УДК 342.951(477) DOI: https://doi.org/10.32631/pb.2020.4.04

ІРИНА ДМИТРІВНА КАЗАНЧУК,
кандидат юридичних наук, доцент,
Харківський національний університет внутрішніх справ;
https://orcid.org/0000-0003-4269-2749,
e-mail: irinakazanchuk@gmail.com;

ВАЛЕНТИНА ПЕТРІВНА ЯЦЕНКО,
кандидат юридичних наук, доцент,
Харківський національний університет внутрішніх справ;
https://orcid.org/0000-0002-2038-1467

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Визначено й охарактеризовано зміст і складові інформаційної безпеки в Україні. Проаналізовано сучасн
ий стан правового регулювання організації та діяльності підрозділів кіберполіції Національної поліції України. Звернено увагу на певні недоліки українського законодавства у сфері забезпечення поліцією інформаційної безпеки в сучасних умовах. З урахуванням специфіки завдань та функцій кіберполіції надано пропозиції щодо вдосконалення їх структури та напрямків діяльності в інформаційній сфері.

Ключові слова: *інформаційна безпека, правове регулювання, Національна поліція України, підрозділи кіберполіції, протидія, інформаційна сфера.*

Оригінальна стаття

Постановка проблеми

У ст. 2 Закону України «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII вказано на пріоритетність реалізації державної політики у сферах національної безпеки та оборони України у напрямку забезпечення державної, зовнішньополітичної, інформаційної безпеки, кібербезпеки України тощо[1]. Проте, незважаючи на поетапну інтеграцію України до міжнародної інформаційної правової системи, на сучасному етапі нагальним є виконання завдань щодо належного забезпечення інформаційної безпеки, визнаної важливою складовою національної безпеки. Особлива увага до інформаційної безпеки обумовлюється не лише зростанням кількості викликів і загроз національним інтересам та інформаційно-психологічною війною проти Української держави, але й наявністю великої кількості порушень прав громадян, що вчиняються в інформаційному просторі.

У цьому контексті соціально-політичні події, що відбувалися та досі відбуваються в житті української та світової спільноти, обумовили перезавантаження правового статусу правоохоронних органів, насамперед органів Національної поліції України, у сфері забезпечення інформаційної безпеки, вдосконалення правового регулювання їх діяльності щодо захисту інтересів суспільства і держави в інформаційній сфері, забезпечення інформаційних прав, свобод та інтересів кожної людини. Так, за оперативними даними Департаменту кіберполіції Національної поліції, щороку кількість виявлених кіберзлочинів та правопорушень в інформаційному просторі збільшується в середньому на 2,5 тис. У кількісному вимірі перше місце посідає кібершахрайство, коли шахраї шляхом обману заволодівають інформацією про банківські картки. Це також кардинг – крадіжка даних банківської карти й отримання доступу до інтернет-банкінгу жертви. На другому місці – протиправний контент. Ідеться про захист інтелектуальної власності та боротьбу з поширенням дитячої порнографії. І на третьому місці – поширення шкідливого програмного забезпечення і створення майданчиків для продажу викраденої інформації[2].

[1] Про національну безпеку України : Закон України від 21.06.2018 № 2496-VIII // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 01.12.2020).

[2] Сергій Демедюк: Перше місце серед кіберзлочинів посідає кібершахрайство // Єдиний портал органів системи МВС України : офіц. сайт.

У 2019 р. в умовах пандемії коронавірусу у світі головною метою кібершахраїв стали пересічні користувачі Інтернету, а вже потім індустрії та державні установи. Зокрема, від початку карантину в Україні правоохоронці перевірили 344 повідомлення про можливі протиправні дії, насамперед онлайн-шахрайство під час купівлі засобів індивідуального захисту, та виявили 228 фактів розміщення на інформаційних ресурсах неправдивої або провокаційної інформації (фейків) про пандемію коронавірусу[1].

Отже, недостатня розробленість на теоретичному рівні окремих питань стосовно забезпечення інформаційної безпеки, наявність практичних правових питань, з якими стикаються підрозділи Національної поліції у своїй діяльності у сфері протидії загрозам і викликам в інформаційному просторі, та недосконаліть правового регулювання поліцейської діяльності поліції у сфері забезпечення інформаційної безпеки обумовили актуальність цієї тематики.

