persons in need of special protection by the state and / or rehabilitation.

In accordance with the characteristics of such activities should include: 1) is a type of police law enforcement activity, characterized by standardization, system, organization and professionalism; 2) is a set of active actions of authorized entities (officials and officials of police bodies) who have knowledge and skills in the field of law and special criminological knowledge; 3) is carried out by legal means and methods allowed by the legislation with use of actual criminological technologies (methods), and also scientific methods of knowledge; 4) possible forms of such activity are educational, scientific and practical, while scientific criminological activity performs a supporting function in relation to this kind of practical activity; 5) in its intellectual content can be organizational (managerial), cognitive-search, communicative; 6) its general purpose is to counteract criminal offenses (their detection, cessation, prevention, prevention), as well as related negative phenomena for society (abuse of rights, etc.), elimination of determinants of criminal offenses, identification of criminal offenses and crime, victims of criminal offenses, identification of persons in need of special protection by the state and / or rehabilitation; 7) each of the forms of such activity within the defined purpose, aimed at solving a separate task, namely: a) criminological educational activity – training of specialists with special criminological knowledge and skills; b) criminological scientific activity – the search for ways to solve current theoretical and applied criminological problems; c) criminological practical activity – reduction of the number of committed criminal offenses, elimination of their causes and conditions, taking appropriate measures against persons who are prone to committing offenses or have already committed them, as well as with regard to potential and actual victims; 8) may be carried out as an independent type of police activity, and in parallel with its other types, for example in the implementation of operational and investigative or criminal procedure activities.

Key words: *criminology, police, legal activity, police activity, criminological activity, prevention of criminal offenses.*

УДК 342.95
DOI: 10.31733/2078-3566-2020-4-15-24

Ганна БЛІНОВА©
доктор юридичних наук, доцент

Ельміра МАМЕДОВА©
ад'юнкт

(Дніпропетровський державний університет внутрішніх справ)

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ТА КІБЕРБЕЗПЕКА ПАТРУЛЬНОЇ ПОЛІЦІЇ: СПІВВІДНОШЕННЯ ПОНЯТЬ

Висвітлено наукові підходи та нормативно-правовове визначення змісту понять інформаційне забезпечення та кібербезпека патрульної поліції. Виявлено недоліки визначення термінологічного апарату у сфері інформаційного забезпечення та кібербезпеки Національної поліції загалом та патрульної поліції зокрема. Сформульовано поняття кібербезпеки патрульної поліції як стану 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. Запропоновано розробити концепцію інформаційного забезпечення патрульної поліції, яка міститиме розділ про кібербезпеку патрульної поліції.

Ключові слова: *Національна поліція України, інформаційне забезпечення, кібербезпека, патрульна поліція.*

© Блінова Г. О., 2020
https://orcid.org/0000-0002-3320-585X
BlinovaHANNA@i.ua

© Мамедова Е. А., 2020
BlinovaHANNA@i.ua

Постановка проблеми. Останнім часом Україна неодноразово стикалася з актуалізацією загроз інформаційній безпеці органів публічної влади. Серед них недавнє поширення шкідливого програмного забезпечення Petya, вимагача WannaCry, атаки 2015–2016 років на енергетичний сектор, атака на президентські вибори у 2014 році, різні інциденти, пов'язані з інформаційними системами та мережами державних органів і держкомпаній у 2016 році, інциденти, пов'язані з Євромайданом у 2013–2014 роках, а також низка профільних кіберзлочинів. Інший напрям негативного зовнішнього інформаційного впливу, що здійснюється із використанням новітніх інформаційних технологій – це зміна свідомості громадян, спрямована на розпалювання міжнаціональної та релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу або будь-яке порушення суверенітету, територіальної цілісності України, громадського порядку та безпеки. Загрози можуть бути різної природи, результатом дій різних суб'єктів, що мають великий спектр мотивів. Вони можуть бути спрямовані на багато об'єктів, мати різну величину, атакувати велике коло жертв і приносити безліч шкідливих наслідків. Відповідно, потрібен ефективний алгоритм оцінки якості кожної загрози, що визначатиме поєднання заходів і можливостей різних правоохоронних структур для протидії ним.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. Дослідженням питань інформаційного забезпечення, інформаційної безпеки та кібербезпеки суб'єктів публічної влади та правоохоронних органів опікувались такі вчені, як Є. Д. Бондаренко, В. В. Бухарев, В. О. Єльцов, Д. П. Кисленко, В. В. Лушер, Г. М. Шорохова та інші. Проте на сьогодні відсутня сучасна концепція кібербезпеки Національної поліції загалом та патрульної поліції зокрема.

Метою статті є визначення ознак, особливостей інформаційного забезпечення та кібербезпеки патрульної поліції, формулювання відповідних авторських понять. Завданнями дослідження є узагальнення наукових концепцій, що визначають зміст інформаційного забезпечення, інформаційної та кібербезпеки поліції, визначення співвідношення цих понять, виявлення шляхів їх нормативного закріплення.

