теоретичне і практичне значення. Історико-правові дисципліни є фундаментальними у професійній підготовці майбутніх правників, оскільки закладають основи розуміння закономірностей державно-правового розвитку. Водночас їх вивчення сприяє не лише формуванню базових знань, але і навиків критичного мислення, наукового аналізу історичних джерел, що є ключовим у розпізнаванні дезінформації, виробленню усвідомлених оцінок державно-правових явищ. Опанування історико-правовими знаннями закладає міцні підвалини національно орієнтованої правової свідомості, що дозволяє протистояти ворожим інформаційним впливам.

Список використаних джерел

1. Константінов С.Ф. Юридична освіта та підготовка правників в умовах воєнного стану. *Нове українське право*. 2023. № 2. С. 98–103.
2. Капранов Д.В. Історична пам'ять і дезінформація: механізми протидії в умовах гібридної війни. *Інформаційне право України*. 2023. № 1. С. 51–58.

Дручек Олена Василівна,
професор кафедри правового забезпечення та правоохоронної діяльності факультету забезпечення державної безпеки Київського інституту Національної гвардії України, кандидат юридичних наук, доцент
Москалюк Олена Михайлівна,
старший спеціаліст-криміналіст з особливих доручень управління криміналістичного забезпечення головного слідчого управління Національної поліції України, кандидат юридичних наук

ІНФОРМАЦІЙНА БЕЗПЕКА У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ: ПРОБЛЕМИ ПОНЯТТЯ ТА ЗМІСТУ

За сучасних умов інформація є найціннішим ресурсом, що глобальним чином впливає на потенціал розвитку держави, суспільства та людської цивілізації у цілому. Водночас, інформація є суспільним і технологічним феноменом, швидкі і почасти неконтрольовані зміни котрого призводять до зміни його якості, а, отже – до трансформації змісту. Відтак, сучасне суспільство перебуває під постійною загрозою отримання недостовірної, спотвореної інформації, маніпулювання нею, інформаційного шпигунства, комп'ютерної злочинності тощо.

Значне зростання ролі інформації в умовах ведення повномасштабної війни, розв'язаною росією проти України, а також стрімкий розвиток використання

надсучасних інформаційних технологій, включно із ШІ, суттєво впливають як на функціонування сектору безпеки та оборони у цілому, так і на функціонування Національної поліції України, зокрема. Адже непрофесійний підхід до інформатизації може не тільки перешкодити отриманню очікуваних результатів у конкретному сегменті функціонування зазначених суб'єктів, а й перетворитися на джерело серйозних загроз існуванню держави у цілому.

Аналізуючи національне законодавство у сфері інформаційної безпеки, приходимо до висновку, що у його межах наразі не визначено вимоги, заходи та способи забезпечення та гарантування інформаційної безпеки у діяльності правоохоронних органів України, зокрема, Національної поліції.

Незважаючи на те, що у розділі 4 Закону України «Про Національну поліцію» [1] визначено основні положення інформаційно-аналітичного забезпечення поліції, ні у цьому, ні у будь-якому іншому правовому акті не розкрито зміст поняття «інформаційна безпека у діяльності Національної поліції України».

Проблемні питання інформаційної безпеки діяльності правоохоронних органів розробляли О. Негодченко [2], Є Нікулін [3], Н. Моргун [4], А. Пересада [5], А. Суббот [6] та інші дослідники.

Вважаємо, що в основу вирішення проблеми визначення поняття інформаційної безпеки у діяльності Національній поліції України (НПУ) має бути покладено підхід, відповідно до якого зазначене поняття розглядається як елемент системи національної безпеки та складова інформаційної безпеки – стану захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом» [7].

Концептуальне розуміння інформаційної безпеки ґрунтується, передовсім, на його розумінні зазначеного поняття як сукупності певних проявів, що обумовлюють безпеку інформаційного простору, а саме: процесу забезпечення захищеності інформації; діяльність уповноважених суб'єктів державної влади щодо захисту інформаційного простору; стану захищеності інформації; сукупність суспільних відносин у сфері захисту інформації та напрямок державної політики [8, с. 25–30]. Виходячи із зазначеного, інформаційна безпека в умовах інформаційного суспільства розглядається як суспільно-правовий та технічний феномен, що об'єктивується в організаційній, технічній та правовій сфері, та потребує окремого напряму правового регулювання.

Важливим для формування поняття інформаційної безпеки у діяльності НПУ вважаємо виділення ключових ознак загального поняття «інформаційна безпека», які обґрунтовують Н. Моргун, О. Шевчук, С. Марчевський, а саме: а)

наявність відомостей про які-небудь події та чиюсь діяльність; б) належність таких відомостей до інтересів окремих суб'єктів; в) забезпечення уповноваженими суб'єктами захисту інформаційного простору від внутрішніх та зовнішніх загроз; г) наявність певних правовідносин, однією із сторін яких виступає держава; ґ) наявність інформаційного простору (інформаційних ресурсів, інформаційної інфраструктури; засобів інформаційної взаємодії) [4, с. 412].

