УДК 340.13:004.056.5
DOI https://doi.org/10.32782/2524-0374/2020-4/29

АКТУАЛЬНІ ПИТАННЯ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В ДЕРЖАВНІЙ ПРИКОРДОННІЙ СЛУЖБІ УКРАЇНИ

TOPICAL ISSUES OF THE REGULATORY FRAMEWORK IN THE SPHERE OF CYBER SECURITY OF THE STATE BORDER GUARD SERVICE OF UKRAINE

Басараб О.Т., к.ю.н.,
старший викладач кафедри теорії та історії держави і права та приватноправових дисциплін
Національна академія Державної прикордонної служби України імені Богдана Хмельницького

Басараб О.К., к.т.н.,
доцент кафедри зв'язку, автоматизації та кібербезпеки
Національна академія Державної прикордонної служби України імені Богдана Хмельницького

Ларіонова І.Т., старший викладач кафедри тактичної та спеціальної фізичної підготовки
Харківський національний університет внутрішніх справ

Статтю присвячено вивченню актуальних питань нормативно-правового регулювання кібернетичної безпеки у Державній прикордонній службі України з огляду на сучасні виклики сьогодення.

Зазначається, що в умовах активізації кібернетичних атак на інформаційно-телекомунікаційні системи органів державної влади України, правоохоронних органів та військових формувань комп'ютерні мережі прикордонного відомства також потребують надійного захисту.

Сьогодні у Державній прикордонній службі України функціонує інтегрована інформаційно-телекомунікаційна система «Гарт», яка забезпечує обробку інформації за відповідними видами оперативно-службової діяльності. Віртуальний простір, у межах якого циркулює інформація, з використанням вищезазначеної системи являє собою кібернетичний простір прикордонного відомства, безпека якого повною мірою залежить від двох основних аспектів: організаційно-технічного забезпечення та якісної нормативно-правової бази.

З огляду на мету та завдання наукової статті, авторами детально досліджено нормативно-правовий аспект. У результаті наукових пошуків установлено, що правове регулювання кібернетичної безпеки Державної прикордонної служби України здійснюється нормативними актами різної юридичної сили: Конституцією України, законами та підзаконними актами України.

Конституція України містить вихідні положення щодо організації безпеки як національного кібернетичного простору в цілому, так і віртуального простору Державної прикордонної служби України, які знаходять своє відображення у законах та підзаконних нормативно-правових актах України.

Аналіз чинного законодавства у сфері забезпечення безпеки у кібернетичному просторі прикордонного відомства дав змогу виявити деяку його недосконалість.

Зроблено висновок, що актуальними та такими, що потребують вирішення найближчим часом, є питання відсутності спеціальних нормативно-правових актів у сфері забезпечення безпеки кібернетичного простору Державної прикордонної служби України, прогалини у положеннях чинних нормативно-правових актів у частині, що стосується порядку організації кібернетичної безпеки у прикордонному відомстві, а також відсутність науково обґрунтованої концепції щодо подальшого порядку розбудови кібернетичної безпеки Державної прикордонної служби України.

Ключові слова: кібернетична безпека, кібернетичний простір, нормативно-правові акти, Державна прикордонна служба України, прикордонне відомство.

The article is devoted to the study of topical issues of legal regulation of cyber security in the State Border Guard Service of Ukraine, taking into account current challenges of today.

It is noted that in the conditions of intensification of cyber attacks on information and telecommunication systems of state authorities of Ukraine, law enforcement agencies and military formations, computer networks of the border agency also need reliable protection.

Today, the State Border Guard Service of Ukraine has the integrated information and telecommunication system "Hart", which provides information processing for the relevant types of operational and service activities. The virtual space within which information circulates, using the above mentioned system, is the cyber space of the border agency, the security of which fully depends on two main aspects: organizational and technical support and qualitative regulatory framework.

Taking into account the given purpose and objectives of the scientific article, it was studied the regulatory aspect.

As a result of the scientific research, it was established that the legal regulation of cyber security of the State Border Guard Service of Ukraine is carried out by acts of different legal force: the Constitution of Ukraine, laws and subordinate legal acts of Ukraine. The Constitution of Ukraine contains basic provisions on cyber, which are reflected in the laws and subordinate legal acts of Ukraine. The analysis of all above mentioned acts revealed some of its imperfections.

It is concluded that topical issues of the regulatory framework in the sphere of cyber security of the State Border Guard Service of Ukraine are following: lack of special normative acts on cyber security of the border agency; absence of norms on cyber security of the State Border Guard Service of Ukraine in the current regulatory framework; absence of the Concept on the cyber security of the State Border Guard Service of Ukraine.

