УДК 007-049.5:356.13
DOI https://doi.org/10.32849/2663-5313.2019.7.26

Ірина Кушнір,
канд. юрид. наук,
старший викладач кафедри теорії та історії
держави і права та приватно-правових дисциплін
Національної академії Державної прикордонної
служби України імені Богдана Хмельницького

ІНФОРМАЦІЙНІ ЗАГРОЗИ В ДІЯЛЬНОСТІ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

Сучасне інформаційне суспільство потребує всебічного захисту інформації, інформаційних прав та потреб усіх учасників прикордонних відносин. Обмежити негативний вплив на інформаційні відносини в діяльності Державної прикордонної служби України можливо завдяки оцінці та своєчасному виявленню інформаційних загроз. Сьогодні своєчасне недооцінювання інформаційних загроз для України призвело до втрати де-факто частини території, а форма загроз трансформована в «інформаційну війну». Тому для своєчасного виявлення та ефективної протидії такому характеру загроз необхідно розуміти її сутність, зміст і конкретні форми прояву (види). Проблемність даного питання полягає в тому, що сьогодні не вироблено єдиного підходу до переліку інформаційних загроз, які мають загальні та спеціальні особливості для кожної окремої сфери, зокрема і для охорони державного кордону. Загрози інформаційній безпеці мають системний характер і включають загрози безпеці інформації та інформаційній інфраструктурі; загрози безпеці суб'єктів інформаційної сфери й соціальних зв'язків між ними від інформаційних впливів; загрози належному порядку реалізації прав та інтересів суб'єктів інформаційної сфери. Розглянуті наукові підходи до видової різноманітності інформаційних загроз дозволили сформулювати критерії для їх розмежування у діяльності Державної прикордонної служби України, а саме: за локалізацією; за наміром; залежно від процесу інформаційної діяльності; за характером прояву; за способом впливу; за способом заподіяння шкоди, а також визначити поняття «інформаційні загрози у діяльності Державної прикордонної служби України». Інформаційні загрози у діяльності Державної прикордонної служби України мають комплексний характер та створюють небезпеку прикордонній безпеці як складовій частині державної безпеки. Поняття «загроза» є спорідненим із поняттям «небезпека», яка створює умови заподіяння або реально завдає шкоду не лише інформаційним відносинам досліджуваної діяльності, але й усій прикордонній безпеці: це може бути як порушення цілісності інформації, подання невідповідної інформації, так і викрадення службової інформації, що спричиняють конкретну шкоду, наприклад, у вигляді прийняття неправильного управлінського рішення, ведення інформаційної війни чи дезінформацію.

Ключові слова: інформація, небезпека, національна безпека, інформаційний складник, охорона державного кордону, прикордонна сфера.

Постановка проблеми. Інформаційні загрози у сфері охорони державного кордону, за яку відповідальна Державна прикордонна служба України (далі – ДПСУ), завжди були, є і будуть, деякі з них змінюються та удосконалюються. Завдання ДПСУ полягає в тому, щоб реально оцінювати нинішні та передбачати майбутні небезпеки, у зв'язку із цим планувати свою подальшу діяльність, ґрунтовану на попередженні, недопущенні та своєчасному усуненні цих загроз. Недооцінювання чи ігнорування інформаційних загроз може призвести до серйозних проблем і прогалин у цілісній системі прикордонної безпеки, адже інформаційний складник як інтегроване явище відіграє одну із фундаментальних ролей. У результаті своєчасно не виявленої та неочікуваної інформаційної загрози з боку Російської Федерації відбулася втрата частини української території (Автономна Республіка Крим, частина Донецької та Луганської областей). Інформаційні загрози завдають суттєву шкоду не тільки суто інформаційного, але й матеріального і психологічного характеру, можуть негативно впливати на стан охорони державних кордонів, діяльність ДПСУ, на морально-психологічну стійкість персоналу відомства, імідж прикордонного відомства тощо.

Аналіз останніх досліджень. Зважаючи на те, що сьогодні узагальнено інформаційні загрози в діяльності ДПСУ не розглядались,

теоретичною основою для нашого дослідження стали напрацювання, пов'язані з інформаційними загрозами державній безпеці, таких науковців, як: Ю. Васильєв, Л. Євдоченко, О. Золотар, О. Кузьменко, В. Ліпкан, О. Литвиненко, О. Олійник, В. Остроухов, В. Петрик, М. Присяжнюк, А. Погребняк, Т. Ткачук, І. Трубін, Р. Хмелевський, та інших.