Виявлені зв'язки між складовими поняття інформаційної безпеки обумовлюють можливість їх застосування до аналізу поняття «інформаційна безпека у діяльності НПУ». Так, Є.Ю. Нікулін під зазначеним поняттям розуміє такий стан внутрішніх та зовнішніх правовідносин, при якому, по-перше, забезпечується та гарантується правомірність використання уповноваженими особами органів Національної поліції інформації в межах відомчого, міжвідомчого, загальнодержавного та міжнародного інформаційного простору; по-друге, здійснюються заходи, спрямовані на своєчасне виявлення, запобігання і нейтралізацію реальних і потенційних загроз інформаційній безпеці поліції та протидію несанкціонованим діям щодо інформації у ввіреному інформаційному просторі» [3, с. 20]. Натомість, Н. Моргун, О. Шевчук, С. Марчевський розглядають інформаційну безпеку у діяльності НПУ у якості складової національної безпеки України, що виявляється у правовідносинах уповноважених суб'єктів поліції між собою та з іншими суб'єктами (людиною, суспільством, державою, юридичними особами), які спрямовані на забезпечення захисту інформаційного простору від будь-яких загроз [4, с. 213-414].

Зміст функції забезпечення інформаційної безпеки НПУ, на нашу думку, пов'язаний із функцією охорони та захисту інформації у суспільних відносинах, які мають місце у суспільстві, що обумовлює необхідність застосування поліцейськими спеціальних знань із технічних галузей, підгалузей, окремих інституцій як технічних, так і суспільних наук.

Під системою інформаційного забезпечення органів поліції Г.М. Шорохова розуміє сукупність взаємопов'язаних і взаємодіючих організаційних елементів і технічних засобів, які здійснюють інформаційне забезпечення НПУ[9, с. 266].

Забезпечення захисту інформаційного простору від будь-яких загроз відбувається органами (підрозділами) поліції під час виконання ними завдань з надання поліцейських послуг у сферах: охорони прав і свобод людини, а також інтересів суспільства і держави; забезпечення публічної безпеки і порядку; протидії злочинності; надання в межах, визначених Законом України «Про Національну поліцію», послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги.

У ст. 25 Закону України «Про Національну поліцію» [1] визначено повноваження поліції у сфері інформаційно-аналітичного забезпечення. Зокрема, визначено, що поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень у таких напрямах: 1) формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; 2) користується базами (банками) даних Міністерства

внутрішніх справ України та інших органів державної влади; 3)здійснює інформаційно-пошукову та інформаційно-аналітичну роботу; 4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями; 5) надає до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів. 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.

Однією із умов підвищення ефективності системи інформаційної безпеки функціонування НПУ у період воєнного стану в Україні є пошук принципово нових способів організації роботи з інформаційними ресурсами, стандартизація яких спрямована на створення та гармонізацію єдиного інформаційного простору сектору безпеки та оборони та, зокрема, правоохоронних органів.

Узагальнення позицій спеціалістів із проблем формування систем протистояння інформаційній небезпеці [10, 11, 12] дозволяє окреслити систему необхідних заходів, які можуть бути застосовані для захисту інформаційної безпеки діяльності НПУ у період воєнного стану, та здійснюватися комплексно, на основі нових наукових розробок і програмних продуктів. На нашу думку, комплекс таких заходів має реалізовуватися за двома основними напрямами: 1) захист інформаційних систем, що використовуються у діяльності НПУ у процесі виконання поставлених перед нею задач; 2) захист працівників поліції від шкідливого інформаційно-психологічного впливу.

Так, у межах першого із зазначених напрямів доцільним вважаємо: а) здійснення захисту об'єктів, що перебувають у розпорядженні органів НПУ, та розташованої в них комп'ютерної техніки від пошкодження або іншого навмисного виведення з ладу; б) захист інформаційних систем НПУ від кібератак, зокрема, шляхом установки відповідних систем захисту, що забезпечують повний захист периметра від вторгнень; в) захист інформації, яка становить державну, військову або службову таємницю, від несанкціонованого витоку; г) радіоелектронний захист; ґ)розробку засобів електронної розвідки; д) використання соціальних мереж для формування відповідної інформаційної політики та протистояння дезінформації противника; д) захист систем зв'язку. У межах другого із зазначених напрямів доцільним вважаємо: а) запобігання психологічного впливу на психіку працівників НПУ; б) використання всіх доступних видів психологічної роботи із поліцейськими, з подальшим їх поширенням на різні категорії населення; в) здійснення цілеспрямованих заходів інформаційно-психологічної підтримки.

Вважаємо, що зазначені заходи своїм результатом матимуть створення стійкого захисту від інформаційного впливу та готовності працівника поліції до відсікання інформації, яка має на меті дестабілізацію морально-психологічного стану та забезпечення перемоги ворога у інформаційній війні.