Key words: cyber security, cyber space, normative acts, State Border Guard Service of Ukraine, border agency.

Постановка проблеми. Стрімкий розвиток інформаційно-телекомунікаційних технологій значною мірою розширив сфери застосування комп'ютерної техніки. Сьогодні комп'ютеризація торкнулася практично усіх галузей суспільного життя, забезпечивши цим самим оперативність в обміні інформацією та швидкість прийняття управлінських рішень.

Разом із тим в умовах широкомасштабного використання інформаційно-телекомунікаційних систем актуальним постає питання забезпечення належного захисту інформації, особливо коли йдеться про органи державної влади, правоохоронні органи та військові формування. Так, за даними пресслужби Державної служби спеціального зв'язку та захисту інформації України, лише протягом тижня в період з 1 по 7 липня 2020 р. спеціалізованим структурним підрозділом реагування на кіберінциденти CERT-UA (Computer Emergency Response Team of Ukraine) було заблоковано 1 888 кібератак на інформаційно-телекомунікаційні системи державних органів влади та зареєстровано 19 514 інцидентів, 73% з яких стосувалися розповсюдження шкідливого програмного забезпечення та 26% – фішингу [1].

Інформаційно-телекомунікаційна мережа Державної прикордонної служби України (далі – ДПС України) також зазнавала впливу комп'ютерного вірусу, але завдяки вправним діям фахівців із кібербезпеки проблему було вчасно локалізовано [2].

З огляду на зазначене, дослідження сучасного стану нормативно-правового регулювання кібербезпеки ДПС України та виявлення актуальних питань, що потребують розв'язання, набуває особливого значення.

Аналіз останніх наукових досліджень і публікацій свідчить про те, що проблема захисту інформаційно-телекомунікаційних систем неодноразово знаходила своє відображення у працях С.Г. Божок, І.В. Діордіци, В.А. Ліпкана, Н.В. Коваленка, Б.А. Кормича, І.П. Кушнір, Ю.Є. Максименка, М.А. Стрельбіцького, О.К. Юдіна та ін.

Однак, незважаючи на велику кількість публікацій із цієї тематики, нормативно-правове регулювання кібербезпеки у ДПС України все ще потребує додаткового вивчення.

Метою і завданням наукової статті є дослідження сучасного стану нормативно-правового регулювання кібербезпеки у ДПС України та визначення актуальних питань, що потребують вирішення.

Виклад основного матеріалу. Відповідно до статті 1 Закону України «Про Державну прикордонну службу України» від 03.04.2003, на прикордонне відомство покладаються завдання щодо забезпечення недоторканості державного кордону та охорони суверенних прав України в її прилеглій зоні та виключній (морській) економічній зоні [3]. Очевидно, що ефективне виконання зазначених завдань у сучасних умовах неможливе без використання інформаційних технологій.

Сьогодні у ДПС України функціонує інтегрована інформаційно-телекомунікаційна система «Гарт» (далі – ІІТС «Гарт»), яка являє собою сукупність інформаційно-телекомунікаційних систем, що діють як єдине ціле і забезпечують обробку інформації за відповідними видами оперативно-службової діяльності.

Віртуальний простір, у межах якого циркулює інформація, з використанням ІІТС «Гарт» являє собою кібернетичний простір (кіберпростір) ДПС України [4], який в умовах численних кібернетичних атак потребує надійного захисту, оскільки інформація, що обробляється в ІІТС «Гарт», є власністю ДПС України і не підлягає поширенню або передачі іншим особам за винятком окремих випадків, передбачених законодавством.

У теорії інформаційного права під захистом інформації зазвичай розуміють застосування сукупності організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованій системі та особам, які користуються інформацією [5, с. 216]. Відповідно до ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017, захист інформації у кібернетичному просторі є не що інше, як сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [6]. Тому цілком логічно припустити, що безпека кіберпростору ДПС України повною мірою залежить від двох основних аспектів: організаційно-технічного забезпечення та якісної нормативно-правової бази.

Зупинимося детальніше на дослідженні актуальних питань нормативно-правового регулювання кібербезпеки в ДПС України.

Вихідним, на нашу думку, є положення ст. 17 Конституції України, відповідно до якого захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу. Забезпечення державної безпеки і захист державного кордону України покладаються на відповідні військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом [7].

Реалізація та деталізація цього конституційного положення знайшла своє відображення у низці законів України. Зокрема, відповідно до ст. 1 Закону України «Про національну безпеку України» від 21.06.2018, система органів державної влади, Збройних сил України, інших утворених відповідно до законів України військових формувань, правоохоронних та розвідувальних органів, державних органів спеціального призначення з правоохоронними функціями, сил цивільного захисту, оборонно-промислового комплексу України, діяльність яких за функціональним призначенням спрямована на захист національних інтересів України від загроз, утворюють собою сектор безпеки й оборони [8].

