УДК 340.13 : 004.056.5

Ольга Басараб

Кандидат юридичних наук
старший викладач кафедри теорії та історії
держави і права та приватно-правових дисциплін
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького, Хмельницький
https://orcid.org/0000-0001-7839-6955
ot_basarab@ukr.net

Олександр Басараб

Кандидат технічних наук
доцент кафедри зв'язку, автоматизації та кібербезпеки
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького, Хмельницький
https://orcid.org/0000-0002-2852-9534
a_basarab@ukr.net

Інна Ларіонова

Старший викладач кафедри
тактичної та спеціальної фізичної підготовки
Харківський національний університет внутрішніх справ, Харків
https://orcid.org/0000-0001-7006-6476
inna.larionova@gmail.com

ЩОДО ВИЗНАЧЕННЯ ПОНЯТТЯ «КІБЕРБЕЗПЕКА ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ» – ТЕОРЕТИКО-ПРАВОВИЙ АСПЕКТ

У статті аргументується потреба визначення поняття «кібербезпека Державної прикордонної служби України». Наводяться статистичні дані щодо кількості спроб кібернетичних атак на підприємства та державні установи України. Актуалізується питання необхідності нарощування зусиль у сфері забезпечення кібернетичної безпеки прикордонного відомства. Досліджується стан, структура та призначення інформаційно-телекомунікаційної системи Державної прикордонної служби України «Гарт». Визначено види інформації, що підлягають обов'язковому захисту у прикордонній інформаційно-телекомунікаційній системі: відкрита, конфіденційна, службова, інформація, яка становить державну, або іншу, передбачену законом таємницю, інформація, вимога щодо захисту якої встановлена законом.

Обґрунтовано, що віртуальний простір, у межах якого циркулює інформація, що обробляється з використанням інформаційно-телекомунікаційної системи Державної прикордонної служби України «Гарт» являє собою кібернетичний простір (кіберпростір) Державної прикордонної служби України. Забезпечення безпеки кіберпростору прикордонного відомства здійснюється у відповідності до норм міжнародного права, Конституції України, законів та підзаконних актів національного законодавства. Відсутність нормативного визначення поняття «кібербезпека Державної прикордонної служби України» обумовила необхідність його обґрунтування на науковому рівні.

За результатами дослідження сформульовано визначення поняття «кібербезпека Державної прикордонної служби України» – це комплекс правових, організаційних та технічних заходів, спрямованих на забезпечення безпеки функціонування інформаційно-телекомунікаційних систем Державної прикордонної служби України, шляхом своєчасного виявлення, запобігання та нейтралізації реальних і потенційних загроз у кібернетичному просторі Державної прикордонної служби України.

Ключові слова: кібернетична безпека; кібернетичний простір; Державна прикордонна служба України; інформаційно-комунікаційні системи; інформація, кібернетичні загрози.

1. ВСТУП

Постановка проблеми. В умовах реалізації статті 17 Конституції України [1] та протидії новим видам загроз, де поряд із традиційними способами ведення бойових дій, все частіше застосовуються засоби електронних комунікацій для кібератак, дотримання належного рівня кібернетичної безпеки (кібербезпеки) у інформаційному просторі Державної прикордонної служби України (далі – ДПС України) є необхідною умовою забезпечення надійної охорони та захисту державного кордону України.

З розгортанням гібридної війни на сході нашої держави, кібератаки на підприємства та державні установи стали більш масштабними. За даними Міністерства оборони України перші атаки ще були зафіксовані під час масових протестів наприкінці 2013 року. Уже тоді більше 22 підприємств та державних установ України були заражені комп'ютерним хробаком «Uroboros» (вірусом, який має здатність самостійно розповсюджуватися через локальні і глобальні комп'ютерні мережі) [2]. Головною метою поширення цього вірусу було викрадення інформації, у тому числі персональних даних та паролів доступу до інформаційних ресурсів. Основними об'єктами ураження були веб-ресурси органів державної влади, в тому числі силових структур, засобів масової інформації та великих промислових підприємств. У липні 2014 року офіційний веб-портал Президента України зазнав потужної DDoS-атаки. З того часу кібернетичні атаки все частіше почали охоплювати енергетичну сферу, фінансові та державні установи сектору безпеки та оборони.

