ДЕРЖАВНА ПРИКОРДОННА СЛУЖБА УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ ІМЕНІ БОГДАНА ХМЕЛЬНИЦЬКОГО

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова праця
на правах рукопису

КУШНІР ІРИНА ПАВЛІВНА

УДК 340.13 : 007 : 001.89] : 365.13 (477) (043.5)

ДИСЕРТАЦІЯ

ТЕОРЕТИЧНІ ТА ОРГАНІЗАЦІЙНІ ЗАСАДИ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНИХ ВІДНОСИН У ДІЯЛЬНОСТІ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

12.00.07 – адміністративне право і процес;
фінансове право; інформаційне право

Подається на здобуття наукового ступеня доктора юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ **І. П. Кушнір**

Науковий консультант – **Ляшук Роман Миколайович,** доктор юридичних наук, доцент

Київ – 2020

АНОТАЦІЯ

Кушнір І. П. Теоретичні та організаційні засади нормативно-правового регулювання інформаційних відносин в діяльності Державної прикордонної служби України. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». – Національна академія Державної прикордонної служби України імені Богдана Хмельницького, Національний авіаційний університет, Міністерство освіти і науки України. – Хмельницький, Київ, 2020.

Дисертація є першим в Україні комплексним дослідженням теоретичних та практичних засад суспільних відносини, що виникають під час обігу, охорони та захисту інформації у діяльності ДПСУ.

У дисертаційній роботі вирішено актуальну наукову проблему, що полягає у теоретичному узагальненні та розв'язанні проблем нормативно-правового регулювання інформаційних відносин у діяльності ДПСУ, формулюванні обґрунтованих рекомендацій щодо підвищення ефективності інформаційних відносин і напрямків удосконалення їх нормативно-правового регулювання.

Здійснено концептуальний підхід щодо дослідження проблеми нормативно-правового регулювання інформаційних відносин у діяльності ДПСУ, що зумовлений двоїстим характером цих відносин, а саме: зовнішніх – реалізація інформаційних прав осіб, що перетинають державний кордон України, або задоволення інформаційних потреб, захист приватності у зв'язку із функціонуванням органів і підрозділів ДПСУ тощо; внутрішніх – забезпечення інформаційної діяльності у ДПСУ, усебічний розвиток інформаційної складової в управлінні оперативно-службовою діяльністю ДПСУ, забезпечення інформаційної відкритості та збільшення довіри громадян до ДПСУ, створення умов для протидії та недопущення інформаційних загроз прикордонній безпеці, досягнення розуміння кожним військовослужбовцем і працівником ДПСУ

цінності інформації в охороні державного кордону України, особливо в умовах реальної зовнішньої агресії.

Доведено, що основними пріоритетами у врегулюванні інформаційних відносин за участю ДПСУ є реалізація інформаційних прав громадян, забезпечення приватності, інформаційна безпека, які повинні співвідноситись і збалансовуватись із заходами забезпечення прикордонної безпеки.

Запропоновано розглядати методологічну основу дослідження через систему взаємопов'язаних методів, крізь призму онтологічного, гносеологічного, аксіологічного та праксеологічного сприйняття дійсності. Установлена квінтесенція методологічного підґрунтя пізнання правового регулювання інформаційних відносин у діяльності ДПСУ, зокрема: створення теоретичної основи для формування нових змістовно якісних знань відповідно до сучасних умов розвитку інформаційних відносин у прикордонній сфері; формування логічних засад процесу опрацювання великого обсягу інформації теоретичного та практичного значення, пов'язаної з інформаційною діяльністю ДПСУ; формулювання чітких теоретичних і практичних цілей дослідження; обрання оптимального методологічного інструментарію дослідження, що залежить від світогляду науковця, специфіки прикордонної сфери та очікуваного результату дослідження й впливає на кінцевий результат; створення фундаменту для вироблення та уніфікації понятійного апарату інформаційних відносин; забезпечення всебічності отримання відомостей, даних про інформаційні відносини у сфері діяльності ДПСУ; формування та зміцнення теоретико-методологічної майстерності конкретного науковця. Методологія інформаційних відносин у діяльності ДПСУ є доволі складним і несформованим на сьогодні у межах науки інформаційного права явищем, яке можливо пізнати через систему методів, на підставі яких здійснюється розкриття теоретико-правових засад інформаційних відносин у функціонуванні ДПСУ. Методологічний інструментарій створює умови для пізнання та відображення об'єктивної дійсності цих відносин, дозволяє розкрити нове бачення інформаційних відносин

у діяльності ДПСУ, а також є теоретичним підґрунтям для вирішення практичних завдань у діяльності ДПСУ.