Відповідно до ст. 5 Закону України «Про основні засади забезпечення кібербезпеки в Україні» від 05.10.2017, координація діяльності у сфері кібербезпеки як складової частини національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України [6].

Своєю чергою, у п. 2 ст. 12 Закону України «Про національну безпеку України» від 21.06.2018 зазначається, що ДПС України входить до складу сектору безпеки і оборони та, відповідно до п. 6 ст. 18, є правоохоронним органом спеціального призначення, що реалізує державну політику у сфері безпеки державного кордону України та охорони суверенних прав України в її виключній (морській) економічній зоні [8].

Згідно зі ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017, Адміністрація Державної прикордонної служби України як центральний орган виконавчої влади, що реалізує державну політику у сфері охорони державного кордону, є суб'єктом забезпечення кібербезпеки в інформаційному просторі ДПС України та у межах своєї компетенції уповноважена:

– здійснювати заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

– виявляти та реагувати на кіберінциденти та кібератаки та усувати їх наслідки;

– здійснювати інформаційний обмін щодо реалізації та потенційних кіберзагроз;

– розробляти і реалізувати запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

– забезпечувати проведення аудиту інформаційної безпеки підпорядкованих підрозділів;

– здійснювати інші заходи у сфері забезпечення розвитку та безпеки кіберпростору [6].

Серед законів, які визначають основи правового регулювання кібербезпеки у ДПС України, варто також згадати закони України «Про захист інформації в інформаційно-телекомунікаціних системах» від 05.07.1994, «Про телекомунікації» від 18.11.2003, «Про інформацію» від 02.10.1992, «Про захист персональних даних» від 01.06.2010 тощо.

Правовим інструментарієм для виконання законів у сфері забезпечення кіберзахисту ДПС України є підзаконні нормативно-правові акти Президента України, міністра внутрішніх справ та голови ДПС України.

Серед актів Президента України, на нашу думку, особливий інтерес викликають Концепція розвитку сектору безпеки і оборони України, від 14.03.2016 № 92/2016, а також укази глави держави «Про Стратегію кібербезпеки України» від 15.03.2016 № 96/2016 та «Про затвер-

дження доктрини інформаційної безпеки України» від 25.02.2017 № 47/2017. Однак аналіз змісту вищезазначених актів дає нам змогу говорити про значні прогалини у правовому забезпеченні кібербезпеки ДПС України.

Зокрема, у частині, що стосується «Стратегії кібербезпеки України». У ст. 31 Закону України «Про національну безпеку України» від 21.06.2018 зазначено, що Стратегія є документом довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, підвищення ефективності основних суб'єктів забезпечення кібербезпеки, насамперед суб'єктів сектору безпеки і оборони, щодо виконання завдань у кіберпросторі, а також потреби бюджетного фінансування, достатні для досягнення визначених цілей і виконання передбачених завдань, та основні напрями використання фінансових ресурсів. Стратегія кібербезпеки України є основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України [8]. Однак у документі практично відсутні положення щодо організації кібербезпеки у ДПС України як одного із суб'єктів сектору безпеки й оборони [9].

Схожа ситуація також із Доктриною інформаційної безпеки України від 25.02.2017 № 47/2017 [10].

Аналіз зазначеної проблеми, на нашу думку, потребує особливої уваги та пошуку шляхів її вирішення, оскільки сукупність інформаційних та телекомунікаційних систем ДПС України утворюють окрему систему, у якій обробляються державні інформаційні ресурси, персональні дані та інформація з обмеженим доступом. Окрім того, у ст. 2 «Концепції розвитку сектору безпеки і оборони» захист державного кордону визначено одним з основних завдань сектору безпеки і оборони. Тоді як ст. 8 Закону України «Про Державну прикордонну службу України» від 03.04.2003 покладає координацію діяльності військових формувань та відповідних правоохоронних органів, пов'язану із захистом державного кордону України, на прикордонне відомство [3].

Щодо актів Уряду ДПС України керується постановами Кабінету Міністрів України «Про затвердження порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури» від 23.08.2016 № 563, «Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373, «Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19.06.2019 № 518 тощо.

Однак зазначені документи містять загальні положення організаційних засад забезпечення захисту державних інформаційних ресурсів або інформації, вимоги щодо захисту якої встановлено законом в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, механізму формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури.