З огляду на зазначене, вважаємо за необхідне розробити закон «Про інформаційну безпеку правоохоронних органів України», чим закласти

нормативну базу відповідного напряму державного управління. У зазначеному контексті слушним буде виокремлення інформаційної безпеки правоохоронних органів як різновиду інформаційної безпеки, а також подальша реалізації завдання – це вироблення необхідних нормативно-правових документів, координації процесів належного використання інформації у діяльності правоохоронних органів.

Список використаних джерел

1. Про Національну поліцію: Закон України від 2 лип. 2015 р. № 580-VIII. URL:https://zakon.rada.gov.ua/laws/show/580-19#Text// (дата звернення: 29.04.2025).
2. Негодченко В.О. Інформаційна безпека в органах Національної поліції України: адміністративно-правове забезпечення. *Право і суспільство.* № 6. 2020. С. 167– 174. DOI: https://doi.org/10.32842/2078- 3736/2020.6.1.24. (дата звернення: 29.04.2025).
3. Нікулін Є.Ю. Адміністративно-правове забезпечення інформаційної безпеки Національної поліції України: дис. … канд. юрид. наук. : 12.00.07. Київ. 2021. 133 с. URL: https://uacademic.info/ua/document/0422U100087#google_vignette. (дата звернення: 29.04.2025).
4. Моргун Н.С., Шевчук О.О., Марчевський С.В. Щодо визначення поняття інформаційної безпеки у діяльності Національній поліції України. *Аналітично-порівняльне правознавство.* 2024. № 8. С. 409-415. URL: https://app-journal.in.ua/wp-content/uploads/2024/08/69.pdf. (дата звернення: 29.04.2025).
5. Пересада О.М. Роль Національної поліції України в забезпеченні інформаційної безпеки держави: теоретико-методологічні аспекти. *Правовий часопис Донбасу.* № 4 (69). 2019. С. 183–189. DOI: https:// doi.org/10.32366/2523-4269-2019-69-4- 183-189.
6. Суббот А. Інформаційна безпека діяльності працівників правоохоронних органів. *Віче.* 2014. № 22. С. 19-22. URL: http://nbuv.gov.ua/UJRN/viche_2014_22_6.
7. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text. (дата звернення: 29.04.2025).
8. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. Київ : КНТ, 2006. 280 с.
9. Шорохова Г.М. Інформаційне забезпечення діяльності територіальних органів поліції України. *Юридичний науковий електронний журнал.* 2018. № 6. С. 264–267. URL: http://www.lsej.org.ua/6_2018/73.pdf. (дата звернення: 29.04.2025).
10. Кавун С.В., Носов В.В., Манжай О.В. Інформаційна безпека. Навчальний посібник. Ч. 2. Харків: Вид. ХНЕУ, 2018. 196 с.
11. Петровський О. Проблемні питання формування єдиного інформаційного простору правоохоронних органів. *Підприємництво, господарство і право.* 2017. № 8. С. 145–148.

12. Смотрич Д., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету.* Серія ПРАВО. 2023. Випуск 77: частина 2. С.121-127. DOI https://doi.org/10.24144/2307-3322.2023.77.2.20.

Іванчук Наталія Віталіївна,
старший викладач кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук

КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ДЕРЖАВНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасне життя неможливо уявити без глибокого проникнення інформатизації в усі його сфери. Інформаційна розвиненість поступово стає однією з важливих складових, що визначають образ «сучасної людини», створюючи необхідну основу для її повноцінного існування. С кожним роком інформація набуває все більшого загальносуспільного значення, що надає особливу актуальність гуманітарним дослідженням явищ, нерозривно пов’язаних з нею.

Інформатизація сучасного суспільства передбачає проникнення інформаційних технологій практично в усі сфери суспільного життя, що надає домінуючого значення діяльності держави, пов’язаній із забезпеченням вільного обміну інформацією, інтеграцією у світове інформаційне суспільство, забезпеченням інформаційної безпеки та інші.

Однак, в умовах глобалізації інформаційного обміну і широкого впровадження інформаційних технологій в усіх сферах життєдіяльності суспільства України існує проблема захисту інформації, що обробляється в інформаційних, інформаційно-телекомунікаційних та автоматизованих системах від викликів і загроз у кібернетичному та віртуальному просторі, а також від кримінальних протиправних дій правопорушників. Тим більше, що у сучасному за інформатизованому суспільстві інформація стала не просто засобом комунікації, а й об’єктом діяльності людей, тому сьогодні її сутність вивчається багатьма галузями знань.

Забезпечення інформаційної безпеки України є однією з найважливіших функцій держави. Держава, маючи найбільші можливості впливу на суспільні відносини, потенційно є найнебезпечнішим елементом, але водночас і основним стимулятором та організатором покращення умов функціонування суспільства. Тому, основою забезпечення високого рівня інформаційної безпеки повинна стати ефективна управлінська діяльність, яку доцільно розглядати в двох аспектах: як управління технічними системами та як вплив на соціальні процеси з метою досягнення поставлених цілей. У світлі розбудови глобального інформаційного суспільства другий аспект набуває особливого значення.