу (планшетного пристрою, комп'ютера) є найчастішою проблемою під час роботи з ним - так вказали 48,5% опитаних, також при його використанні не можна отримати потрібну інформацію -

22,1% вказали на цю проблему, інформацію, яку видає пристрій треба повторно перевіряти – так зазначили 18,6% респондентів, на відсутність зв'язку та Інтернету вказали 4,3% поліцейських [17]. На наш погляд це свідчить про необхідність дослідження механізму кібербезпеки патрульної поліції та пошуку шляхів удосконалення засад його адміністративно-правового забезпечення.

Для удосконалення забезпечення інформаційної/кібербезпеки у підрозділі патрульні бачать такі напрямки: проведення тренінгів про засади забезпечення кібербезпеки для покращення обізнаності мене та працівників мого підрозділу – 47,6%, розробка окремої інструкції про забезпечення кібербезпеки в патрульній поліції – 43,3%, внесення змін до чинного законодавства – 41,6%, посилення дисциплінарної відповідальності за порушення правил забезпечення кібербезпеки 15,6% [17].

Висновки. На сьогодні відсутня комплексна концепція кібербезпеки патрульної поліції, що призводить до порушень інформаційного законодавства в роботі патрульної поліції, завдається шкода правам громадян та юридичних осіб та створюються перешкоди для виконання службових обов'язків. Тому ми пропонуємо під механізмом адміністративно-правового забезпечення кібербезпеки патрульної поліції розуміти систему юридичних, організаційних, ідеологічних, технічних та інших заходів впливу з використання інформаційних ресурсів, мереж, програмного забезпечення, носіїв інформації, засобів фото- та відеозйомки в роботі патрульних поліцейських, що здійснюється уповноваженими суб'єктами на суспільні відносини, які виникають при використанні кіберпростору для ефективного інформаційного забезпечення функціонування патрульної поліції, своєчасного виявлення, запобігання і нейтралізації реальних і потенційних кіберзагроз.

Основними принципами (засадами) адміністративно-правового забезпечення кібербезпеки патрульної поліції є : принцип мінімального необхідного регулювання, тобто рішення суб'єктів владних повноважень системи МВС мають бути необхідними та мінімально достатніми для

досягнення мети й завдань із забезпечення кібербезпеки; забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, послуг із захисту інформації, кіберзахисту, зокрема прав щодо невтручання в приватне життя та захисту персональних даних як поліцейських так і громадян; принцип прозорості, згідно з яким рішення та заходи органів Національної поліції мають бути належно обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності та їх застосування; принцип об'єктивності і правової визначеності, тобто максимально можливе застосування національного та міжнародного права щодо повноважень й обов'язків органів поліції у сфері кібербезпеки.

Основними елементами механізму адміністративно-правового забезпечення кібербезпеки патрульної поліції є: нормативні засади та норми права; об'єкт, тобто правовідносини, що виникають за участю патрульної поліції та патрульних поліцейських, їх зміст, види, структуру та особливості реалізації; суб'єкти адміністративно-правового забезпечення кібернетичної безпеки патрульної поліції; засоби та заходи адміністративно-правового забезпечення кібербезпеки патрульної поліції.

Аналіз результатів опитування 231 патрульних поліцейських виявив низку проблем реалізації механізму адміністративно-правового забезпечення кібербезпеки патрульної поліції. Для мінімізації прояву цих проблем та для удосконалення механізму адміністративно-правового забезпечення кібербезпеки патрульної поліції можна запропонувати наступні заходи: у Правилах етичної поведінки поліцейських закріпити положення про дотримання принципів та правил кібербезпеки; закріпити в посадових інструкціях керівників підрозділів патрульної служби обов'язків з перевірки дотримання вимог кібербезпеки працівниками патрульної поліції; ввести зміни до посадових інструкцій працівників відповідних підрозділів патрульної поліції, з метою конкретизації їх повноважень щодо дотримання правил кібербезпеки; розробити методичні реко-

мендації та пам'ятки для працівників поліції щодо дотримання правил кібербезпеки.

Серед організаційних напрямів удосконалення забезпечення кібербезпеки патрульної поліції може бути запропоновано: підвищити рівень контролю за доступом до інформації, що знаходиться у відомчих інформаційних системах через встановлення суворих правил та процедур для доступу до даних в обсязі необхідному для виконання конкретного службового обов'язку чи певного кола службових обов'язків; забезпечити дотримання патрульними поліцейськими вимог професійної етики щодо конфіденційності обробки інформації з обмеженим доступом, персональних даних для запобігання їх розголошенню або незаконному використанню; підвищення надійності технічного захисту систем та мереж, де циркулюють службова інформація від кіберзагроз; конкретизація підстав дисциплінарної відповідальності працівників поліції у сфері кібербезпеки; розроблення планів взаємодії із фахівцями кіберполіції для проведення тренінгів та удосконалення технічного забезпечення кібербезпеки патрульної поліції; створення алгоритмів дій працівників патрульної поліції при ознаках виникнення чи реалізації кіберзагроз та постійне ознайомлення з ними працівників поліції на інструктажах.