Про недосконалість нормативно-правової бази системи Міністерства внутрішніх справ, до якої входить ДПС України, йдеться також у Концепції програми інформатизації системи Міністерства внутрішніх справ на 2018–2020 рр. від 05.11.2018. Цей документ вартий нашої уваги, оскільки він є практично єдиним актом, виданим на рівні міністерства із цього питання. Відповідно до Концепції, відсутність належного правового забезпечення породжує наявність десятків неузгоджених наказів, угод, протоколів та регламентів, підготовка яких здійснюється не системно та вибірково. Незважаючи на значні зусилля, витрачені на розроблення цих документів, нормативно-правова база у сфері інформаційно-телекомунікаційних технологій вимагає уніфікації та гармонізації, у тому числі з нормами європейського законодавства, оскільки сьогодні не відповідає сучасним вимогам і темпу розвитку, носить суперечливий характер у різних нормативно-правових актах [11].

Нормотворча діяльність Адміністрації Державної прикордонної служби України як суб'єкта забезпечення кібербезпеки в інформаційному просторі ДПС України також потребує активізації та вдосконалення.

Сьогодні ми маємо Положення про центр кібербезпеки Головного центру зв'язку, автоматизації та захисту інформації від 15.05.2018 № 10 од, що визначає структуру та завдання структурних підрозділів центру, а також права та обов'язки персоналу [12].

Однак в умовах сучасних кібернетичних загроз для врегулювання широкого спектру суспільних відносин у сфері забезпечення кібербезпеки ДПС України цього документу недостатньо. Проблема ускладнюється ще й тим, що нині відсутня науково обґрунтована концепція з кібербезпеки ДПС України, яка б визначила подальшу програму розвитку у цій галузі.

Висновки. Таким чином, аналіз стану нормативно-правового регулювання кібербезпеки ДПС України свідчить про деяку його недосконалість. Серед актуальних питань, які потребують вирішення, можна виділити такі:

– практично відсутні спеціальні нормативно-правові акти з кібербезпеки ДПС України, які б ураховували технічний потенціал інформаційно-телекомунікаційної мережі прикордонного відомства щодо забезпечення безперервного виконання завдань прикордонними підрозділами;

– у положеннях чинних нормативно-правових актів, що визначають основи кібернетичної безпеки в Україні, не повною мірою відображена організація кібербезпеки у ДПС України як суб'єкта сектору безпеки і оборони;

– відсутня концепція кібербезпеки ДПС України.

Ураховуючи вищезазначене, перспектива подальших розвідок у даному напрямі полягає у винайденні шляхів вирішення вищезазначених питань та вдосконаленні правового забезпечення кібербезпеки ДПС України.

ЛІТЕРАТУРА

1. В Україні за тиждень заблокували майже 2 тисячі кібератак на держоргани. *УНІАН.* URL : https://www.unian.ua/economics/telecom/v-ukrajini-zablokuvali-mayzhe-2-tisyachi-kiberatak-na-derzhorgani-novini-11065415.html) (дата звернення: 10.07.2020).

2. Прикордонник України від 28.09.2018 № 38. *Кіберварта*. URL : http://dpsu.gov.ua/upload/file/pu_36_2018.pdf (дата звернення: 06.06.2020).

3. Про Державну прикордонну службу України : Закон України від 03.04.2003 р. № 661-IV. URL : http://zakon5.rada.gov.ua/laws/show/661-15 (дата звернення: 10.07.2020).

4. 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.

5. Кормич Б. Інформаційне право : підручник. Харків : Бурун і К, 2011. 335 с.

6. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 11.07.2020).

7. Конституція України від 28.06.1996 № 254к/96-ВР. URL : http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-0%B2%D1%80 (дата звернення: 11.07.2020).
8. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL : https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 12.07.2020).
9. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 27.01.2016 № 47/2017. URL : https://zakon.rada.gov.ua/laws/show/96/2016#Text (дата звернення: 12.07.2020).
10. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 № 47/2017. URL : https://www.president.gov.ua/documents/472017-21374 (дата звернення: 15.07.2020).
11. Концепція (нова редакція) програми інформатизації системи Міністерства внутрішніх справ України, на 2018–2020 роки : Рішення Колегії МВС від 05.11.2018 № 18 КМ. URL : https://mvs.gov.ua/upload/file/koncepc_ya_nformatizac_mvs_12.12.2018.pdf (дата звернення: 15.07.2020).
12. Про затвердження положення про центр кібербезпеки Головного центру зв'язку, автоматизації та захисту інформації : Наказ Головного центру зв'язку, автоматизації та захисту інформації від 15.05.2018 № 10од. URL : https://dpsu.gov.ua/ua/structure/chastini-centralnogopidporyadkuvannya/golovniy-centr-zvyazku-avtomatizacii-ta-zahistu-informacii/ (дата звернення: 15.07.2020).