Виходячи з **мети** нашого дослідження – проаналізувати інформаційні загрози у сфері охорони державного кордону, сформульовані такі завдання: розкрити характер і зміст інформаційних загроз; запропонувати поняття інформаційних загроз та класифікувати їх у діяльності ДПСУ.

Виклад основного матеріалу. Сьогодні не вироблено єдиного підходу до переліку інформаційних загроз, хоча вони мають як загальні, так і спеціальні особливості для кожної окремої сфери, зокрема і для охорони державного кордону. Саме тому загрози інформаційній безпеці мають комплексний, системний характер і містять загрози безпеці інформації та інформаційній інфраструктурі; загрози безпеці суб'єктів інформаційної сфери й соціальних зв'язків між ними від інформаційних впливів; загрози належному порядку реалізації прав та інтересів суб'єктів інформаційної сфери [1, с. 183]. При цьому джерелами загроз можуть бути людина, технічні пристрої, моделі, алгоритми, програми, технологічні схеми обробки; зовнішнє середовище тощо [2, с. 67].

Поняття «загроза» розкривається у Словнику сучасної української мови як: груба, зухвала обіцянка заподіяти яке-небудь зло, неприємність; погрожування, нахваляння; можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого-, чого-небудь; те, що може заподіювати яке-небудь зло, якусь неприємність [3, с. 387]. Отже, справедливою є думка О. О. Золотар та І. О. Трубіна про те, що інформаційні загрози створюють інформаційну небезпеку, яка поширюється в інформаційному просторі [4, с. 107]. Інформаційні загрози породжують інформаційну небезпеку або посягають на безпеку. При цьому небезпека зумовлює можливість якогось лиха, нещастя, якоїсь катастрофи, шкоди і т. ін., стан, коли кому-, чому-небудь щось загрожує [5]. Загроза та небезпека породжують настання негативних наслідків для інформаційних та інших суспільних відносин, тобто мають однакові наслідки, а отже, їх можна ототожнювати. В. А. Ліпкан зазначає, що інформаційна війна, інформаційне протиборство й інформаційна боротьба є проявами одного, більш широкого поняття – загрози національним інтересам та національній безпеці в інформаційній сфері [6].

Інформаційні загрози безпеці держави розглядають як сукупність умов і факторів, які становлять небезпеку життєво важливим інтересам держави, суспільства й особи у зв'язку з можливістю негативного інформаційного впливу на свідомість і поведінку громадян, а також інформаційні ресурси та інформаційно-технічну інфраструктуру [7, с. 89].

Отже, інформаційні загрози знаходяться поміж площинами безпеки та небезпеки і є межею для розмежування правового чи протиправного впливу на інформаційні відносини. Усе залежить від того, була чи не була конкретна інформаційна загроза втілена, заподіяла чи створила загрозу заподіяння шкоди інформації, інформаційним правам суб'єктів відповідних відносин.

В. О. Олійник зазначає у своєму дисертаційному дослідженні, що інформаційна безпека, яка є складовою частиною національної безпеки в узагальненому вигляді, ґрунтується на таких базових елементах: національні інтереси – загроза – захист [8, с. 8].

О. О. Золотар запропонувала ширшу систему елементів інформаційної безпеки: правова та наукова (доктринальна) основа; об'єктно-суб'єктний склад, тобто об'єкти інформаційної безпеки, а також система органів (підрозділів), що здійснюють забезпечення; політика інформаційної безпеки; засоби і способи забезпечення інформаційної безпеки. Системний підхід є необхідною умовою для визначення загроз, а також пошуку оптимальних шляхів їх нейтралізації [9, с. 4–5]. Вважаємо, що необхідно комплексно та системно підходити до інформаційних загроз та визначення їх місця у системі інформаційних відносин, з урахуванням інформаційних потреб у сфері охорони державних кордонів у сучасному інформаційному суспільстві.

Інформаційна загроза потребує своєчасного державно-правового передбачення, визнання та закріплення її у законодавстві як дії суб'єктів, що у разі вчинення будуть осуджені та тягнуть за собою настання юридичної відповідальності, а також унеможливлення створення небезпеки під час організації інформаційної діяльності.