З кожним днем війна у кіберпросторі стає більш масштабною. За даними компанії «Zecurion Analytics», Росія входить до п'ятірки країн з

найрозвиненішими кіберпідрозділами та витрачає на кібервійська близько 300 мільйонів доларів на рік [2]. Більше витрачає тільки Великобританія, Китай і Сполучені Штати Америки.

У травні 2017 року інформаційно-телекомунікаційна мережа Донецького прикордонного загону ДПС України також зазнала впливу комп'ютерного вірусу, але завдяки вправним діям фахівців з кібербезпеки проблема була вчасно локалізована [3].

Проте, всупереч зростанню ризиків кібернетичних загроз, в ДПС України даній проблемі не приділяється достатня увага з боку правотворців, внаслідок чого відсутнє нормативне підґрунтя для забезпечення належного рівня кіберзахисту, протидії кіберінцидентам тощо.

З огляду на зазначене, визначення поняття «кібербезпека ДПС України» в умовах необхідності вироблення комплексу заходів з кіберзахисту та кібероборони кібернетичного простору (кіберпростору) ДПС України, видається особливо важливим.

Аналіз останніх наукових досліджень і публікацій свідчить про те, що проблема безпечного функціонування інформаційно-телекомунікаційних систем знайшла своє відображення у працях Діордіци І. В., Ліпкана В. А., Коваленка Н. В., Кушнір І. П., Максименка Ю. Є., Стрельбіцького М. А. та інших.

Однак, незважаючи на велику кількість публікацій з цієї тематики, на теперішній час відсутній єдиний підхід щодо визначення поняття «кібербезпека ДПС України», а ті визначення, що існують не у повній мірі відповідають специфічному поняттю кібернетичної безпеки у сфері функціонування інтегрованої інформаційно-телекомунікаційної системи прикордонного відомства.

Метою дослідження є дослідити та сформулювати поняття «кібербезпека ДПС України» на підставі норм чинного законодавства щодо визначення цієї категорії та з урахуванням специфіки діяльності ДПС України.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

На сьогоднішній день в ДПС України функціонує інтегрована інформаційно-телекомунікаційна система (далі – ІІТС) «Гарт», яка включає в себе сукупність інформаційно-телекомунікаційних систем, що забезпечують обробку інформації за відповідними видами оперативно-службової діяльності, які у процесі обробки цієї інформації діють як єдине ціле.

Структура ІІТС «Гарт» відповідає організаційній структурі ДПС України та включає чотири рівні автоматизації: Адміністрація Державної прикордонної служби України, регіональні управління, органи охорони державного кордону, прикордонні підрозділи.

ІІТС ДПС України «Гарт» призначена для:

забезпечення високого ступеня оперативності, відкритості, повноти і достовірності обліку, обробки і передачі інформації про обстановку на державному кордоні та стану оперативно-службової діяльності ДПС України;

підвищення оперативності та якості аналізу, оцінки і прогнозу розвитку обстановки на державному кордоні;

забезпечення своєчасною, цілісною і достовірною інформацією усіх ланок управління ДПС України при виробленні управлінських рішень.

Відповідно до Постанови Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», ДПС України як правоохоронний орган спеціального призначення зобов’язана забезпечувати надійний захист інформації, що функціонує в її ІІТС. Захисту в системі підлягає:

відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах, або передається телекомунікаційними мережами;

конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України «Про доступ до публічної інформації» від 13.01.2011 р.;

службова інформація;

інформація, яка становить державну, або іншу, передбачену законом таємницю;

інформація, вимога щодо захисту якої встановлена законом [4].

Віртуальний простір, у межах якого циркулює інформація, що обробляється з використанням ІІТС «Гарт» являє собою кібернетичний простір (кіберпростір) ДПС України.