Визначено поняття «інформаційні відносини у діяльності Державної прикордонної служби України» та сформульовані особливості, які розкривають правову природу досліджуваних відносин, а саме: вони є різновидом суспільних відносин, притаманних сфері охорони державного кордону, специфічність яких обумовлюється динамічними процесами, пов'язаними з охороною державного кордону, забезпеченням контролю за його перетинанням, підтриманням прикордонного режиму та утриманням державного кордону; урегульовуються нормами інформаційного, адміністративного, кримінального та інших галузей права, а також нормами прикордонного законодавства; мають публічний характер у зв'язку з тим, що відбуваються за участі та ресурсів органу публічної адміністрації, – ДПСУ; абсолютний характер цих відносин означено конкретизацією одного з суб'єктів – розпорядника інформації у сфері охорони державного кордону, де інший суб'єкт є невизначений; характер і мета таких відносин обумовлюється інформаційною потребою з приводу інформації у діяльності ДПСУ та визначає вид інформаційної діяльності; стосуються інтересів суміжних держав, фізичних і юридичних осіб, які перетинають державний кордон або здійснюють різну діяльність уздовж чи безпосередньо на державному кордоні України, а також стосуються інтересів персоналу ДПСУ; є інформаційною складовою прикордонної безпеки, інформаційної безпеки держави, що у загальному впливає на забезпечення державної та національної безпеки; мають подвійну спрямованість: внутрішнє та зовнішнє. До внутрішніх належать інформаційні відносини, пов'язані зі здійсненням особовим складом відомства завдань, реалізацією їх правового статусу. До зовнішніх належать відносини, пов'язані з інформацією, необхідною для суб'єктів, які перетинають державний кордон, перебувають у прикордонній смузі або контрольованому прикордонному районі.

З'ясовано, що інформаційні відносини розкривають специфічні, особливі для діяльності ДПСУ (у забезпеченні охорони державного кордону України)

елементи, а саме: суб'єкт інформаційних правовідносин; зміст (інформаційно-правовий статус суб'єкта); об'єкт інформаційних правовідносин. Державна прикордонна служба України у досліджуваних відносинах є суб'єктом владних повноважень і розпорядником інформації у сфері відповідальності, що розкриває її як особливого суб'єкта у межах цих відносин.

Установлено, що формування та реалізація прикордонної інформаційної безпеки ґрунтується на врахуванні актуальних загроз національній безпеці України, забезпеченні інформаційних прав і визначенні пріоритетів державної політики в інформаційній сфері, залежить від чіткого нормативного регулювання та злагодженої роботи всіх структурних елементів ДПСУ у напрямку її забезпечення. Визначено, що державна політика у сфері прикордонної інформаційної безпеки передбачає діяльність компетентних органів держави із формування правових засад, напрямків інформаційної безпеки та їх реалізацію, що ґрунтується на урахуванні загроз територіальній цілісності держави та прикордонній безпеці в інформаційній сфері, спрямована на забезпечення інформаційних потреб сучасного суспільства з оволодіння даними про особливості перетинання державного кордону України, про стан охорони державного кордону та про діяльність прикордонного відомства тощо.

Основу правового регулювання інформаційної складової у діяльності ДПСУ утворює система загального та спеціального характеру, різної ієрархії нормативно-правових актів, які визначають основні засади, принципи, механізми забезпечення обігу інформації, зокрема і з використанням інформаційно-телекомунікаційних систем у сфері охорони державного кордону, що здійснюється в процесі виконання завдань ДПСУ.

Аргументовано, що установлення режиму інформації з обмеженим доступом зумовлено досягненням конкретної мети, – визначення та дотримання додаткових обмежувальних заходів для доступу до інформації та захисту тієї частини інформації, розголошення якої може завдати значної шкоди національним інтересам у прикордонній сфері. Доведено, що правовий режим інформації з обмеженим доступом є одним із головних визначальних чинників

прикордонної безпеки, а саме: важливим засобом захисту та збереження цілісності інформації, розпорядником якої є ДПСУ.

Обґрунтовано, що практична складова організації інформаційних відносин в управлінні оперативно-службовою діяльністю ДПСУ сконцентрована на процесі прийняття рішень начальниками органів і підрозділів охорони державного кордону. У процесі прийняття управлінського рішення у сфері охорони державного кордону інформація здійснює кругообіг, тільки змінюється її зміст, кількість та якість. Достовірна й актуальна інформація є основою правильного та своєчасного рішення у сфері охорони державного кордону України та впливає на прикордонну безпеку держави. Важливе значення в оперативно-службовій діяльності відіграє інформаційна взаємодія, яка є не лише фактичною передачею відповідних даних, але й організацією та здійсненням інформаційного процесу.

