адміністративно-правових відносинах. Таким чином доведено, що ЗВО МВС мають власний адмністративно-правовий статус.

2. Сучасний стан адміністративно-правового статусу ЗВО МВС України характеризується такими особливостями:

– цільовий блок – характеризується активним рухом у напрямку євро- та євроатлантичної інтеграції, що підвищує цінність злагодження призначень МОН (реалізації освітньої функції держави) та МВС (забезпечення громадського порядку і безпеки), які реалізуються в діяльності ЗВО МВС;

– структурно-організаційний блок – має особливу дворівневу підпорядкованість закладів вищої освіти МВС та МОН. Причому реформа першого з них активно вплинула на структуру відомчої вищої освіти, а зміни останньої в підходах та процедурах вищої освіти відобразились в організації роботи відомчих ЗВО;

– компетенційний блок – характеризується змінами в нормативно- правовій базі, яка регулює діяльність ЗВО МВС та свідчить про процес активного реформування системи вищої освіти і необхідність доопрацювання підзаконних нормативних актів для приведення їх у відповідність із загальними змінами системи вищої освіти.

Отримано 24.03.2020

УДК 340.13:004.056.5

БАСАРАБ О. Т.,
кандидат юридичних наук, старший викладач кафедри теорії та історії держави і права та приватно-правових дисциплін Національної академії Державної прикордонної служби України імені Богдана Хмельницького (м. Хмельницький);
https://orcid.org/0000-0001-7839-6955;

БАСАРАБ О. К.,
кандидат технічних наук, доцент кафедри зв'язку, автоматизації та кібербезпеки Національної академії Державної прикордонної служби України імені Богдана Хмельницького (м. Хмельницький);
https://orcid.org/0000-0002-2852-9534;

ЛАРІОНОВА І. Т.,
старший викладач кафедри тактичної та спеціальної фізичної підготовки факультету № 2 Харківського національного університету внутрішніх справ;
https://orcid.org/0000-0001-7006-6476

НОРМАТИВНО-ПРАВОВІ ОСНОВИ ЩОДО ПЕРСПЕКТИВ ПІДГОТОВКИ ФАХІВЦІВ КІБЕРБЕЗПЕКИ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

У роботі аналізуються правові основи забезпечення кібербезпеки Державної прикордонної служби України. Аргументуються перспективи щодо підготовки фахівців кібербезпеки прикордонного відомства.

Ключові слова: *кібербезпека, Державна прикордонна служба України, прикордонне відомство.*

В умовах активного розвитку комп'ютерних технологій, питання протидії кіберзлочинам набуває важливого значення. Особливо гостро постає зазначена проблема, коли мова йде про захист інформаційно-телекомунікаційних систем органів державної влади, правоохоронних органів, військових формувань, а також об'єктів критичної інфраструктури,

інформаційні ресурси яких призначені для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства та держави в цілому.

Відповідно до статті 1 закону України «Про основні засади забезпечення кібербезпеки України» кіберзлочином (комп'ютерним злочином) вважається суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [1].

Віртуальний простір, у межах якого циркулює інформація, що обробляється з використанням інтегрованої інформаційно-телекомунікаційної системи «Гарт», являє собою кібернетичний простір (кіберпростір) Державної прикордонної служби України (далі – ДПС України), який, з огляду на характер сучасних кіберзагроз, потребує надійного захисту [2].

Правову основу у сфері забезпечення безпеки у кіберпросторі ДПС України становлять норми міжнародного права, Конституція України, закони України («Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994, «Про інформацію» від 02.10.1992, «Про Державну прикордонну службу України» від 03.04.2003, «Про телекомунікації» від 18.11.2003, «Про захист персональних даних» від 01.06.2010, «Про основні засади забезпечення кібербезпеки України» від 05.10.2017, «Про національну безпеку України» від 21.06.2018), укази Президента України (Концепція розвитку сектору безпеки і оборони України, від 14.03.2016 № 92/2016, «Про Стратегію кібербезпеки України» від 15.03.2016 № 96/2016, «Про затвердження доктрини інформаційної безпеки України» від 25.02.2017 № 47/2017), Постанови Кабінету Міністрів України («Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373, «Про затвердження порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури» від 23.08.2016 № 563, «Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19.06.2019 № 518), накази та розпорядження Міністерства внутрішніх справ України та Адміністрації Державної прикордонної служби України (наказ Головного центру зв'язку, автоматизації та захисту інформації АДПСУ від 15.05.2018 №10од. «Про затвердження положення про центр кібербезпеки Головного центру зв'язку, автоматизації та захисту інформації», Концепція програми інформатизації системи Міністерства внутрішніх справ України на 2018-2020 роки від 05.11.2018 року № 18 КМ) та інші нормативно-правові акти.