Більш конкретно розкрити інформаційні загрози у досліджуваній сфері можуть її конкретні види. У доктрині інформаційного права сформувались такі підходи:

загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу; загрози несанкціонованого й неправомірного впливу

сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання); загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, у тому числі й речову) [10];

дані навмисно перехоплюються, читаються або змінюються; користувачі ідентифікують себе неправильно (з шахрайською метою); користувач отримує несанкціонований доступ з однієї мережі до іншої [11, с. 188];

загрози порушення конфіденційності інформації, у результаті реалізації яких інформація стає доступною суб'єкту, що не володіє повноваженнями для ознайомлення з нею; загрози порушення цілісності інформації, до яких належить будь-яке зловмисне спотворення інформації, оброблюваної з використанням автоматизованих систем; загрози порушення доступності інформації, що виникають у тих випадках, коли доступ до деякого ресурсу автоматизованих систем для легальних користувачів блокується [12, с. 6–7];

загроза витоку інформації із серверів і мережі пристроїв інформаційних систем, де концентрується великий обсяг інформації; інформаційні системи (відомчі, міжвідомчі – авт.), у яких здійснюється перетворення (можливо через відкриту, незашифровану форму подання) даних при узгодженні протоколів обміну в різних ділянках мережі [13, с. 57];

за способом впливу на об'єкти інформаційної безпеки (інформаційні, фізичні, програмно-математичні, організаційно-правові); за джерелами надходження (внутрішні та зовнішні); за характером вияву (політичні, економічні, організаційно-технічні) [14, с. 8].

випадкові загрози: а) помилки обслуговуючого персоналу і користувачів; б) втрата інформації внаслідок неправильного її збереження; в) випадкове знищення або заміна; г) збій у роботі устаткування, електроживлення, дискових систем, комплектуючих елементів мережі; д) некоректна робота програмного забезпечення, зокрема, внаслідок зараження комп'ютерними вірусами тощо [15, с. 46–47]; та навмисні загрози: а) несанкціонований доступ до інформації і мережевих ресурсів; б) розкриття і модифікація даних і програм, їх копіювання; в) розкриття, модифікація або підміна трафіка обчислювальної мережі; г) розробка і поширення комп'ютерних вірусів, введення в програмне забезпечення логічних бомб; д) крадіжка магнітних носіїв і розрахункових документів; е) руйнування архівної інформації або навмисне її знищення; ж) фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому; з) перехоплення та ознайомлення з інформацією, яка передана по каналах зв'язку [15, с. 50].

Отже, розглянута видова різноманітність інформаційних загроз дозволила нам виокремити такі її види в діяльності ДПСУ за такими критеріями:

за локалізацією: зовнішні (ведення інформаційної війни РФ проти України); внутрішньодержавні (надання представникам ДПСУ неправдивої, недостовірної інформації); внутрішньовідомчі (витікання інформації через персонал ДПСУ);

за наміром: навмисні (розголошення конфіденційної чи службової інформації); ненавмисні (помилки збереження інформації, втрата носія інформації);

залежно від процесу інформаційної діяльності – під час: створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації;

за характером прояву: відомчі (посягають на прикордонну безпеку держави), корпоративні (зазіхають на безпеку окремого підрозділу), особисті (стосовно окремих громадян, посадових осіб ДПСУ);

за способом впливу: інтелектуальні (дезінформація); програмні (хакерські атаки); організаційні (порушення режиму інформації); організаційно-технічні (використання ПК для роботи з обмеженою інформацією, на якому така робота заборонена);

за способом заподіяння шкоди: прослуховування, розголошення, викрадення інформації, хакерські атаки, перекручування даних, порушення режиму інформації, спостереження за діями прикордонних нарядів (з метою з'ясування їхньої тактики та способів дій, щоб надалі планувати порушення прикордонного законодавства, чи здійснення диверсійних операцій); стихійні лиха (пожежі, повені тощо).

Отже, інформаційні загрози у діяльності ДПСУ – це створені людиною умови чи події, що не залежать від людини (стихійні лиха), які утворюють небезпеку чи заподіюють шкоду інформаційним відносинам, інформаційним правам, інформаційним ресурсам ДПСУ та посягають на прикордонну безпеку.