Список використаних джерел:

1. Бегаль І. У 2022 році кількість кібератак на Україну зросла майже втричі. 90% хакерських груп з РФ контролюють силовики. URL: <https://forbes.ua/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zroslo-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454>
2. Україна з 14 січня 2022 року залишається на першому місці у світі за кількістю кібератак проти неї - заступник голови Держспецзв'язку. Інтерфакс-Україна. URL: <https://interfax.com.ua/news/interview/911979.html>
3. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В.Т. Бусел. К. Ірпінь: Перун, 2003. 1440 с.
4. Блінова Г.О. Адміністративно-правові засади інформаційного забезпечення органів публічної адміністрації в Україні: актуальні питання теорії та практики: дис.... докт. юрид. наук: 12.00.07. Запоріжжя, 2019. 570 с.
5. Плескач М.В. Сутність поняття та основні елементи механізму адміністративно-правового забезпечення кібернетичної безпеки людини. Часопис Київського університету права. 2020. №4. С. 201-209.
6. 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/Nponyua_2015_16_52
7. Греца Я.В. Правовий механізм реалізації та захисту прав і законних інтересів суб'єктів податкових правовідносин: автореф. дис. ... канд. юрид. наук: 12.00.07 / Ін-т законодавства Верховної Ради України. К., 2006. 20 с.
8. Слинко Д.В. Процесуально-правовий механізм формування і прийняття рішень в органах внутрішніх справ: автореф. дис. ... канд. юрид. наук: 12.00.01 / Нац. ун-т внутр. справ. Х., 2002. 18 с.
9. Негодченко О.В. Забезпечення прав і свобод людини органами внутрішніх справ: організаційно-правові засади: автореф. дис. ... д-ра. юрид. наук : 12.00.07 / Нац. ун-т внутр. справ. Х., 2004. 39 с.
10. Волинка К.Г. Механізм забезпечення прав і свобод особи: питання теорії і практики: автореф. дис. ... канд. юрид. наук: 12.00.01 / НАН України; Ін-т держави і права ім. В.М. Корецького. К., 2000. 18 с.
11. Сидоренко О.П. Правове забезпечення: до питання інтерпретації поняття. Актуальні проблеми вітчизняної юриспруденції. 2018. № 1. С. 39-46.
12. Скакун О.Ф. Теорія держави і права: підручник. Харків: Консум, 2001. 656 с. С. 499.
13. Гумін О.М. Адміністративно-правове забезпечення: поняття та структура. Наше право. 2014. № 4. С. 46-50. С. 50.
14. Блінова Г.О. Мамедова Е.А. Інформаційне забезпечення та кібербезпека патрульної поліції: співвідношення понять. Науковий вісник Дніпропетровського державного університету внутрішніх справ. - 2020. - № 4. - С. 15-24. DOI: 10.31733/2078-3566-2020-4-15-24
15. Про основні засади забезпечення кібербезпеки України. Закон України від 5 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

16. Демиденко В.О. Принципи застосування органами місцевого самоврядування законодавства України у сфері кібербезпеки. Юридичний часопис Національної академії внутрішніх справ. 2018. № 1. С. 141-152 URL: <https://elar.naiu.kiev.ua/server/api/core/bitstreams/2ffd93eb-2b23-4212-a70e-202e93aee9d1/content>
17. Адміністративно-правові засади забезпечення кібербезпеки патрульної поліції України. Аналітичний звіт. Дніпропетровський державний університет внутрішніх справ. 2023. 37 с.

Mamedova E. The mechanism of administrative law support for cybersecurity of the patrol police in Ukraine: current state and prospects for improvement

The article highlights scientific approaches and normative-legal definition of the content of the concept of the mechanism of administrative-legal provision of cyber security of the patrol police. It was found that the protection of information systems of the National Police used by the patrol service, which process a significant part of official information and personal data of citizens, do not fully meet the requirements of the law, which increases the risks of interference in such systems, threatens the confidentiality and integrity of existing information in registers, databases data, which is designed to meet the needs and ensure the interests of citizens, society and the state guaranteed by the Constitution. The article reveals the problems of forming a modern concept of the mechanism of administrative and legal support for cyber security of the patrol police and its principles. It was clarified that the formation of this concept should be carried out taking into account the needs of the state and the rights of citizens, observance of the rule of law, legal remedies, respect for basic values, human and individual rights to freedom of expression, equal protection of universally recognized basic rights. The main principles of the mechanism of administrative and legal protection of cyber security of the patrol police are defined as: the principle of minimum necessary regulation, the principle of ensuring the protection of the rights of users of communication systems and/or consumers of electronic communications services, information protection services, cyber protection, in particular the rights to non-interference in private life and protection of personal data both policemen and citizens; the principle of transparency of the decisions and actions of the National Police bodies regarding the provision of cyber security; the principle of objectivity and legal certainty. The mechanism of administrative and legal protection of cyber security of the patrol police is defined as a system of legal, organizational, ideological, technical and other influence measures using information resources, networks, software, media, photo and video recording equipment in the work of patrol police officers, which is carried out by authorized sub objects on social relations that arise when using cyberspace for effective information support for the functioning of the patrol police, timely detection, prevention and neutralization of real and potential cyber threats. The article defines the elements of the mechanism of administrative and legal support for cyber security of the patrol police. The shortcomings of the current functioning of the mechanism of administrative and legal support for cyber security of the patrol police were identified, and directions for improvement of a legal and organizational nature were proposed.

Key words: National Police of Ukraine, cyber security, patrol police, principles of cyber security, security mechanism, administrative and legal security, elements of the mechanism, shortcomings of functioning, directions for improvement.