Очевидно, що виконання положень вищезазначених нормативно-правових актів, в частині, що стосується організації та забезпечення надійного захисту кіберпростору ДПС України, повинні здійснювати спеціально підготовлені фахівці, обізнані не тільки у питаннях функціонування інформаційно-телекомунікаційних систем, але й у специфіці діяльності прикордонного відомства. Навчальною базою для реалізації такого виду освітньої діяльності може виступити Національна академія Державної прикордонної служби України імені Богдана Хмельницького (далі – НАДПС України).

Нормативним підґрунтям для підготовки вищезазначених фахівців слугуватиме: Закон України «Про вищу освіту» від 01.07.2014, наказ Міністерства освіти і науки «Про затвердження положення про акредитацію освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти» від 11.07.2019 № 977, Положення про організацію освітнього процесу в Національній академії Державної прикордонної служби України імені Богдана Хмельницького, затверджене наказом ректора НАДПС України від 26.12.2018 № 316, Положення про систему поточного і підсумкового оцінювання результатів навчання курсантів (слухачів, студентів) Національної академії, затверджене наказом ректора НАДПС України від 18.11.2019 № 395 тощо.

Таким чином, у контексті необхідності забезпечення надійного та безпечного функціонування інформаційно-телекомунікаційної системи ДПС України, проблема підготовки фахівців кібербезпеки потребує особливої уваги та пошуку шляхів щодо її вирішення.

Аналіз чинного законодавства дозволяє нам зробити висновок про наявність достатніх нормативно-правових основ щодо перспектив підготовки фахівців кібербезпеки ДПС України.

Список бібліографічних посилань

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 10.03.2020).

2. Басараб О. Т., Басараб О. К., Ларіонова І. Т. Щодо визначення поняття «кібербезпека Державної прикордонної служби України» – теоретико-правовий аспект. *Вісник Національної академії Державної прикордонної служби України. Серія: Юридичні науки*. 2019. Вип. 3. URL: http://nbuv.gov.ua/j-pdf/vnadpcurn_2019_3_5.pdf (дата звернення: 10.03.2020).

3. Про державну прикордонну службу України : Закон України від 03.04.2003 № 661-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/661-15 (дата звернення: 10.03.2020).

Отримано 12.03.2020

УДК 342.951:351.82

БІЛІЧЕНКО В. В.,
старший викладач кафедри тактико-спеціальної підготовки
Дніпропетровського державного університету внутрішніх справ;
https://orcid.org/0000-0002-0640-0895

МІЖНАРОДНИЙ ДОСВІД ВИКОРИСТАННЯ МОДЕЛЕЙ ВЗАЄМОДІЇ ПОЛІЦІЇ З НАСЕЛЕННЯМ

Стаття присвячена питанню взаємодії правоохоронних органів з населенням, на прикладі Національної поліції України. Зазначається необхідність впровадження моделі» «Community Policing», як однієї з найефективніших моделей взаємодії поліції з населенням, яка використовується в США, Великобританії, Фінляндії, Німеччині, Японії та інших. Наведено позитивні аспекти закордонного досвіду реалізації вищезазначеної моделі взаємодії правоохоронних органів з місцевим населенням.

Ключові слова: *поліція, населення, взаємодія з населенням на засадах партнерства, «Community Policing», «поліціювання».*

Постановка проблеми. У зв'язку зі стрімким процесом реформування, з активним процесом децентралізації та інтеграції української держави до європейських стандартів у правоохоронній сфері, досить велику роль відіграють правоохоронні органи, зокрема органи Національної поліції, які повинні забезпечувати публічну безпеку та публічний порядок, а і в деяких випадках надавати якісні поліцейські послуги.

Поліція є центральним органом виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку [1]. Поліцейська діяльність орієнтована на забезпечення законних прав та свобод громадян країни.

Робота поліції та оцінка їх діяльності залежить від основного критерію – рівень довіри населення до органів Національної поліції України [1].

Дана довіра виникає за умови тісної та ефективної діяльності поліції з населенням на засадах партнерства, що зазначено у ст. 11 Закону України «Про Національну поліцію України» [1].