Стан дослідження проблеми

Зауважимо, що окремим аспектам правового регулювання відносин у сфері реалізації державної інформаційної політики присвячено праці багатьох учених, а саме І. В. Арістової, О. М. Бандурки, А. І. Берлача, І. Л. Бачило, К. І. Бєлякова, В. М. Богуша, Н. І. Ковальової, Т. О. Коломоєць, В. О. Копилова, Б. А. Кормича, І. Ю. Крегула, В. А. Ліпкана, М. В. Різака, Т. Ю. Ткачука, А. Фердросса, Ч. Хайда, В. В. Шамрая, Д. В. Шпенова, Х. П. Ярмакі та ін. Проте у більшості наукових праць із цього питання досліджуються окремі проблеми сутності інформаційної безпеки держави крізь призму забезпечення національної безпеки держави. Наразі в контексті реформування української правоохоронної системи практично відсутні комплексні наукові дослідження, присвячені визначенню особливостей правового регулювання діяльності Національної поліції у сфері забезпечення інформаційної безпеки. Особливо це важливо в умовах розвитку процесу інтеграції України у європейський інформаційний простір.

Мета і завдання дослідження

Ураховуючи викладене, *метою* статті обрано аналіз наявних наукових підходів, адміністративного законодавства України і практики його реалізації щодо визначення сутності інформаційної безпеки, особливостей правового регулювання діяльності органів (підрозділів) Національної поліції України у сфері забезпечення інформаційної безпеки та шляхів його вдосконалення в сучасних умовах розвитку Української держави.

Відповідно до поставленої мети у статті планується вирішити такі *завдання:* визначити особливості правового регулювання діяльності органів (підрозділів) Національної поліції України у сфері забезпечення інформаційної безпеки, охарактеризувати місце поліції в системі суб'єктів забезпечення інформаційної безпеки України, а також запропонувати шляхи вдосконалення діяльності поліції у розглядуваній сфері в умовах зростання інформаційних викликів та кіберзагроз у суспільстві.

Наукова новизна дослідження визначається тим, що в умовах сьогодення в українській науці практично відсутні ґрунтовні дослідження теоретико-правових і прикладних аспектів правового регулювання діяльності органів (підрозділів) Національної поліції України у сфері забезпечення інформаційної безпеки в Україні.

Виклад основного матеріалу

Більшість науковців відзначає, що категорія «інформаційна безпека» охоплює різнопланові явища, а тому під час її вивчення необхідно звертати увагу на ті інформаційні сфери, в яких найбільше виявляється державний вплив, а саме захист національного інформаційного ринку, недопущення інформаційної війни, захист інформації з обмеженим доступом тощо [1, с. 15]. Інформаційна безпека є складовою загальної проблеми інформаційного забезпечення розвитку людини, держави і суспільства. Вона орієнтується на захист важливих об'єктів інформаційних ресурсів і законних інтересів. Тому Б. А. Кормич слушно розділяє інформаційну безпеку на міжнародну, національну, безпеку підприємств та безпеку особистості в інформаційній сфері. Отже, управління інформаційною безпекою здійснюється на кожному з рівнів: на міжнародному, національному, на рівні підприємства та особи, що ще раз свідчить про широкі масштаби інформатизації сучасного світу [2, с. 85].

На законодавчому рівні інформаційна безпека розглядається як складова національної

15.01.2018. URL: https://mvs.gov.ua/ua/news/11683_Sergiy_Demedyuk_Pershe_misce_sered_kiberzlochiniv_posida_kibershahraystvo_FOTO.htm (дата звернення: 01.12.2020).

[1] Шостак А. Чи існує в Україні інформаційна безпека? / UPLAN : сайт. URL: https://uplan.org.ua/analytics/chy-isnuie-v-ukraini-informatsiina-bezpeka/ (дата звернення: 01.12.2020).

безпеки, а отже, визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається заподіяння шкоди через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив, негативні наслідки застосування інформаційних технологій, несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації[1]. Відповідно, забезпечення інформаційної безпеки поряд із захистом суверенітету і територіальної цілісності визнається найважливішою функцією держави [3, с. 104] і справою всього українського народу.

Варто наголосити, що інформаційна безпека у сучасних умовах – це не лише забезпечення безпеки інформації, яка міститься чи зберігається на електронних носіях, серверах чи персональних пристроях. Це також раціональна інформаційна політика на рівні держави та підприємства, що не обмежує законних прав людини і громадянина на доступ до інформації й, у свою чергу, регулює інформаційні відносини.