Ключовими аспектами нормативно-правового регулювання відносин ДПСУ з інформаційною сферою суспільства є:

інформаційна відкритість, що полягає у дієвості механізмів оприлюднення та надання інформації, пов’язаної із функціонуванням ДПСУ, а її результатом має бути доступність й отримання безперешкодно громадянами інформації у сфері компетенції прикордонного відомства, за їх потребами та інтересами;

забезпечення приватності в аспекті ідентифікації осіб, що вступають у відносини з органами та підрозділами ДПСУ, під час проходження прикордонного контролю у пунктах пропуску через державний кордон України, доступу до інформації та забезпечення захисту такої інформації;

реалізація механізмів звернення та запиту на публічну інформацію.

Забезпечення інформаційної безпеки у діяльності ДПСУ зумовлено: установленням і постійним моніторингом сучасних інформаційних загроз у сфері безпеки державного кордону України, які мають комплексний характер (порушення цілісності інформації, подання невідповідної інформації, викрадення службової інформації, що спричиняють конкретну шкоду, у вигляді прийняття неправильного управлінського рішення, ведення інформаційної війни чи дезінформації); існуванням дієвих правових гарантій (юридичної

відповідальності) охорони інформаційних відносин у прикордонній сфері, при цьому кожному окремому виду притаманні характерні риси; утвердженням стійких комплексних організаційно-правових механізмів забезпечення інформаційної безпеки в мережі Інтернет та в інформаційних системах ДПСУ.

На підставі проведеного дослідження розроблені конкретні рекомендації, що сприятимуть удосконаленню інформаційних відносин, а саме: розвитку відкритості та доступності у діяльності ДПСУ, безпеки в інформаційних системах ДПСУ, електронного урядування та електронної ідентифікації, формуванню стійкого освітнього потенціалу, свідомості, компетенцій у військовослужбовців ДПСУ про основні засади та принципи інформаційного законодавства, розвитку інформаційної культури, «комп'ютерної гігієни».

Запропоновані напрямки удосконалення нормативно-правового регулювання інформаційних відносин у діяльності ДПСУ, серед яких: необхідність здійснення систематизації норм інформаційного законодавства шляхом кодифікації, прийняття Інформаційного кодексу України, згрупування статей КК України та КУпАП, які передбачають відповідальність за порушення норм інформаційного законодавства; удосконалення термінології інформаційного законодавства; покращання нормативно-правового регулювання інформаційних відносин у нормах прикордонного законодавства (прийняття Концепції інформаційного забезпечення ДПСУ, створення відомчої нормативно-правової бази доступної до персоналу ДПСУ, внесення змін у норми окремих нормативно-правових актів).

Ключові слова: інформаційні відносини, нормативно-правове регулювання, інформація, Державна прикордонна служба України, інформаційне суспільство, охорона державного кордону, розпорядник інформації, прикордонна безпека, оперативно-службова діяльність.

SUMMARY

Kushnir I. P. Theoretical and Organizational Fundamentals of Normative and Legal Regulation of Information Relations in Activities of the State Border Guard Service of Ukraine. – Qualifying scientific work with manuscript copyright.

Thesis for obtaining the degree of Doctor of Law in specialty 12.00.07 Administrative Law and Process; Financial Law; Information Law. – Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, National Aviation University, Ministry of Education and Science of Ukraine. – Khmelnytskyi, Kyiv, 2020.

In Ukraine, the thesis is the first comprehensive research of theoretical and practical principles of public relations that arise while information is circulated, secured, and protected in the SBGS activities.

The research work solved the topical scientific problem which consists in theoretical generalizing and solving the problems of normative and legal regulation of information relations in activities of SBGS, formulating the proved recommendations to improve the efficiency of information relations and directions to develop their normative and legal regulation.

A conceptual approach to the study of the problem of normative and legal regulation of information relations in the activities of the SBGS, which is stipulated by the dual nature of these relations, namely: external – realization of information rights of persons crossing the state border of Ukraine, or satisfaction of information needs, protection of privacy in connection with the functioning of SBGS bodies and units, etc.; internal – provision of information activities in the SBGS, comprehensive development of the information component in the management of SBGS operational and service activities, ensuring information openness and increasing public confidence in the SBGS, creating conditions for counteracting and preventing information threats to border security, achieving the understanding of information value in protection of the state border of Ukraine by each serviceman and employee of the SBGS, especially in the conditions of real external aggression.