Виклад основного матеріалу. Проблема реалізації кіберзагроз та негативного зовнішнього інформаційного впливу характерна не тільки для України [8]. Європейський парламент для протидії таким негативним сучасним викликам ухвалив низку документів, серед яких Резолюція «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін» [24; 11], Директива Європейського Парламенту і Ради «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» [14], Регламент Європейського парламенту і Ради «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)» [25] та інші. Зі свого боку, Україна створила такі нормативно правові документи, як стратегії, доктрини, програми, які спрямовані на визначення національних інтересів України в інформаційному просторі, ідентифікацію загроз їх реалізації, напрямів і пріоритетів державної політики в інформаційному просторі.

Документами, що місять принципи формування та реалізації державної інформаційної політики, у тому числі пов'язаних з протидією деструктивному зовнішньому інформаційному впливу, є Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та плану заходів щодо її реалізації, затверджені Розпорядженнями Кабінету Міністрів України від 20.09.2017 р. № 649-р , від 8 листопада 2017 р. № 797-р та від 17 січня 2018 р. № 67-р. [19], а також Укази Президента України від 14.09.2020 р. № 392/2020 «Про Стратегію національної безпеки України» [17]; від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [18] та інші.

Основними пріоритетами державної політики в інформаційній сфері згідно із зазначеними документами є законодавче регулювання механізму пошуку, фіксації, блокування і видалення з інформаційного простору держави, зокрема з українського сегмента мережі «Інтернет», інформації, яка загрожує життю або здоров'ю громадян України, розпалює війну, міжнаціональну і релігійну ворожнечу, пропагує зміну конституційного ладу або порушення територіальної цілісності України, загрожує державному суверенітету і просуває комуністичні і/або націонал-соціалістичні (нацистські) тоталітарні режими і їх символи, а також створення інтегрованої інформаційної системи оцінки загроз та швидкого реагування на них.

Зазначені обставини вплинули на умови функціонування правоохоронних органів.

Слід погодитись із Г. М. Шорохом, що на сьогодні важко уявити роботу будь-якого з підрозділів Національної поліції України без інформаційної підтримки та інформаційного забезпечення, накопичення та систематизації інформації в базах даних [23, с. 246]. Практика використання засобів інформаційного забезпечення працівниками поліції свідчить про складності організаційного, правового та технічного характеру, що супроводжують цей процес. Внаслідок реалізації ризиків зниження рівня інформаційного забезпечення, інформаційної безпеки та кібербезпеки підрозділів та працівників Національної поліції значно знижується їх ефективність.

Стратегія розвитку Міністерства внутрішніх справ України до 2020 року визначила, що недоліками у сфері інформаційного забезпечення підрозділів поліції є застарілі підходи до управління інформаційними ресурсами органів системи МВС, недостатній рівень використання ними інформаційно-комунікаційних технологій; відсутність системного вирішення проблеми авторизованого доступу користувачів, еталонної консолідації, перевірки актуальності і достовірності даних інформаційних ресурсів системи МВС; ступінь інтеграції в міжнародний інформаційний простір у сфері безпеки не відповідає сучасним викликам, які стоять перед системою МВС. Цією стратегією передбачено, що роль Міністерства внутрішніх справ України полягає у створенні умов розвитку безпечного середовища життєдіяльності, як основи безпеки на території України, а також сучасної системи внутрішньої безпеки. Цим документом, на нашу думку, приділяється значна увага підвищенню ефективності роботи і взаємодії підрозділів поліції через максимальне використання інформаційно-комунікаційних технологій у реалізації завдань органами системи МВС. Основними кроками для реалізації цього завдання стратегія визначає: реалізацію концепції діяльності органів системи МВС, заснованої на використанні різних джерел інформації (Intelligence Led Policing); запровадження в системі МВС механізму узгодження інформації про особу, що міститься у наявних державних та єдиних реєстрах, інших інформаційних базах, які є у власності держави або підприємств, установ та організацій та використовуються з метою проведення ідентифікації осіб, з єдиним ідентифікатором – унікальним номером запису в Єдиному державному демографічному реєстрі; об'єднання і захист відомчих інформаційних ресурсів органів системи МВС у межах єдиного інтегрованого інформаційного середовища; упровадження сучасного авторизованого доступу користувачів до інформаційних ресурсів системи МВС та надання громадянам доступу до відкритих даних органів системи МВС і власних персональних даних; підготовка належних інформаційних систем МВС до приєднання до Шенгенської інформаційної системи; розширення та оновлення знань, умінь та навичок працівників у роботі з відомчими інформаційними системами [20; 7]. Отже, питання інформаційного забезпечення та кібербезпеки Національної поліції України мають стратегічне значення для ефективної діяльності Міністерства внутрішніх справ України.

Теоретична невизначеність понять інформаційного забезпечення та кібербезпеки Національної поліції загалом і патрульної поліції зокрема є однією з причин, визначених у Стратегії розвитку Міністерства внутрішніх справ України до 2020 року, недоліків у сфері інформаційного забезпечення підрозділів поліції.