Отже, поняття інформаційної безпеки охоплює, з одного боку, забезпечення якісного інформування громадян та вільного доступу до різних джерел інформації, а з іншого – контроль за непоширенням таємної інформації [4, с. 128], що дозволяє захистити інтереси суспільства і держави, сприяння цілісності суспільства, захист від негативних інформаційних впливів, реалізацію права громадян на отримання всебічної та якісної інформації тощо.

Основними правовими актами регулювання суспільних відносин у цій сфері є Конституція України, Доктрина інформаційної безпеки в Україні, Закон України «Про основні засади забезпечення кібербезпеки Україні», Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"» від 15 березня 2016 р.[2] Ці документи містять теоретичні поняття про мету, загрози і принципи інформаційної та кібербезпеки в Україні й підкреслюють актуальність питання та необхідність його вивчення. Слід зазначити, що, аналізуючи зміст цих документів, можна дійти висновку, що за кібербезпеку в Україні відповідають одночасно Кабінет Міністрів України, Національна поліція, Служба безпеки України, Держспецзв'язок і Міністерство оборони України. При цьому чіткого юридичного розмежування повноважень цих органів щодо кібербезпеки немає.

Ураховуючи це, вдосконалення правових засад функціонування кіберполіції є нагальним завданням подальшого реформування системи МВС України. Створений Департамент кіберполіції Національної поліції України є міжрегіональним територіальним підрозділом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та згідно із законодавством України здійснює оперативно-розшукову діяльність[3], а отже, забезпечує реалізацію державної політики у сфері протидії кіберзлочинності, займається захистом персональних даних громадян у віртуальному просторі, в тому числі боротьбою з піратством, а також поліцейською допомогою он-лайн. У контексті адаптації українського законодавства до міжнародних норм і стандартів головна мета діяльності підрозділів кіберполіції Національної поліції України полягає у реалізації єдиної ефективної державної політики у сфері запобігання та нейтралізації внутрішніх загроз національній безпеці й зміцненні законності та правопорядку, завдяки чому правоохоронні органи України мають перетворитися на потужний державний механізм забезпечення внутрішньої, зокрема інформаційної, безпеки держави.

Відповідно до законів України «Про інформацію» від 2 жовтня 1992 р. і «Про захист персональних даних» від 1 червня 2010 р. та інших нормативно-правових актів України діяльність кіберполіції спрямовано на:

1) протидію кіберзлочинності, тобто протиправним діянням, що вчиняються з використанням інформаційних технологій або є пов'язаними з втручанням у роботу комп'ютерів, програмного забезпечення чи мереж, несанкціонованою модифікацією даних, а також інші протиправні діяння, вчинені за допомогою пристроїв доступу до інформаційного простору;

[1] Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 № 537-V // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/537-16 (дата звернення: 01.12.2020).

[2] Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016 // Президент України : офіц. інтернет-представництво URL: www.president.gov.ua/documents/962016-19836 (дата звернення: 01.12.2020).

[3] Про затвердження Положення про Департамент кіберполіції Національної поліції України : Наказ Нац. поліції України від 10.11.2015 № 85.

2) забезпечення кібербезпеки – стану захищеності прав та інтересів людини, суспільства й держави у кіберпросторі від протиправних посягань.

3) протидію правопорушенням в інформаційній сфері, яка стосується передусім вирішення проблем реалізації інформаційної політики держави, її стратегічних напрямків і тактичних заходів; ця діяльність вимагає створення системи правових і виховних заходів, спрямованих на нейтралізацію, зниження, запобігання та припинення кіберзагроз та інформаційних викликів.

Загальні завдання та повноваження працівників підрозділів кіберполіції як поліцейських визначено у Законі України «Про Національну поліцію»[1] та у Постанові Кабінету Міністрів України «Про затвердження Положення про Національну поліцію» від 28 жовтня 2015 р. № 877[2]. За специфікою (сферою) діяльності відповідно до Положення про Департамент кіберполіції Національної поліції України, затвердженого Наказом Національної поліції України від 10 жовтня 2015 р. № 85, основними завданнями кіберполіції є такі:

1) участь у формуванні та забезпеченні реалізації державної політики у сфері протидії кіберзлочинності щодо попередження і протидії кримінальним правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку;

2) сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень у сфері інформаційної безпеки, використання платіжних систем, електронної комерції та господарської діяльності;

3) завчасне інформування населення про появу новітніх кіберзлочинів;

4) упровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини;

5) реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів;

6) участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності;

7) участь у міжнародних операціях та співпраця в режимі реального часу, забезпечення діяльності мережі контактних пунктів між країнами світу[3].