It is proved that the main priorities in adjusting the information relations with the participation of the SBGS are implementation of information rights of citizens, provision of privacy, information security, which should be correlated and balanced with border security measures.

It is proposed to consider the methodological basis of the research through a system of interrelated methods, through the prism of ontological, epistemological, axiological and praxeological perception of reality. The quintessence of the methodological basis of knowledge of the legal regulation of information relations in the SBGS activities was established, in particular: creation of a theoretical basis to form new meaningful knowledge in accordance with modern conditions for the development of information relations in sphere of border guarding; formation of logical foundations for the process of processing a large amount of information of theoretical and practical significance related to the SBGS information activities; formulation of clear theoretical and practical goals of the research; selection of the optimal methodological tools for the research, which depends on the world view of a scientist, the specifics of the sphere of border guarding and the expected result of the research and affects the final result; creation of a foundation for the development and unification of the conceptual apparatus for information relations; ensuring the comprehensive acquisition of information, data on information relations in the field of SBGS activities; formation and strengthening of theoretical and methodological skills of a particular scientist. The methodology of information relations in the SBGS activities is quite complex and unformed phenomenon today within the science of information law that can be cognized through a system of methods on the basis of which the theoretical and legal foundations of information relations in the SBGS activities are revealed. Methodological tools create conditions for cognition and reflection of the objective reality of these relations, enable to reveal a new vision of information relations in the SBGS activities, and is a theoretical basis for solving practical problems in the SBGS activities.

The concept of “information relations in the activities of the State Border Guard Service of Ukraine” is defined and the features that reveal the legal nature of the researched relations are formulated, namely: they are a kind of social relations inherent

in the sphere of state border protection, the specificity of which is determined by the dynamic processes associated with the protection of the state border, ensuring control over border crossing, providing the border regime and maintaining the state border; they are regulated by the norms of information, administrative, criminal and other branches of law, as well as the norms of legislation on border issues; they have a public character as they occur with the participation and resources of the public administration body, – the SBGS; the absolute nature of these relations is marked by specifying one of the subjects – the manager of information in the sphere of state border protection, where the other subject is uncertain; the nature and purpose of such relations are determined by the information need for information activities of the SBGS and determine the type of information activities; concern the interests of neighbouring states, individuals and legal entities that cross the state border or carry out various activities along or directly on the state border of Ukraine, as well as the interests of SBGS personnel; they are an information component of border security, information security of the state, which in general affects the provision of state and national security; they have a dual focus: internal and external. Internal relations include information relations related to the execution of tasks by the personnel of the agency, the implementation of their legal status. External relations include relations related to information necessary for subjects crossing the state border, staying in the border zone or in the controlled border area.

It was found that information relations reveal specific elements which are special for the SBGS activities (for ensuring the protection of the state border of Ukraine), namely: subject of information legal relations; content (information and legal status of the subject); object of information legal relations. The State Border Guard Service of Ukraine in the researched relations is a subject of authority powers and the administrator of information in the area of responsibility, which reveals it as a special subject within these relations.

It is established that the formation and implementation of border information security is based on taking into account the current threats to national security of Ukraine, ensuring information rights and determining priorities of state policy in the information sphere, depends on accurate statutory regulation and coordinated work of

all structural elements of SBGS in the direction of its provision. It is determined that the state policy in the sphere of border information security provides for the activities of competent state bodies to form the legal framework, directions of information security and their implementation which is based on consideration of threats to the territorial integrity of the state and border security in the information sphere and aimed at meeting the information needs of modern society to acquire the data on the peculiarities of crossing the state border of Ukraine, the state of protection of the state border and the activities of the border guard agency, etc.

The basis of legal regulation of the information component in the SBGS activities is a system of general and special nature with different hierarchy of statutory and regulatory acts that define the basic principles, foundations, mechanisms for ensuring the circulation of information, including the use of information and telecommunications systems in the sphere of state border protection in the process of performing the SBGS tasks.

It is argued that the sensitive information regime is established to achieve a specific goal, – to define and ensure additional restrictive measures to access information and protect that part of information which disclosure may cause significant harm to national interests in the sphere of border guarding. It is proved that the legal regime of sensitive information is one of the main determining factors of border security, namely: an important means of protecting and preserving the integrity of information managed by the SBGS.

It is substantiated that the practical component of the organization of information relations in the management of operational and service activities of the SBGS is focused on the decision-making process of the chiefs of the state border protection bodies and units. In the process of making management decisions in the sphere of state border protection, information circulates permanently, only its content, quantity and quality change. Reliable and up-to-date information is the basis of a correct and timely decision in the sphere of the state border protection of Ukraine and affects the border security of the state. An important role in operational and service activities is played by information interaction, which is not only the actual transmission of relevant data, but

also the organization and implementation of the information process.