Досліджуючи різні наукові позиції щодо змісту та ознак інформаційного забезпечення органів публічної адміністрації, ми підтримуємо концепцію широкого підходу до розуміння цього поняття, що зумовлено сучасними тенденціями глобалізації та постійного прискорення розвитку електронних ресурсів. Прихильниками цього підходу є такі науковці, як Є. Д. Бондаренко, В. О. Єльцов, О. В. Костенко, В. В. Лушер та інші. За їх концепціями інформаційне забезпечення можна визначити як: 1) це процес задоволення потреб в інформації, заснованій на застосуванні спеціальних засобів і методів її одержання, опрацюванні, накопиченні і видачі в зручному для використання виді, а структура цього забезпечення містить інформаційний фонд та спеціальні прийоми і методи інформаційного забезпечення [3]; 2) являє собою сукупність організаційної діяльності з одержання, опрацювання, накопичення і видачі інформації, прийомів та методів її здійснення, а також матеріальних об'єктів – інформаційний фонд [3]; 3) сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки [6, с. 101]; 4) комплекс нормативно-правових, організаційно-управлінських, науково-

технічних та інших заходів поєднання усієї інформації, що використовується в органах прокуратури, специфічних засобів і методів її оброблення, використання, дослідження, зберігання та захисту [10, с. 340]. О. В. Костенко детальніше визначила ознаки, притаманні інформаційному забезпеченню, врахувавши його зміст, методи реалізації, мету, призначення [9, с. 116].

У попередніх працях ми визначили ознаки поняття «інформаційне забезпечення»: 1) мета – задоволення інформаційних потреб та забезпечення реалізації інформаційних прав; 2) ресурс – інформація, вид, якість, обсяг, структура, форма, строк та носії використання якої визначаються інформаційними потребами та правами суб'єкта; 3) зміст – неперервний процес, що складається з різних видів інформаційної діяльності; 4) методи – створення, використання, дослідження, зберігання, захист, передавання, обробка, знищення інформації; 5) засоби – інформаційні системи, мережі, ресурси та інформаційні технології, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки; 6) заходи щодо реалізації інформаційного забезпечення – комплекс нормативно-правових, організаційно-управлінських, науково-технічних та інших заходів; 7) суб'єкт – фізичні та юридичні особи та їх об'єднання [2, с. 18–19]. З огляду на зазначене, нами було сформульовано поняття інформаційного забезпечення органів публічної адміністрації [1, с. 30]. На наш погляд, це поняття може бути покладене в основу формулювання поняття інформаційного забезпечення Національної поліції загалом і патрульної поліції зокрема. Особливості змісту інформаційного забезпечення патрульної поліції визначатимуть її інформаційні потреби, зумовлені колом повноважень.

Згідно з Положенням про Департамент патрульної поліції, цей міжрегіональний територіальний орган Національної поліції у інформаційній сфері виконує такі функції: 1) у межах інформаційно-аналітичної діяльності патрульної поліції формує бази (банки) даних, що входять до єдиної інформаційної системи Національної поліції України та Міністерства внутрішніх справ України, користується базами (банками) даних Національної поліції України, Міністерства внутрішніх справ України та інших державних органів, здійснює інформаційно-пошукову та інформаційно-аналітичну роботу, а також обробку персональних даних у межах повноважень, визначених законом; 2) здійснює інформаційну взаємодію з іншими державними органами України, органами правопорядку іноземних держав та міжнародними організаціями [13]; 3) для забезпечення публічної безпеки та порядку, попередження, виявлення або фіксування правопорушення, охорони власності, забезпечення безпеки осіб, а також забезпечення дотримання правил дорожнього руху застосовує технічні прилади та технічні засоби, що мають функції фото та кінозйомки, відеозапису, чи засоби фото- і кінозйомки, відеозапису; 4) інформує в порядку та у спосіб, які передбачені законодавством, органи державної влади, органи місцевого самоврядування, а також громадськість про здійснення державної політики у сферах забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, безпеки дорожнього руху; 5) керівництво департаменту здійснює постійний контроль за збереженням інформації з обмеженим доступом, збереженням державної таємниці та дотриманням режиму секретності в Департаменті патрульної поліції. На наш погляд, визначені у цьому наказі засади інформаційного забезпечення та кібербезпеки патрульної поліції є неповними, їх слід сприймати із врахуванням норм Закону України «Про Національну поліції» [15], що ґрунтовніше визначають елементи механізму інформаційного забезпечення підрозділів Національної поліції та поширюються на патрульну поліцію. Визначені у цих нормативно-правових актах повноваження та функції патрульної поліції зумовлюють пов'язані із ними службові інтереси.

Зважаючи на зазначене, підтримуємо позицію Г. М. Шорохової, який інформаційне забезпечення органів поліції визначає як комплекс методів, заходів, засобів різного характеру, які забезпечують створення та функціонування інформаційних технологій, а також їх ефективне використання для вирішення покладених на поліцію завдань [23, с. 274–278].

З інформаційним забезпеченням патрульної поліції тісно пов'язані питання кібербезпеки, причому найчастіше науковці досліджують повноваження Національної поліції як суб'єкта забезпечення кібербезпеки держави, суспільства, різних спільнот та окремих громадян. Зокрема, в галузі забезпечення кібербезпеки, вважає В. В. Бухарев, Національна поліція України наділена повноваженнями щодо забезпечення прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення

поінформованості громадян про безпеку в кіберпросторі [15]. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», МВС було включено до національної системи суб'єктів забезпечення кібербезпеки, через що на МВС було покладено повноваження щодо: створення і забезпечення функціонування підрозділів з протидії кіберзлочинності; розробки та реалізації комплексу організаційних і практичних заходів, спрямованих на боротьбу з кіберзлочинами; створення і забезпечення функціонування цілодобової контактної мережі для надання невідкладної допомоги у розслідуванні кіберзлочинів тощо [15]. В положеннях Закону «Про основи забезпечення кібербезпеки України» МВС віднесено до загальних суб'єктів забезпечення інституту [4]. Водночас науковці не достатньо приділяють уваги визначенню змісту поняття кібербезпека поліції, якого на сьогодні не сформульовано.

