**УДК 340.13:004.056.5**

**Ольга Тимофіївна БАСАРАБ,**
*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*

**Олександр Корнійович БАСАРАБ,**
*кандидат технічних наук,*
*доцент кафедри зв'язку, автоматизації та кібербезпеки Національної академії Державної прикордонної служби України імені Богдана Хмельницького*

**Інна Тимофіївна ЛАРІОНОВА,**
*старший викладач кафедри тактичної та спеціальної фізичної підготовки Харківського національного університету внутрішніх справ*

# ДО ПИТАННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ У КІБЕРПРОСТОРІ ДЕРЖАВНОЮ ПРИКОРДОННОЮ СЛУЖБОЮ УКРАЇНИ

В умовах ведення гібридної війни на сході нашої держави, проблема захисту інформаційно-телекомунікаційних систем органів державної влади, правоохоронних органів та військових формувань від кібернетичних злочинів, набуває особливого значення.

Віртуальний простір, у межах якого циркулює інформація, що обробляється з використанням інтегрованої інформаційно-телекомунікаційної системи «Гарт» являє собою окремий кібернетичний простір (кіберпростір) Державної прикордонної служби України (далі – ДПС України), який, з огляду на характер сучасних кіберзагроз також потребує надійного захисту [1].

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 [2].

Правове регулювання протидії кіберзлочинам у кіберпросторі ДПС України здійснюють норми міжнародного права, Конституція України, закони України («Про захист інформації в інформаційно-телекомунікаціних 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.

Аналіз вищезазначеного законодавства дозволяє зробити висновок про наявність достатнього правового підґрунтя у сфері протидії кібернетичним злочинам у кібернетичному просторі ДПС України. Разом з тим, окремі питання правового забезпечення безпеки кіберпростору прикордонного відомства від злочинних посягань, на нашу думку, варті уваги нормотворців та потребують удосконалення.

Зокрема, у Стратегії кібербезпеки України, яка є основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України, практично відсутні положення

щодо організації кібербезпеки у ДПС України, як одного із суб'єктів сектору безпеки і оборони [3]. Схожа ситуація, також, з указом президента України «Про затвердження доктрини інформаційної безпеки України» від 25.02.2017 № 47/2017 та окремими актами уряду.

Таким чином, сучасний стан правового забезпечення протидії кіберзлочинам у кіберпросторі ДПС України потребує удосконалення, шляхом внесення змін та доповнень до низки нормативно-правових актів із обов'язковим урахуванням специфіки діяльності прикордонного відомства.

**Список бібліографічних посилань**

1. 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: 06.04.2020).
2. 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: 06.04.2020).
3. Про стратегію кібербезпеки України : Указ Президента України від 15.03.2016 № 96/2016 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 06.04.2020).

*Одержано 07.04.2020*