The key aspects of legal regulation of the SBGS relations with the information sphere of society are:

information transparency which consists in effective mechanisms for publishing and providing information related to the functioning of the State Border Guard Service of Ukraine, and its result should be the available and unobstructed information in the sphere of competence of the border guard agency which can be obtained by citizens according to their needs and interests.

ensuring privacy in the aspect of identification of persons entering into relations with SBGS bodies and units, during border control procedures at border crossing points on the state border of Ukraine, access to information and ensuring the protection of such information;

implementing mechanisms for addressing and requesting public information.

Ensuring information security in the activities of the SBGS is conditioned by: establishment and constant monitoring of modern information threats in the sphere of state border security of Ukraine, which are complex (violation of the information integrity, submission of inappropriate information, theft of official information, causing specific damage in the form of wrong management decisions, information warfare or dissemination of false information); the existence of effective legal guarantees (legal responsibility) for the protection of information relations in the sphere of border guarding with each certain type having its own characteristics; approval of stable complex organizational and legal mechanisms to ensure information security on the Internet and in the information systems of the SBGS.

Based on the research, specific recommendations were developed that will help improve information relations, namely: development of openness and accessibility in SBGS activities, security in SBGS information systems, e-government and electronic identification, formation of sustainable educational potential, consciousness, competencies of SBGS servicemen on basic foundations and principles of information legislation, development of information culture, “computer hygiene”.

The directions for improving normative legal regulation of information relations in SBGS activities are offered, including: the need to systematize the norms of information legislation through codification, adoption of the Information Code of Ukraine, grouping of articles of the Criminal Code of Ukraine and the Code of Administrative Offences of Ukraine, which provide for liability for violation of information legislation; improving the terminology of information legislation; improvement of normative legal regulation of information relations in norms of border legislation (adoption of the Concept of SBGS Information Support, creation of departmental normative legal base accessible to SBGS personnel, modification of norms of separate normative legal acts).

Keywords: information relations, normative legal regulation, information, State Border Guard Service of Ukraine, information society, state border protection, information manager, border security, operative and service activities.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Монографії:

1. Кушнір І. П. Нормативно-правове регулювання інформаційних відносин у діяльності Державної прикордонної служби України: теоретичні та організаційні аспекти : монографія / за заг. ред. д-ра юрид наук Р. М. Ляшука, Хмельницький. Вид-во: ПП «Монускрипт», 2020. 528 с.

Калюжний Р. А. *Рецензія на монографію* Кушнір І. П. «Нормативно-правове регулювання інформаційних відносин у діяльності Державної прикордонної служби України: теоретичні та організаційні аспекти». Юридичний вісник «Повітряне і космічне право». 2020. № 2 (55). С. 224–225.

Орловська Н. А. *Рецензія на монографію* Кушнір І. П. «Нормативно-правове регулювання інформаційних відносин у діяльності Державної прикордонної служби України: теоретичні та організаційні аспекти». Часопис Київського університету права. 2020. № 2. С. 513.

2. Kushnir I. Topical directions for improvement of information relations in

activities of The State Border Guard Service Of Ukraine. Low and Border: Addressing Security Threats at the Ukrainian Border : collective monograph / N. Orlovska, S. Filippov, V. Kushar, I. Hloviuk, V. Polovnikov, I. Kushnir, P. Volynets. Lviv-Torun : Liha-Pres. 2019. P. 89–108.

Статті в наукових фахових виданнях України та періодичних наукових виданнях, внесених до міжнародних наукометричних баз:

3. Кушнір І. П. Інформаційні відносини у прикордонній сфері. *Науковий вісник Ужгородського національного університету*. 2016. № 36. Т. 2. С. 36–38.

4. Кушнір І. П. Напрями прикордонної інформаційної безпеки як складова національної безпеки України. *Порівняльно-аналітичне право*. № 5. 2017. С. 230–233. URL: http://pap.in.ua/index.php/arhiv-vidannja/96.

5. Кушнір І. П. Доктринальні підходи до різноманітності інформаційних правовідносин. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки.* 2017. Вип. 4. URL: http://nbuv.gov.ua/UJRN/vnadpcurn_2017_4_8.

6. Кушнір І. П. Класифікація інформаційно-правових відносин у прикордонній сфері. *Вісник Запорізького національного університету. Юридичні науки.* 2017. № 4. С. 56–62. URL: http://nbuv.gov.ua/UJRN/Vznu_Jur_2017_4_9.