Відсутність достатньої уваги до питань організаційно-правового забезпечення кібербезпеки патрульної поліції призводить до реалізації загроз у цій сфері. Одна з останніх таких кібератак сталася 23 вересня 2020 року, коли на деяких інтернет-сторінках обласних управлінь Національної поліції була поширена неправдива інформація, повідомлялося про викид радіоактивних речовин на 3-му енергоблоці Рівненської АЕС [12]. На той момент сайт Національної поліції та відповідно інтернет-сайти інших головних управлінь поліції були відключені. Департамент патрульної поліції був змушений відключити базу ІІПС «Армор», що не давало змоги патрульним поліцейським здійснювати перевірку осіб, транспортних засобів, також виносити електронні постанови правопорушникам. На той момент виклики на спеціальну лінію «102» приймалися і передавалися до чергової частини, своєю чергою, чергова частина патрульної поліції також виявилася без зв'язку. Не бачивши на моніторі карти знаходження патрулів, черговий був змушений відправляти будь-який й орієнтуватися тільки на квадрат прив'язки патруля, в якому екіпаж не завжди знаходився. Виклики спецлінії «102» оголошувалися по радіозв'язку, який, як ми знаємо, не є захищеним, також в телефонному режимі. Черговий не бачив рапорту про виконану роботу на виклик і час завершення виклику, щоб направити екіпаж за наступною адресою. Це призвело до черги необслуговуваних викликів, громадяни не отримали ту допомогу, якої потребували в ту хвилину.

Закон України «Про основні засади забезпечення кібербезпеки України» дає таке визначення кібербезпеки: це є захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [16]. Кібербезпеку як об'єкт адміністративно-правової охорони В. В. Бухарев визначає як певний правовий інститут, охорона якого відбувається в межах норм адміністративного права та здійснюється окремими державними органами на засадах імперативності та ієрархічності. Цей науковець визначає такі особливості кібербезпеки як об'єкта адміністративно-правової охорони: а) відсутність чіткого визначення змісту адміністративно-правової охорони кібербезпеки; б) адміністративно-правова охорона кібербезпеки хоча і являє собою єдиний юридичний інститут, проте закріплюється у нормах різних нормативно-правових актів, якими регулюється діяльність відповідних органів державної влади; в) її забезпечення здійснюється не тільки у правовідносинах, які виникають у сфері вчинення адміністративних правопорушень. Інститут має більш широкий обсяг застосування, який передбачає не тільки припинення відповідних порушень, а також їх попередження; г) основні засади забезпечення кібербезпеки лише нещодавно знайшли своє закріплення у відповідному нормативно-правовому акті – Законі України «Про основні засади забезпечення кібербезпеки України»; ґ) має місце спеціальний понятійний апарат [4, с. 94]. Науковий стан вивчення змісту поняття кібербезпека патрульної поліції не дозволяє дослідити сформульовані відповідні поняття через їх відсутність. Водночас поняття кібербезпеки тісно пов'язано із поняттям інформаційної безпеки, оскільки є похідним від останнього.

У наших попередніх працях було сформульовано поняття інформаційної безпеки органів внутрішніх справ України як такий стан захищеності службових інтересів, за якого зводиться до мінімуму заподіяння шкоди та створення перешкод у діяльності органів внутрішніх справ через неповноту, несвоєчасність, недостовірність інформації, що використовується, або протиправний інформаційний вплив, недоліки функціонування інформаційних систем, мереж, технологій, а також через порушення режиму службової таємниці [21, с. 15]. Було також визначено основні елементами інформаційної безпеки

ОВС [22, с. 69]. Отже, кібербезпеку патрульної поліції можна розглядати як безпеку служби, кібербезпеку Департаменту патрульної поліції – як кібербезпеку установи, а кібербезпеку патрульного поліцейського – як вид кібербезпеки людини.

Інші науковці, наприклад В. А. Веклич та Д. П. Кисленко, визначили інформаційну безпеку поліції охорони як захист інформаційної сфери поліції охорони від внутрішніх та зовнішніх загроз. На їх думку, інформаційна безпека поліції охорони полягає у спроможності працівників поліції охорони убезпечити інформаційні ресурси від несанкціонованого доступу до них, та унеможливити витоки службової інформації. Забезпечення інформаційної безпеки в діяльності поліції охорони здійснюється через: організаційно-аналітичне управління; управління технічної охорони; відділ правового забезпечення; режимно-секретний сектор Департаменту поліції охорони – структурні служби Департаменту поліції охорони, які забезпечують правове та організаційно-технічне забезпечення інформаційної безпеки в діяльності поліції охорони. Поліція охорони Національної поліції України, зазначають В. А. Веклич та Д. П. Кисленко, є складовою частиною системи інформаційної безпеки. Забезпечення інформаційної безпеки поліції охорони здійснюється відповідно до встановлених законом повноважень та спрямоване на своєчасне виявлення, запобігання та припинення загроз в її інформаційному просторі [5, с. 59].