Відповідно до закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017, прикордонне відомство, у межах своєї компетенції повинно:

здійснювати заходи щодо запобігання використання 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 [5].

Особлива важливість забезпечення належної безпеки кібернетичного простору ДПС України спонукала керівництво прикордонного відомства до створення спеціального органу – центру кібербезпеки. До складу центру входять: відділ реагування на кіберінциденти та відділ моніторингу

інформаційно-телекомунікаційних мереж.

Основними завданнями центру є:

здійснення аналізу: стану кібербезпеки; здійснення заходів щодо профілактики і боротьби з кіберзлочинністю; стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом; даних про кіберінциденти в інформаційно-телекомунікаційних системах; стану забезпечення кадрами системи кібербезпеки та підготовка пропозицій щодо її удосконалення;

забезпечення впровадження державної та відомчої політики з питань кібербезпеки;

забезпечення кібербезпеки відомчих електронних інформаційних ресурсів, елементів Національної телекомунікаційної мережі, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України;

забезпечення належного рівня координації, взаємодії та інформаційного обміну з суб'єктами забезпечення кібербезпеки;

опрацювання питань щодо визначення шляхів, механізмів та способів вирішення проблемних питань, що виникають під час реалізації державної політики у сфері забезпечення кібербезпеки [6].

У питаннях правового забезпечення кібернетичної безпеки прикордонне відомство керується нормами міжнародного права, Конституцією України, законами та підзаконними актами національного законодавства.

На сьогоднішній день нормативне визначення поняття «кібербезпека ДПС України» відсутнє, тому існує об’єктивна необхідність його обґрунтування на науковому рівні. Загальне визначення кібербезпеки, викладене у статті 1 закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017, відповідно до якої, це є «захищеність життєво важливих інтересів людини і громадянина, суспільства і держави під час використання

кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [5]. За умови врахування специфіки функціонування ІІТС ДПС України, вищенаведене положення, на нашу думку, може слугувати основою для формулювання визначення «кібербезпека ДПС України», інакше його зміст не у повній мірі відображає сутність цього поняття.

У дослідженні питання безпеки кіберпростору ДПС України варто також, на нашу думку, звернутись до міжнародного досвіду країн Європейського Союзу та держав-членів, які з кожним роком нарощують свої зусилля у цьому напрямку, впроваджуючи програми та ініціативи для посилення кібербезпеки, під якою частіше всього розуміються заходи і дії, спрямовані на захист кіберпростору у цивільній і військовій сферах від загроз, що можуть завдати шкоди взаємозалежним мережам та інформаційній інфраструктурі, або пов'язаним з ними. Кібербезпека спрямована на збереження доступності та цілісності мереж та інфраструктури, а також конфіденційності інформації, яка міститься в них [7]. Відповідно до Політики захисту кіберпростору Республіки Польща, кібербезпека – це сукупність організаційних, правових, технічних та освітніх заходів, спрямованих на забезпечення безперервного функціонування кіберпростору [8]. В свою чергу, Стратегія кібербезпеки Німеччини визначає її як бажаний стан безпеки інформаційних технологій, за якого ризики для кіберпростору скорочені до прийнятного мінімуму, а Стратегія безпеки та оборони інформаційних систем Франції – як бажаний стан інформаційної системи, за якого вона може протидіяти викликам кіберпростору, що можуть негативно вплинути на достовірність, цілісність та конфіденційність даних, які зберігаються, або обробляються даною системою [8].

Європейське агентство з питань мережевої та інформаційної безпеки, засноване у 2004 році, яке спочатку надавало настанови та рекомендації з інформаційної безпеки, а згодом розширило сферу своєї діяльності на вирішення питань кібернетичної безпеки, дає таке визначення: кібербезпека –

це є захист інформаційних активів шляхом боротьби із загрозами безпеці інформації, яка обробляється, зберігається та передається за допомогою інформаційних систем, що взаємодіють за допомогою мереж [9].