7. Кушнір І. П. Основні засади інформаційної політики держави в прикордонній сфері. *Науковий вісник Херсонського державного університету. Юридичні науки*. 2017. Вип. 6. Т. 2. С. 81–84.

8. Кушнір І. П. Види інформації, розпорядником якої є Державна прикордонна служба України, їх сутнісна характеристика. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2018. Вип. 1. URL: http://nbuv.gov.ua/UJRN/vnadpcurn_2018_1_6.

9. Кушнір І. П. Органи охорони державного кордону як суб’єкти інформаційних правовідносин. *Правові новели*. 2018. № 5. С. 71–77.

10. Кушнір І. П. Кримінально-правове забезпечення охорони інформаційних відносин у прикордонній сфері. *Питання боротьби зі злочинністю.* 2018. Вип. 36. 186 с. С. 82–93.

11. Кушнір І. П. Інформаційно-правова діяльність Державної прикордонної служби України: нормативно-правовий аспект. *Конституційно-правові академічні студії*. 2018. № 2. С. 165–170.

12. Кушнір І. П. Інформаційно-правовий статус Державної прикордонної служби України. *Приватне та публічне право*. 2018. № 4. с. 50–53.

13. Кушнір І. П. Аналіз змісту поняття «безпека державного кордону». *Вісник Південного регіонального центру Національної академії правових наук України*. 2018. № 16. С. 76–81.

14. Кушнір І. П. Організаційно-правові питання забезпечення захисту інформації в інформаційних системах Державної прикордонної служби України. *Прикарпатський юридичний вісник*. 2018. № 3. С. 81–84.

15. Кушнір І. П. Співвідношення понять «інформаційна безпека» та «захист інформації» в діяльності Державної прикордонної служби України. Науковий вісник *Міжнародного гуманітарного університету. Юриспруденція.* 2018. № 35. Т. 1. с. 81–84.

16. Кушнір І. П. Особливості правових відносини щодо забезпечення запиту на публічну інформацію, розпорядником якої є Державна прикордонна служба України. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2018. Вип. 4. URL: https://nadpsu.edu.ua/wp-content/uploads/2019/02/visnuk_4_2019_ur.pdf.

17. Кушнір І. П. Адміністративна відповідальність за порушення законодавства про інформацію у прикордонній сфері. *Право і інформація.* № 1(28). 2019. С. 45–51.

18. Кушнір І. П. Інформаційна відкритість у діяльності Державної прикордонної служби України. *Правова позиція.* 2019. № 1 (22). С. 30–36.

19. Кушнір І. П. Інформаційні загрози в діяльності Державної

прикордонної служби України. *Підприємництво, господарство і право*. 2019. № 7. С. 147–150.

20. Кушнір І. П. Царенко О. М. Правовий режим інформації з обмеженим доступом у діяльності Державної прикордонної служби України. *Право та державне управління.* 2019. № 3. С. 180–185.

21. Кушнір І. П., Коротушак А. І. Питання удосконалення впровадження електронного урядування у Державній прикордонній службі України. *Вісник Південного регіонального центру Національної академії правових наук України*. 2019. № 20. С. 96–102.

22. Кушнір І. П. Теоретичні засади дослідження інформаційних відносин у діяльності Державної прикордонної служби України. *Держава та регіони. Право.* 2019. № 4. С. 86–91.

23. Кушнір І. П., Царенко С. І., Царенко О. М. Особливості застосування дисциплінарної відповідальності за порушення інформаційного законодавства у діяльності Державної прикордонної служби України *Актуальні проблеми вітчизняної юриспруденції.* 2019. № 6. С. 80–84.

24. Кушнір І. П., Новодранов Р. С. Проблеми та перспективи розвитку консультаційної роботи Контактного центру Державної прикордонної служби України. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2019. Вип. 4. URL: http://periodica.nadpsu.edu.ua/index.php/legal/article/view/316/317.

25. Кушнір І. П. Актуальні питання забезпечення інформаційної приватності у діяльності Державної прикордонної служби України. *Конституційно-правові академічні студії*. 2020. № 1. С. 7–13.

Статті у наукових періодичних виданнях інших держав:

26. Кушнір І., Степанова Ю. Інформаційна безпека держави у прикордонній сфері як об’єкт державної зради. National law journal: theory and practice. 2018. № 4 (32). Т. 1. С. 123–126.

27. Кушнір І. П. Реалізація права на звернення громадян у Державній прикордонній службі України. Visegrad Journal on Human Rights. 2018. 4 (volume 2). С. 56-60.