Сьогоднішні системи управління документами, в тому числі використовувані патрульною поліцією, являють собою майже всі комп'ютерні цифрові файли. Сервіс «102» заснований на інтернет-протоколі і дозволяє обмінюватися текстовими повідомленнями, а також фотографіями і відео. Автоматизовані диспетчерські системи також є різновидом цифрових технологій. У цьому постійно мінливому світі захист інформації правоохоронних органів вимагає набагато більшого, ніж просто фізична безпека. Керівники поліції повинні дуже серйозно ставитися до кібербезпеки і усвідомлювати потенційну загрозу надання послуг громадської безпеки.

Отже, ми робимо висновки, що патрульна поліція повинна не відставати від технологічного розвитку і мати необхідні знання та навички для боротьби з цифровою злочинністю, що зростає, на національному, регіональному та міжнародному рівнях. Вирішення проблеми інформаційного супроводження, а саме налагодження комунікації між поліцейськими, поліпшення радіозв'язку, мобільного устаткування, забезпечення кібербезпеки патрульної поліції повинно стати пріоритетами державної політики у сфері інформаційного забезпечення правоохоронних органів України. Удосконалення законодавчого регулювання механізму пошуку, фіксації, блокування і видалення з інформаційного простору держави, зокрема з українського сегмента мережі «Інтернет», інформації, яка загрожує життю або здоров'ю громадян України, розпалює війну, міжнаціональну і релігійну ворожнечу, загрожує державному суверенітету і просуває комуністичні і або націонал-соціалістичні (нацистські) тоталітарні режими і їх символи, сприятиме також створенню в патрульній поліції України інтегрованої інформаційної системи оцінки загроз та швидкого реагування на них.

Висновки. Зважаючи на зазначені вище визначення та ознаки інформаційного забезпечення, вважаємо за можливе визначити такі ознаки інформаційного забезпечення патрульної поліції: 1) цілі – задоволення інформаційних потреб патрульної поліції, забезпечення реалізації інформаційних прав поліцейських, ефективне інформаційне забезпечення функціонування патрульної поліції; 2) ресурс – інформація, вид, якість, обсяг, структура, форма, строк та носії використання якої визначаються інформаційними потребами та правами патрульної поліції; 3) зміст – неперервний процес, що складається з різних видів інформаційної діяльності працівників патрульної поліції; 4) методи – створення, використання, дослідження, зберігання, захист, передавання, обробка, знищення інформації; 5) засоби – інформаційні системи, мережі, ресурси та інформаційні технології, які використовуються в системі МВС України; 6) заходи із реалізації інформаційного забезпечення – комплекс нормативно-правових, організаційно-управлінських, науково-технічних та інших заходів; 7) суб'єкт – патрульна поліція України.

Отже, інформаційне забезпечення патрульної поліції можна визначити як забезпечений комплексом нормативно-правових, організаційно-управлінських, науково-технічних заходів неперервний процес створення, використання, дослідження, зберігання, захисту, передавання, обробки, знищення інформації визначеного виду, якості, обсягу, структури, форми за допомогою інформаційних систем, засобів, мереж, ресурсів та технологій, що використовуються в системі МВС України, спрямований на задоволення

інформаційних потреб та реалізацію інформаційних інтересів патрульної поліції.

Ознаками кібербезпеки патрульної поліції є: 1) це стан захищеності службових інтересів патрульної поліції; 2) досягається шляхом дотримання правових, організаційних технічних вимог з використання інформаційних ресурсів, мереж, носіїв інформації, програмного забезпечення, засобів фото- та відеозйомки в роботі патрульних поліцейських; 3) забезпечується спеціальними підрозділами патрульної поліції та кожним патрульним поліцейським в межах своїх функціональних обов'язків та обсягу спеціальних знань; 4) проявляється у сфері кіберпростору; 5) мета – своєчасне виявлення, запобігання і нейтралізація реальних і потенційних кіберзагроз.

Тому кібербезпеку патрульної поліції можна визначити 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.

У зв'язку із пришвидшенням процесів інформаційно-технічного удосконалення роботи патрульної поліції та збільшенням ризиків негативного впливу на функціонування її системи інформаційного забезпечення вважаємо за необхідне розробити концепцію інформаційного забезпечення патрульної поліції, що буде містити запропоновані визначення та в окремий розділ про кібербезпеку патрульної поліції. Також для підвищення рівня кібербезпеки патрульної поліції пропонуємо посилити співпрацю з кіберполіцією, розробити відповідні методичні рекомендації, запровадити тренінги з питань правового забезпечення та ефективного використання баз даних, інформаційних систем, мереж, програмного забезпечення, засобів відео- та фотозйомки в роботі патрульних поліцейських.

Список використаних джерел

1. Блінова Г. О. Інформаційне забезпечення органів публічної адміністрації в Україні: адміністративно-правові засади : монографія. Запоріжжя : Видавничий дім «Гельветика», 2019. 495 с.

2. Блинова А. А. Понятие и содержание информационного обеспечения органов публічной администрации. Legea si Viata. 2018. № 12. С. 17–21.

3. Бондаренко Є. Д. Особливості інформаційного забезпечення торгівельного підприємства. *Актуальні проблеми сучасної науки* : матеріали V Всеукр. наук.-практ. інтернет-конф. URL: http://intkonf.org/ bondarenko-ed.