А під час карантину у кіберполіції з'явилося нове і доволі специфічне завдання – моніторинг поширення дезінформації про коронавірус.

Відповідно до цих завдань функціями підрозділів кіберполіції є такі: реалізація комплексу організаційних і практичних заходів, спрямованих на попередження та протидію кримінальним правопорушенням у сфері протидії кіберзлочинності; у межах своїх повноважень ужиття необхідних оперативно-розшукових заходів щодо викриття причин та умов, які призводять до вчинення кримінальних правопорушень у сфері протидії кіберзлочинності; ужиття передбачених чинним законодавством заходів зі збирання й узагальнення інформації стосовно об'єктів, зокрема об'єктів сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем, з метою попередження, виявлення і припинення правопорушень; виконання вимог законодавства у сфері протидії кіберзлочинності; забезпечення формування й наповнення інформаційних масивів даних, автоматизованих інформаційних систем відповідно до потреб службової діяльності; розроблення рекомендацій для підвищення професійного рівня і поінформованості органів Національної поліції України, а також громадськості про результати діяльності кіберполіції; вивчення та впровадження позитивного вітчизняного і зарубіжного досвіду запобігання правопорушенням у сфері протидії кіберзлочинності; забезпечення відповідно до чинного законодавства функціонування цілодобової контактної мережі для надання невідкладної допомоги під час розслідування злочинів, пов'язаних з комп'ютерними системами та даними, переслідування осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі; аналіз та систематизація даних про правопорушення, вчинені

[1] Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/580-19 (дата звернення: 01.12.2020).

[2] Про затвердження Положення про Національну поліцію : Постанова Кабінету Міністрів України від 28.10.2015 № 877 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/877-2015-п (дата звернення: 01.12.2020).

[3] Про затвердження Положення про Департамент кіберполіції Національної поліції України : Наказ Нац. поліції України від 10.11.2015 № 85.

у сфері протидії кіберзлочинності та з використанням високих технологій, що надходять від громадян каналами кол-центрів, електронними листами та завдяки терміналам зворотного зв'язку; відповідно до чинного законодавства збір та аналіз інформації про криміногенні процеси на загальнодержавному і регіональному рівнях, оцінювання результатів за окремими показниками службової діяльності; в межах компетенції підтримка взаємодії і партнерських відносин з органами державної влади, іншими правоохоронними органами, приватним сектором та правоохоронними органами іноземних держав, міжнародними установами й організаціями у сфері протидії кіберзлочинності, підвищення довіри населення до поліції; своєчасний розгляд звернень і запитів громадян, підприємств, установ та організацій з питань, віднесених до компетенції кіберполіції, належне дотримання порядку їх прийняття, реєстрації, обліку і розгляду[1]. Також кіберполіція здійснює інформаційну діяльність: проводить серед населення роз'яснювальну роботу з питань захисту від кіберзагроз у повсякденному житті та дотримання законодавства у сфері використання інформаційних технологій.

Оскільки Департамент кіберполіції – це відносно новий орган, він також зосереджується на аналізі та впровадженні закордонного досвіду у свою діяльність. Тому до складу Департаменту кіберполіції входять структурні підрозділи, які діють за міжрегіональним принципом та безпосередньо підпорядковуються начальникові Департаменту (Донецьке, Карпатське, Київське, Подільське, Поліське, Придніпровське, Причорноморське та Слобожанське управління кіберполіції, а також управління інформаційних технологій та програмування в західному, південному та східному регіонах) [5].

На виконання положень Закону України «Про ратифікацію Конвенції про кіберзлочинність» від 7 вересня 2005 р. № 2824-IV та з метою забезпечення міжнародної діяльності кіберполіції у структурі Департаменту кіберполіції діє сектор Національного контактного пункту з реагування на кіберзлочини.

Крім того, з березня 2020 р. кіберполіція запустила безкоштовну телефонну інформаційну підтримку громадян для боротьби с фейками про коронавірус у соцмережах. Так, звернувшись за телефоном до сервісної служби Департаменту кіберполіції, громадяни можуть дізнатися про стан розгляду поданого раніше електронного звернення або отримати роз'яснення щодо діяльності підрозділу, отримати консультацію кваліфікованого спеціаліста або висловити зауваження чи пропозиції до роботи Департаменту. Метою створення такої сервісної служби є покращення комунікації з людьми та надання потрібної їм допомоги, у тому числі щодо протиправних дій, вчинених з використанням засобів електронно-обчислювальної техніки[2].