28. Кушнір І. П. Методологічні засади теорії інформаційних відносин у прикордонній сфері. National law journal: theory and practice. 2019. № 2 (36). С. 17–20.

29. Kushnir I. Information component in preparing and making management decisions in border protection bodies of the state border of Ukraine. Legea si Viata. 2019. № 5. С. 100–104.

30. Кушнір І. П. Основні тенденції інформаційної взаємодії у діяльності Державної прикордонної служби України. Visegrad Journal on Human Rights. 2019. 4 (volume 2). С. 96–101.

31. Kushnir I. A Comparative Analysis of Personal Data and its Protection in the Course of Border Procedures (Ukraine, European Union). *Current Issues in Administrative Law*. Edited by Cătălin-Silviu Săraru. 2020. Cambridge Scholars Publishing. С. 130–141.

Опубліковані праці апробаційного характеру:

32. Кушнір І. П. Суспільні інформаційні відносини в діяльності органів охорони державного кордону. *Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України* : тези VIII Всеукраїнської науково-практичної конференції (Хмельницький, 10 грудня 2015 р.). Хмельницький : Вид-во НАДПСУ, 2015. с. 141.

33. Кушнір І. П. Правове забезпечення захисту інформації пов’язаної із охороною державного кордону. *Кібербезпека України : правові та організаційні питання* : тези Всеукраїнської науково-практичної конференції (м. Одеса, 21 жовтня 2016 р.). Одеса : ОДУВС, 2016. С. 152–154.

34. Кушнір І. П. Забезпечення права подання запиту на інформацію у Державній прикордонній службі України. *Інформаційна безпека: європейські*

орієнтири та перспективи для України : збірник наукових праць за матеріалами ІІІ Міжнародного науково-практичного столу. Серія «Сектор безпеки України». № 14 (м. Харків, 25 листопада 2016 р.). Харків : «Плеяда», 2016. С. 94–94.

35. Кушнір І. П. Отримання громадянами інформації про діяльність Державної прикордонної служби України. *Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України* : тези ІХ Всеукраїнської науково-практичної конференції (Хмельницький, 8 грудня 2016 р.). Хмельницький : Вид-во НАДПСУ, 2016. с. 187.

36. Кушнір І. П. Проблемні питання відомчої нормотворчої компетенції Державної прикордонної служби України. *Молодіжний науковий юридичний форум* : тези доповідей Всеукраїнській науково-практичній конференції до Дня науки (м. Київ, 18 травня 2017 р.). Київ : Вид-во ТОВ МП ЛЕСЯ, 2017. С. 27–28.

37. Кушнір І. П. Державна інформаційна політика у прикордонній сфері. *Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України* : тези Х Всеукраїнської науково-практичної конференції (Хмельницький, 2 листопада 2017 р.). Хмельницький : Вид-во НАДПСУ, 2017. С. 199–200.

38. Кушнір І. П. Питання кримінально-правової охорони інформації у функціонуванні Державної прикордонної служби України. *Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності* : тези ІІ Всеукраїнської науково-практичної конференції (Хмельницький, 2 березня 2018 р.). Хмельницький: Вид-во НАДПСУ, 2018. С. 169–172.

39. Кушнір І. П. Окремі аспекти забезпечення міжвідомчого обміну інформацією між суб’єктами інтегрованого управління кордонами. *Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи* : тези п’ятої Всеукраїнської науково-практичної конференції (Одеса, 13-14 вересня 2018 р.). Одеса. 2018. С. 57–59.

40. Кушнір І. П. Прикордонна інформаційна безпека як складова національної безпеки України *Освітньо-наукове забезпечення складових сектору*

безпеки і оборони України : тези XI Всеукраїнської науково-практичної конференції (Хмельницький, 15 листопада 2018 р.). Хмельницький : Вид-во НАДПСУ, 2018. С. 247–248.

41. Кушнір І. П. Захист інформації отриманої під час здійснення оперативно-розшукової діяльності в інтересах забезпечення захисту державного кордону України: кримінально-правовий аспект. *Актуальні проблеми кримінально-правового, кримінально-процесуального та криміналістичного забезпечення безпеки України* : тези Міжнародної науково-практичної конференції (Дніпро, 30 листопада 2018 р.). Дніпро: Вид-во Біла К. О., 2018. С. 99–100.

42. Кушнір І. П. Кібербезпека як складова інформаційної безпеки у сфері охорони державного кордону України. *Кібербезпека України : правові та організаційні питання* : тези Всеукраїнської науково-практичної конференції (м. Одеса, 30 листопада 2018 р.). Одеса : ОДУВС, 2018. С. 48–49.