4. Бухарев В. В. Адміністративно-правові засади забезпечення кібербезпеки України : дис. … канд. юрид наук. Суми, 2018. 221 с. URL: https://core.ac.uk/download/pdf/324216462.pdf

5. Веклич В. А., Кисленко Д. П. Інформаційна безпека майбутніх фахівців поліції охорони. *Наукові записки Центральноукраїнського державного педагогічного університету імені Володимира Винниченка. Серія : Педагогічні науки.* 2017. Вип. 159. С. 57–61. URL: http://nbuv.gov.ua/UJRN/Nz_p_2017_159_10.

6. Єльцов В. О. Щодо удосконалення інформаційного забезпечення судової діяльності. *Право і безпека*. 2010. № 5. С. 99–103.

7. Інформаційні бази даних для поліції превентивної діяльності як складова інтегрованої системи управління ризиками у сфері публічної безпеки та цивільного захисту : метод. рекомендації. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2020. С. 4–5.

8. Кібератака вірусу Petya: що відомо. URL: https://www.dw.com/uk /a-39452258.

9. Костенко М. Ю. Правовые проблемы налоговой тайны : дис. ... канд. юрид. наук. Москва, 2002.

10. Лушер В. В. Поняття інформаційного забезпечення органів прокуратури України. *Форум права*. 2014. № 1. С. 338–341. URL: http://nbuv.gov.ua/UJRN/FP_index.

11. Міжнародний досвід протидії гібридним загрозам: законодавче регулювання та організації з питань стратегічних комунікацій : інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України. URL: http://euinfocenter.rada.gov.ua/uploads/documents/29377.pdf.

12. На сайтах поліції хакери опублікували фейки про загибель американських військових та викид радіації (оновлено). URL: https://lb.ua/society/2020/09/23/466595_saytah_politsii_hakeri.html.

13. Про затвердження Положення про Департамент патрульної поліції : Наказ МВС №73 від 06.11.2015 р.

14. Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу : Директива Європейського Парламенту і Ради від 6 липня 2016 року № 2016/1148. Офіційний вісник Європейського Союзу від 19.07.2016 р. – 2016 р., / L 194 /, с. 1.

15. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40–41. С. 1970. Ст. 379.

16. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. *Голос України*. 2017. № 208.

17. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14 вересня 2020 року № 392/2020. *Урядовий кур'єр.* 2020. № 179.

18. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 року № 96/2016. *Урядовий кур'єр*. 2016. № 52.

19. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р. *Урядовий кур'єр*. 2018. № 88.

20. Про схвалення Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року : Розпорядження Кабінету Міністрів України від 15 листопада 2017 р. № 1023-р. *Урядовий кур'єр*. № 48.

21. Шлома Г. О. Адміністративно-правове забезпечення службової таємниці в органах внутрішніх справ України : автореф. дис. ... канд. юрид. наук : 12.00.07. Дніпропетр. держ. ун-т внутр. справ. Дніпропетровськ, 2008. 20 с.

22. Шлома Г. О. Адміністративно-правове забезпечення службової таємниці в органах внутрішніх справ України: дис. ... канд. юрид. наук : 12.00.07. Дніпропетр. держ. ун-т внутр. справ. Дніпропетровськ, 2008. 286 с.

23. Шорохова Г. М. Використання інформаційних технологій в діяльності Національної поліції України. *Економіко-правові виклики 2017 року* : матеріали VIII Міжнарод. наук.-практ. конф. НАНР (14 січня 2017 року). Львів : НАНР-Національна академія наукового розвитку, 2017. Т. 2. 296 с.

24. Action Plan on Strategic Communication. URL : http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf.

25. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http:.eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ENм.

Надійшла до редакції 14.12.2020

References

1. Blinova H. O. Informatsiine zabezpechennia orhaniv publichnoi administratsii v Ukraini: administratyvno-pravovi zasady [Information support of public administration bodies in Ukraine: administrative and legal bases] : monohrafiia. Zaporizhzhia: Vydavnychyi dim «Helvetyka», 2019. 495 s. [in Ukr.].

2. Blinova A. A. Ponyatie i soderzhanie informacionnogo obespecheniya organov publichnoj administracii [The concept and content of information support for public administration bodies]. Legea si Viata . 2018. № 12. S. 17–21. [in Rus.].

3. Bondarenko Ye. D. Osoblyvosti informatsiinoho zabezpechennia torhivelnoho pidpryiemstva. [Features of information support of the trade enterprise.]. Aktualni problemy suchasnoi nauky : materialy V Vseukr. nauk.-prakt. internet-konf. URL: http://intkonf.org/ bondarenko-ed. [in Ukr.].

4. Bukharev V. V. Administratyvno-pravovi zasady zabezpechennia kiberbezpeky Ukrainy [Administrative and legal bases of cyber security of Ukraine] : dys. … kand. Yuryd. nauk. Sumy. 2018. 221 s. URL: https://core.ac.uk/download/pdf/324216462.pdf [in Ukr.].