Висновки

Інформаційні загрози у діяльності ДПСУ мають комплексний характер і створюють небезпеку прикордонній безпеці як складовій частині державної безпеки. Поняття «загроза» є спорідненим із поняттям «небезпека», яка створює умови заподіяння або

реально заподіює шкоду не лише інформаційним відносинам досліджуваної діяльності, але й усій прикордонній безпеці: це може бути як порушення цілісності інформації, подання невідповідної інформації, так і викрадення службової інформації, що спричиняють конкретну шкоду, наприклад, у вигляді прийняття неправильного управлінського рішення, ведення інформаційної війни чи дезінформації. Тому питання збереження, охорони та захисту інформації набуває неабиякої актуальності й важливості в діяльності ДПСУ та є перспективним для подальших наукових досліджень.

Список використаних джерел:

1. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право*. 2017. № 10. С. 182–186.

2. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності. *Сучасний захист інформації*. 2016. № 4. С. 65–70.

3. Великий тлумачний словник сучасної української мови / уклад. та голов. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2005. VIII, 1728 с.

4. Золотар О. О., Трубін І. О. Класифікація загроз інформаційній безпеці. *Інформація і право*. 2013. № 3. С. 105–112. URL: http://nbuv.gov.ua/UJRN/Infpr_2013_3_12.

5. Словник української мови : в 11 томах. Т. 5, 1974. С. 246. URL: http://sum.in.ua/s/nebezpeka.

6. Ліпкан В. А. Національна безпека України : навчальний посібник. Київ : КНТ. 2009. 576 с. URL: http://politics.ellib.org.ua/pages-8283.html.

7. Інформаційна безпека (соціально-правові аспекти) / Остроухов В. О. та ін.; за ред. Є. Д. Скулиша. Київ : КНТ, 2010. 776 с.

8. Олійник О. В. Організаційно-правові засади захисту інформаційних ресурсів України : автореф. дис. ... канд. юрид. наук. Київ, 2006. 20 с.

9. Золотар О. О. Правові основи інформаційної безпеки людини : дис. ... д-ра. юрид. наук. Київ, 2018. 479 с.

10. Литвиненко О. Проблема інформаційної безпеки в контексті міграційних процесів. URL: http://nbuv.gov.ua/UJRN/Ukralm_2012_7_35. С. 116.

11. Макарова М. В. Електронна комерція : посібник для студентів вищ. навч. закладів. Київ : Видавничий центр «Академия», 2002. 272 с.

12. Кузьменко Б. В., Чайковська О. А. Захист інформації : навчальний посібник. Ч. 2. Київ : Видавничий відділ КНУКіМ, 2009. 69 с.

13. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2015. Вип. 1 (29). С. 56–61.

14. Євдоченко Л. О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації : автореф. дис. ... канд. наук з держ. упр. Львів, 2011. 24 с.

15. Погребняк А. В. Технології комп'ютерної безпеки : монографія. Рівне : МЕГУ, 2011. 117 с.

Modern information society needs comprehensive protection of information, information rights and needs of all participants in border relations. The negative influence on information relations in the activities of the State Border Guard Service of Ukraine can be limited by evaluating and timely detecting the information threats. Today, underestimation of information threats to Ukraine has led to the loss of the part of territory de facto, and the form of threats has transformed into an "information warfare." Therefore, to timely detect and effectively counteract threats of such a nature, it is necessary to understand its essence, content and concrete forms of manifestation (types). The problem character of this issue lies in the fact that today there is no single approach developed to the list of information threats with common and special features for each separate sphere, including for the field of border guarding. The system of information security threats is systemic and includes threats to the security of information and information infrastructure; threats to the security of the subjects of the information sphere and the social ties between them from information influences; threats to the proper order of realization of rights and interests by the subjects of information sphere. The scientific approaches to the variety of information threats were considered, and it allowed to formulate criteria for their differentiation in the activities of the SBGS, namely: by localization; by intent; depending on the process of information activity; by the nature of manifestation; by way of influence; by way of causing harm as well as defining the concept of "information threats in the activities of the SBGS of Ukraine." Information threats in the activities of the SBGS are complex and pose a threat to border security as a component of state security. The concept of information threat is related to the concept of danger that creates conditions for causing or actually inflicts damage not only on the information relations of the investigated sphere but also on the whole border security. This may be a violation of integrity, the submission of inappropriate information to subordinates to its superiors, and the theft of official information which do specific harm, for example, in the form of making the wrong management decision, conducting information warfare or misinformation.

Key words: information, danger, national security, information component, state border guarding, sphere of border guarding.