Зважаючи на викладене, можна дійти висновку, що функції поліції у сфері інформаційної безпеки поділяються за цільовим призначенням на такі: 1) основні (зовнішні), орієнтовані на правоохоронний аспект; 2) допоміжні (внутрішньосистемні), орієнтовані на сприяння реалізації основних функцій, запровадження відповідних управлінських механізмів у системі.

Слід звернути увагу на те, що на законодавчому рівні не застосовується поділ функцій на основні та допоміжні, існує єдиний перелік функцій, які стосуються різних аспектів поліцейської діяльності. Проте відзначимо, що з огляду на специфіку завдань, функцій та повноважень кіберполіції у сфері забезпечення інформаційної безпеки вона є самостійними структурним підрозділом поліції, що являє собою складну систему, для якої водночас є характерними єдність і цілісність усіх елементів, особливий порядок призначення і функціонування тощо. Крім того, як слушно зазначає К. В. Долженко, важливим є пошук нових ефективних форм і способів забезпечення інформаційної безпеки, за допомогою яких органи поліції сумісно з іншими правоохоронними органами зможуть вирішити весь комплекс завдань із захисту життєво важливих інтересів особи, суспільства та держави. У цьому аспекті потрібне чітке юридичне оформлення під час розроблення нормативних актів, які регулюють діяльність органів поліції у сфері інформаційної безпеки [9, с. 23].

Отже, систему кібербезпеки в Україні сьогодні можна охарактеризувати як слабку. Ситуація складається таким чином, що наразі кожен має піклуватися про свою кібербезпеку самостійно у випадках, коли ділиться масивом персональних даних у мережі. Між тим

[1] Там само.

[2] Кіберполіція відкрила телефонну лінію для інформаційної підтримки громадян // Кіберполіція України : офіц. сайт. 20.03.2020. URL: https://cyberpolice.gov.ua/news/kiberpoliciya-vidkryla-telefonnu-liniyu-dlya-informaczijnoyi-pidtrymky-gromadyan-6426/ (дата звернення: 01.12.2020).

інформаційна безпека та кібербезпека в Україні мають бути однією ефективною системою, що складається одразу з декількох обов'язкових компонентів. Насамперед ідеться про юридичний компонент. На жаль, чинне українське законодавство залишається недосконалим. Окрім цього, багато положень Конвенції про кібербезпеку і досі не імплементовано, хоча цей документ є важливим для забезпечення кібербезпеки в Україні. Також вкрай важливо розвивати освітній компонент. Наразі ніхто, крім кіберполіції, і на тому рівні, на якому вона це може робити, не говорить про важливість підвищення правосвідомості у сфері цифрової безпеки. Хоча необхідно розповідати про кібербезпеку в закладах середньої і вищої освіти й підвищувати кваліфікацію працівників, діяльність яких пов'язано з обробкою персональних даних. Також важливий технічний компонент – це забезпечення цілісності, конфіденційності та доступності інформації інженерно-технічними заходами. Сьогодні велике значення надається комунікаційній складовій, яка вимагає розвитку системи моніторингу та формування контенту для соціальних мереж. В умовах формування інформаційного суспільства кожна людина має бути проінформована про структуру й особливості діяльності кіберполіції.

Тому наразі актуальним завданням є створення реальних стратегічних і тактичних документів, також слід чітко поділити сфери відповідальності між суб'єктами кібербезпеки. Основні пріоритети у цій сфері – це посилення відповідальності, імплементація положень Конвенції про кібербезпеку й запровадження ефективного механізму попередження та реагування на порушення у сфері інформаційних технологій.

Висновки

Отже, вдосконалення правових засад організації та діяльності підрозділів кіберполіції Національної поліції у сфері забезпечення інформаційної безпеки та протидії кіберзагрозам, у першу чергу, спрямовано на таке:

– оптимізацію організаційної структури кіберполіції, у процесі якої особлива увага повинна приділятися визначенню базових вимог до їх діяльності, на основі чого вже повинні формулюватися конкретні функції;

– обґрунтований розподіл функцій (повноважень) між підрозділами кіберполіції та іншими суб'єктами протидії кіберзагрозам в Україні, створення належних умов для виходу на якісний новий рівень взаємодії між ними та координації їх діяльності у сфері забезпечення інформаційної безпеки;

– запровадження нових підходів до формування переліку організаційно-правових форм і методів взаємодії всіх суб'єктів протидії правопорушенням в інформаційній сфері та підвищення контролю за якістю їх реалізації;

– запровадження сучасних механізмів аналітичного і матеріально-технічного забезпечення діяльності кіберполіції, покращення системи заходів, спрямованих на підвищення рівня професіоналізму кіберполіцейських.