5. Veklych V. A., Kyslenko D. P. Informatsiina bezpeka maibutnikh fakhivtsiv politsii okhorony [Information security of future security police specialists]. Naukovi zapysky [Tsentralnoukrainskoho derzhavnoho pedahohichnoho universytetu imeni Volodymyra Vynnychenka]. Ser. : Pedahohichni nauky. 2017. Vyp. 159. S. 57–61. URL: http://nbuv.gov.ua/UJRN/Nz_p_2017_159_10 [in Ukr.].

6. Ieltsov V. O. Shchodo udoskonalennia informatsiinoho zabezpechennia sudovoi diialnosti [Regarding the improvement of information support of judicial activity]. Pravo i bezpeka. 2010. № 5. S. 99–103. [in Ukr.].

7. Informatsiini bazy danykh dlia politsii preventyvnoi diialnosti yak skladova intehrovanoi systemy upravlinnia ryzykamy u sferi publichnoi bezpeky ta tsyvilnoho zakhystu [Information databases for the police of preventive activities as a component of the integrated risk management system in the field of public safety and civil protection]: metod. rekomendatsii. Dnipro : Dniprop. derzh. un-t vnutr. sprav, 2020. 111 s. S. 4–5. [in Ukr.].

8. Kiberataka virusu Petya: shcho vidomo [Petya virus cyberattack: what is known]. URL: https://www.dw.com/uk /a-39452258 [in Ukr.].

9. Kostenko M.Iu. Pravovыe problemы nalohovoi tainы [Legal issues of tax secrecy]: dys. ... kand. yuryd. nauk. Moskva, 2002. [in Rus.].

10. Lusher V. V. Poniattia informatsiinoho zabezpechennia orhaniv prokuratury Ukrainy [The

concept of information support of the prosecutor's office of Ukraine]. Forum prava. 2014. № 1. S. 338–341. URL: http://nbuv.gov.ua/UJRN/FP_index. [in Ukr.].

11. Mizhnarodnyi dosvid protydii hibrydnym zahrozam : zakonodavche rehuliuvannia ta orhanizatsii z pytan stratehichnykh komunikatsii [International experience in combating hybrid threats: legislation and organizations on strategic communications]: informatsiina dovidka pidhotovlena Yevropeiskym informatsiino-doslidnytskym tsentrom na zapyt narodnoho deputata Ukrainy. URL: http://euinfocenter.rada.gov.ua/uploads/documents/29377.pdf [in Ukr.].

12. Na saitakh politsii khakery opublikuvaly feiky pro zahybel amerykanskykh viiskovykh ta vykyd radiatsii (onovleno) [Hackers post fake US military deaths and radiation emissions on police websites (updated)]. URL: https://lb.ua/society/2020/09/23/466595_saytah_politsii_hakeri.html [in Ukr.].

13. Pro zatverdzhennia Polozhennia pro Departament patrulnoi politsii [On approval of the Regulations on the Patrol Police Department] : Nakaz MVS №73 vid 06.11.2015. [in Ukr.].

14. Pro zakhody dlia vysokoho spilnoho rivnia bezpeky merezhevykh ta informatsiinykh system na terytorii Soiuzu [On measures for a high common level of security of network and information systems in the Union] : Dyrektyva Yevropeiskoho Parlamentu i Rady vid 6 lypnia 2016 roku № 2016/1148. Ofitsiinyi visnyk Yevropeiskoho Soiuzu vid 19.07.2016 — 2016 r., / L 194 /, s. 1[in Ukr.].

15. Pro Natsionalnu politsiiu [About the National Police] : Zakon Ukrainy vid 02.07.2015 r. № 580-VIII. Vidomosti Verkhovnoi Rady Ukrainy. 2015. № 40-41. S. 1970. St. 379. [in Ukr.].

16. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of cybersecurity in Ukraine] : Zakon Ukrainy vid 5 zhovtnia 2017 roku № 2163-VIII. Holos Ukrainy vid 09.11.2017. № 208. [in Ukr.].

17. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku «Pro Stratehiiu natsionalnoi bezpeky Ukrainy» [On the decision of the National Security and Defense Council of Ukraine of September 14, 2020 "On the National Security Strategy of Ukraine"] : Ukaz Prezydenta Ukrainy vid 14 veresnia 2020 roku № 392/2020. Uriadovyi kurier vid 16.09.2020. № 179. [in Ukr.].

18. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku «Pro Stratehiiu kiberbezpeky Ukrainy» [On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cyber Security Strategy of Ukraine"] : Ukaz Prezydenta Ukrainy vid 15 bereznia 2016 roku № 96/2016. Uriadovyi kurier vid 18.03.2016. № 52. [in Ukr.].

19. Pro skhvalennia Kontseptsii rozvytku tsyfrovoi ekonomiky ta suspilstva Ukrainy na 2018–2020 roky ta zatverdzhennia planu zakhodiv shchodo yii realizatsii [On approval of the Concept of development of the digital economy and society of Ukraine for 2018-2020 and approval of the action plan for its implementation] : Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 17.01.2018 r. № 67-r. Uriadovyi kurier. 2018. № 88. [in Ukr.].

20. Pro skhvalennia Stratehii rozvytku orhaniv systemy Ministerstva vnutrishnikh sprav na period do 2020 roku [About approval of the Strategy of development of bodies of system of the Ministry of Internal Affairs for the period till 2020] : Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 15 lystopada 2017 r. № 1023-r. Uriadovyi kurier vid 13.03.2018 — № 48. [in Ukr.].