Аналіз підходів до визначення змісту поняття «кібербезпека» дозволяє нам зробити висновок про те, що кібернетична безпека ДПС України являє собою комплексне застосування органічно поєднаних та узгоджених між собою правових, організаційних та технічних заходів, направлених на захист прикордонного кіберпростору, які в кінцевому рахунку і будуть визначати сутність цього поняття.

У контексті реалізації правових заходів важливим аспектом є створення якісного законодавства у сфері кібербезпеки ДПС України відповідно до принципів:

верховенства права, поваги до прав людини і громадянина;

забезпечення національних інтересів України;

пропорційності та адекватності заходів з кіберзахисту реальним і потенційним загрозам;

захищеності кіберпростору ДПС України;

міжвідомчого та міжнародного співробітництва у сфері кібернетичного захисту та впровадження передового досвіду з питань надійного забезпечення кіберпростору ДПС України тощо.

Організаційні заходи, на нашу думку, повинні в себе включати:

упровадження ефективної уніфікованої системи планування та управління ІІТС ДПС України з використанням сучасних європейських та євроатлантичних підходів з метою забезпечення консолідації ресурсів та підвищення економічної ефективності їх використання;

формування високопрофесійного кваліфікованого персоналу для кіберпідрозділів ДПС України, підвищення рівня інформаційно-комунікаційної культури та компетентності усього персоналу прикордонного відомства;

формування наукового-технічного потенціалу у сфері кіберзахисту ДПС України та активне впровадження результатів наукових досліджень.

Реалізація технічних заходів дозволить:

впровадити політику інформаційної безпеки в ІІТС ДПС України;

забезпечити заходи безпеки інформації під час доступу до мережі «Інтернет»;

налагодити та керувати програмними, апаратними та програмно-апаратними засобами (комплексами) захисту інформації від кібератак;

здійснювати моніторинг стану кіберзахисту ІІТС ДПС України, виявляти та усувати фактори, що негативно впливають на захищеність відомчих інформаційних ресурсів.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, кібербезпека ДПС України – це комплекс правових, організаційних та технічних заходів, спрямованих на забезпечення безпеки функціонування ІІТС ДПС України, шляхом своєчасного виявлення, запобігання та нейтралізації реальних і потенційних загроз у кіберпросторі ДПС України.

Перспективи подальших розвідок у даному напрямку будуть спрямовані на дослідження питань удосконалення правового забезпечення кібербезпеки у кібернетичному просторі ДПС України.

Список використаних джерел

1. 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.

2. Офіційний сайт Міністерства оборони України. URL: http://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html.

3. Прикордонник України від 28.09.2018 № 38. Кіберварта. URL: http://dpsu.gov.ua/upload/file/pu_36_2018.pdf.

4. Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 29.03.2006 № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.

5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

6. 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/

7. Стратегія ЄС із кібербезпеки від 02.07.2013. URL: http://ec.europa.eu/ information_society/newsroom/cf/dae/document.cfm?doc_id=1667).

8. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших. URL: https://parlament.org.ua/wp-content/uploads/2016/11/INFODOVIDKA-ZAKONODAVSTVO-TA-STRATEGIYI-KIBERBEZPEKA.pdf.

9. ISACA, Глосарій з кібербезпеки. URL: http://www.isaca.org/ KnowledgeCenter/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf).

References

1. *Konstytutsiya Ukrayiny vid 28.06.1996 № 254k/96-VR* [Constitution of Ukraine dated June 28, 1996 No. 254k/96-BP]. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-0%B2%D1%80 [in Ukrainian]

2. *Ofitsiynyy sayt Ministerstva oborony Ukrayiny* [The official site of the Ministry of Defense of Ukraine]. URL: http://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html [in Ukrainian]

3. *Prykordonnyk Ukrayiny* vid 28.09.2018 № 38 [TheBorder-guard of Ukraine dated September 28, 2018 № 38]. URL: **http://dpsu.gov.ua/upload/file/pu_36_2018.pdf** [in Ukrainian]