Список бібліографічних посилань

1. Малик Я. Інформаційна безпека України: стан та перспективи розвитку. *Ефективність державного управління*. 2015. Вип. 44. С. 13–20.

2. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навч. посіб. Київ : Кондор, 2008. 382 с.

3. Довгань О. Д. Національний інформаційний суверенітет – об'єкт інформаційної безпеки. *Інформація і право*. 2014. № 3 (12). С. 102–112.

4. Мирошниченко М. М. Правове забезпечення інформаційної безпеки держави : дис. … канд. юрид. наук : 12.00.07. Київ, 2018. 214 с.

5. Тімашов В. О. Правові основи діяльності Департаменту кіберполіції // ІТ-право: проблеми і перспективи розвитку в Україні : матеріали ІІІ Міжнар. наук.-практ. конф. (м. Львів, 7 груд. 2018 р.) / Нац. ун-т «Львівська політехніка», Навч.-наук. ін-т права та психології, ГО «Асоціація докторів філософії України». Львів : Растр-7, 2018. С. 121–127.

6. Долженко К. І. Теоретико-правові аспекти забезпечення інформаційної безпеки органами Національної поліції України // Особливості підготовки поліцейських в умовах реформування системи МВС України : зб. матеріалів І міжнар. наук.-практ. конф. (м. Харків, 20 трав. 2016 р.) / МВС України, Департамент патрул. поліції України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2016. С. 20–23.

Надійшла до редколегії 14.12.2020

КАЗАНЧУК И. Д., ЯЦЕНКО В. П. ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ НАЦИОНАЛЬНОЙ ПОЛИЦИИ УКРАИНЫ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УКРАИНЕ

Охарактеризованы содержание и составляющие компоненты информационной безопасности в Украине. Проанализировано современное состояние правового регулирования организации и деятельности подразделений киберполиции Национальной полиции Украины. Обращено внимание на определенные недостатки украинского законодательства в сфере обеспечения полицией информационной безопасности в современных условиях. С учетом специфики задач и функций киберполиции даны предложения по совершенствованию их структуры и направлений деятельности в информационной сфере.

Ключевые слова: *информационная безопасность, правовое регулирование, Национальная полиция Украины, подразделения киберполиции, противодействие, информационная сфера.*

KAZANCHUK I. D., YATSENKO V. P. PECULIARITIES OF LEGAL REGULATION OF THE ACTIVITIES OF THE NATIONAL POLICE OF UKRAINE IN THE FIELD OF ENSURING INFORMATION SECURITY IN UKRAINE

Based on the analysis of scientific concepts and legal principles the author has provided the definition of information security, provision of information security in Ukraine and has characterized its components. The current state of legal regulation of the organization and activity of cyberpolice units of the National Police of Ukraine has been analyzed. Particular attention has been paid to the legal analysis of the tasks, functions and structure of the Cyberpolice Department of the National Police of Ukraine. Special attention has been drawn to certain shortcomings of Ukrainian legislation in the field of ensuring information security by the police, its compliance with the norms and standards of international law. Taking into account the specifics of the tasks, the author has provided characteristics of the functions of cyberpolice units in the information sphere, which should be divided according to the purpose into: 1) basic (external), which are focused on law enforcement and preventive aspects; 2) auxiliary (intrasystem), which are focused on promoting the implementation of basic functions, the introduction of appropriate management mechanisms within the system.

It has been stated that the modern system of ensuring information security and cybersecurity in Ukraine should be one effective system, consisting of such mandatory components as legal, educational and technical. It has been concluded that in order to improve the legal principles for the organization and activities of cyberpolice units of the National Police in the field of ensuring information security and counteracting cyber threats, first of all, it is necessary to optimize the organizational structure of cyberpolice, reasonably distribute the functions (powers) between cyberpolice units and other subjects combating cyber threats in Ukraine, to create appropriate conditions for reaching a qualitatively new level of interaction between them and coordination of their activities in the field of ensuring information security in modern conditions.

Key words: *information security, legal regulation, National Police of Ukraine, cyber police units, counteraction, information sphere.*