21. Shloma H. O. Administratyvno-pravove zabezpechennia sluzhbovoi taiemnytsi v orhanakh vnutrishnikh sprav Ukrainy [Administrative and legal support of official secrecy in the internal affairs bodies of Ukraine] : avtoref. dys. ... kand. yuryd. nauk: 12.00.07. Dnipropetr. derzh. un-t vnutr. sprav. Dnipropetrovsk, 2008. 20 s. S. 15. [in Ukr.].

22. Shloma H. O. Administratyvno-pravove zabezpechennia sluzhbovoi taiemnytsi v orhanakh vnutrishnikh sprav Ukrainy [Administrative and legal support of official secrecy in the internal affairs bodies of Ukraine] : dys. ... kand. yuryd. nauk: 12.00.07. Dnipropetr. derzh. un-t vnutr. sprav. Dnipropetrovsk, 2008. 286 s. S. 69. [in Ukr.].

23. Shorokhova H. M. Vykorystannia informatsiinykh tekhnolohii v diialnosti Natsionalnoi politsii Ukrainy [Use of information technologies in the activity of the National Police of Ukraine]. NANR Ekonomiko-pravovi vyklyky 2017 roku : materialy VIII Mizhnarod. Nauk.-prakt. konf. NANR (14 sichnia 2017 roku). Lviv: NANR-Natsionalna akademiia naukovoho rozvytku, 2017. T. 2 296 s. S. 274–278. [in Ukr.].

24. Action Plan on Strategic Communication. URL: http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf [in Eng.].

25. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http:.eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ENм [in Eng.].

SUMMARY

Hanna O. Blinova, Elmira A. Mamedova. Information support and cyber security patrol police: the relationship between concepts.The article is devoted to the coverage of scientific approaches and normative-legal definition of the content of the concepts of information support and cybersecurity of the patrol police. The shortcomings of the definition of the terminological apparatus in the field of information support and cybersecurity of the National Police in general and the patrol police in particular were revealed. The concept of cybersecurity of patrol police as a state of protection of official interests of patrol police in cyberspace, which is achieved by complying with legal, organizational, technical require-

ments for the use of information resources, networks, software, media, photo and video in the work of patrol police for effective information support for the functioning of the patrol police, timely detection, prevention and neutralization of real and potential cyber threats. Information support of the patrol police is defined as a continuous process of creation, use, research, storage, protection, transmission, processing, destruction of information of a certain type, quality, volume, structure, form, provided by a set of normative-legal, organizational-administrative, scientific and technical measures. using information systems, tools, networks, resources and technologies used in the system of the Ministry of Internal Affairs of Ukraine, aimed at meeting the information needs and realization of the information interests of the patrol police. In order to accelerate the process of information and technical improvement of the patrol police and increase the risks of negative impact on the functioning of its information support system, it is proposed to develop a concept of information support of the patrol police, which will contain appropriate definitions and include a separate section on cyber security Among the organizational measures to increase the level of cybersecurity of the patrol police, it is proposed to strengthen cooperation with cyberpolice, develop appropriate guidelines, introduce training on legal support and effective use of databases, information systems, networks, software, video and photography in patrol police.

Keywords: *National Police of Ukraine, information support, cybersecurity, patrol police.*

УДК 351.74 + 342.95
DOI: 10.31733/2078-3566-2020-4-24-29

Олександр КОБЗАР©
доктор юридичних наук, професор
(Національна академія Національної гвардії України)

Сергій ТКАЧЕНКО©
ад'юнкт
(Дніпропетровський державний університет внутрішніх справ)

МІЖНАРОДНИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ ДОТРИМАННЯ ДИСЦИПЛІНИ І ЗАКОННОСТІ В ОРГАНАХ ПРАВОПОРЯДКУ

Проаналізовано міжнародний досвід функціонування органів та інституцій, що забезпечують дотримання дисципліни і законності в органах правопорядку, порівняно відповідні структури із функціонуванням інспекцій з особового складу департаменту кадрового забезпечення Національної поліції України та запропоновано шляхи оптимізації їх роботи.

Від належного функціонування правоохоронних органів, насамперед, залежить рівень прав і свобод людини і громадянина в кожній державі, де вони існують. Міжнародний досвід відповідних процесів характеризується різними особливостями, що визначають сутність та значення дисципліни та законності у діяльності правоохоронних органів.

Ключові слова*: поліція, інспекція, службове розслідування, дисципліна, законність, забезпечення прав людини, особовий склад, досвід.*

Постановка проблеми. Забезпечення прав та свобод людини і громадянина є пріоритетним напрямом у державному будівництві. Питання їх забезпечення перебуває у тісному взаємному зв'язку із функціонуванням відповідних державних інституцій. Зі свого боку, питання організації умов, в яких дотримання прав і свобод людини і громадянина для державних службовців різних категорій стане нормою – є запорукою функціонування будь-якої галузі державного управління. Система поліції в будь-якій державі функціонує на засадах верховенства права та дотримання прав людини, що підкріплюється зокрема й діяльністю внутрішньовідомчих інституцій, діяльність яких полягає у

© Кобзар О. Ф., 2020
ORCID iD: https://orcid.org/0000-0002-5422-235X
kaf_forever@i.ua
© Ткаченко С. Є., 2020
kaf_forever@i.ua