4. *Pro zatverdzhennya pravyl zabezpechennya zakhystu informatsiyi v informatsiynykh, telekomunikatsiynykh ta informatsiyno-telekomunikatsiynykh systemakh* : Postanova Kabinetu Ministriv Ukrayiny vid 29.03.2006 № 373 [On approving rules for ensuring information protection in information, telecommunications and information and telecommunication systems: Resolution of the Cabinet of Ministers of Ukraine dated March 29, 2006 No. 373]. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF [in Ukrainian]

5. *Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny :* Zakon Ukrayiny vid 05.10.2017 № 2163-VIII [On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine dated October 5, 2017 № 2163-VIII]. URL: https://zakon.rada.gov.ua/laws/show/2163-19 [in Ukrainian]

6. *Pro zatverdzhennya polozhennya pro tsentr kiberbezpeky Holovnoho tsentru zv'yazku, avtomatyzatsiyi ta zakhystu informatsiyi* : nakaz Holovnoho tsentru zv'yazku, avtomatyzatsiyi ta zakhystu informatsiyi vid 15.05.2018 №10od [On approval of the unit on the cyber security center of the Main Center for Communication, Automation and Information Protection : Order of the Main Center for Communication, Automation and Information Protection dated May 15, 2018 №10od]. URL: https://dpsu.gov.ua/ua/structure/chastini-centralnogo-pidporyadkuvannya/golovniy-centr-zvyazku-avtomatizacii-ta-zahistu-informacii/ [in Ukrainian]

7. *Stratehiya EU iz kiberbezpeky* vid 02.07.2013 [EU Cybersecurity Strategy dated July 2, 2013]. URL: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm? doc_id=1667) [in Ukrainian]

8. *Zakonodavstvo ta stratehiyi u sferi kiberbezpeky krayin Yevropeys'koho Soyuzu, USA, Kanady ta inshykh.* [Legislation and strategies in the field of cybersecurity of the European Union, USA, Canada and others]. URL: https://parlament.org.ua/wp-content/uploads/2016/11/INFODOVIDKA-ZAKONODAVSTVO-TA-STRATEGIYI-KIBERBEZPEKA.pdf [in Ukrainian]

9. *ISACA, Hlosariy z kiberbezpeky* [ISACA, A Cybersecurity Glossary]. URL: http://www.isaca.org/KnowledgeCenter/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf) [in Ukrainian]

Olha Basarab, Oleksandr Basarab, Inna Larionova. About definition of the notion «cyber security of the State Border Guard Service of Ukraine»–– theoretical-legal aspect

The article argues for the necessity of working out the notion «cyber security of the State Border Guard Service of Ukraine». It is given statistics on the number of cyber-attack attempts on

Ukrainian business and government agencies. The need to increase efforts in the field of border cyber security is being updated. The state, structure and purpose of the information and telecommunication system of the State Border Guard Service of Ukraine «Hart» are investigated. There are such types of information that must be protected in the State Border Guard Service of Ukraine: open, confidential, official, secret information and information protection requirements of which set by law.

It is substantiated that the virtual space within which information processed using the information and telecommunication system of the State Border Guard Service of Ukraine "Hart" is circulated is a cybernetic space (cyberspace) of the State Border Guard Service of Ukraine.

The security of cyberspace of the border agency is carried out in accordance with the norms of international law, the Constitution of Ukraine, laws and subordinate legal acts of national legislation.

The lack of regulatory definition of the «cybersecurity of the State Border Guard Service of Ukraine» has caused the need for its study on a scientific level.

As the result of the research, the definition of the notion «cyber security of the State Border Guard Service of Ukraine» is formulated, it is the complex of legal, organizational and technical measures aimed at ensuring the security of the functioning of the information and telecommunication systems of the State Border Guard Service of Ukraine, by timely detection, prevention and neutralization of real and potential threats in the cybernetic space of the State Border Guard Service of Ukraine.

Key words: cybernetic security; cybernetic space; the State Border Guard Service of Ukraine; information and telecommunication systems; information, cybernetic threats.