43. Кушнір І. П. Щодо поняття «недостовірні відомості» у складі злочину «незаконне перетинання державного кордону України». *Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності* : тези II Всеукраїнської науково-практичної конференції (Хмельницький, 1 березня 2019 р.). Хмельницький : Вид-во НАДПСУ, 2019. С. 243–244.

44. Кушнір І. П. Інформаційна взаємодія як основа забезпечення спільних дій правоохоронних органів та військових формувань в охороні державного кордону. *Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи* : тези Міжнародної науково-практичної конференції (Одеса, 13-14 вересня 2019 р.). Одеса. 2019. С. 186–187.

45. Кушнір І. П. Питання контролю та нагляду у функціях Державної прикордонної служби України. *Стан та перспективи розвитку адміністративного права України* : тези IV Міжнародної науково-практичної інтернет-конференції (Одеса, 23 жовтня 2019 р.). Одеса. 2019. С. 64.

46. Кушнір І., Степанова Ю. Критерії класифікації злочинів у сфері службової діяльності. *Пріоритетні напрямки розвитку та реформування правоохоронних органів* : тези науково-практичної інтернет-конференції. (Херсон, 31 жовтня 2019 р.). Херсон. 2019. С. 184–189.

47. Кушнір І. П. Правовий режим інформації як детермінанта прикордонної безпеки. *Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України* : тези Міжнародної науково-практичної конференції (Хмельницький, 22 листопада 2019 р.). Хмельницький : Вид-во НАДПСУ, 2019. С. 262–263.

48. Кушнір І. Актуальні засади захисту інформації, що обробляється в автоматизованих системах Державної прикордонної служби України. *Кібербезпека України : правові та організаційні питання* : тези Міжнародної науково-практичної конференції (м. Одеса, 22 листопада 2019 р.). Одеса : ОДУВС, 2019. С. 25–26.

49. Кушнір І. Питання удосконалення термінології інформаційного законодавства. *Українська мова в юриспруденції: стан, проблеми, перспективи* : тези XV Всеукраїнської науково-практичної конференції. КНУВСУ (Київ, 28 листопада 2019 р.). Київ. 2019. Ч. 1. С. 129–131.

50. Кушнір І. Щодо наслідків інформаційно-психологічного впливу як прояв військової боротьби. *Військова освіта і наука: сьогодення та майбутнє* : тези XV Міжнародної науково-практичної конференції. (Київ, 29 листопада 2019 р.) Київ. 2019.с. 239–240.

51. Кушнір І. П. Інформаційна функція у контексті інтегрованого управління кордонами. *Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи* : тези Міжнародної науково-практичної конференції (Одеса, 10-11 вересня 2020 р.). Одеса. 2020. С. 462–463.

52. Кушнір І. П. Інформаційна відкритість, як невід’ємна складова забезпечення прикордонного контролю: досвід Державної прикордонної служби України. *Стратегічні комунікації у сфері забезпечення національної безпеки і*

оборони : проблеми, досвід, перспективи : тези доповідей І-ої Міжнародної науково-практичної конференції (м. Київ, 1 жовтня 2020 р.). Київ. 2020. С. 65–67.

53. Кушнір І. Термін «забезпечення» у контексті інформаційних відносин. *Українська мова в юриспруденції: стан, проблеми, перспективи* : тези XVI Всеукраїнської науково-практичної конференції. КНУВСУ (Київ, 25 листопада 2020 р.). Київ. 2020. С. 64–67.

54. Кушнір І. П. Актуальні питання забезпечення прайвесі (правові та соціальні аспекти). *Актуальні проблеми інтелектуального, інформаційного та IT права* : збірник матеріалів четвертої Всеукраїнської науково-практичної конференції (м. Львів, 12 листопада 2020 р.). Львів. 2020. С. 87–91.

Наукові праці, які додатково
відображають результати дисертації:

55. Кушнір І. П., Ляшук Р. М. Результативність та ефективність в діяльності органів охорони державного кордону України. *Право і суспільство*. № 5. 2017. С. 154–159.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АТО	–	Антитерористична операція
ВРУ	–	Верховна Рада України
ДПСУ	–	Державна прикордонна служба України
ДМСУ	–	Державна митна служба України
ДМС України	–	Державна міграційна служба України
ДПА України	–	Державна податкова адміністрація України
ДФС України	–	Державна фіскальна служба України
ЗМІ	–	засоби масової інформації
ЗС України	–	Збройні сили України
ЄС	–	Європейський Союз
ІТС	–	Інформаційно-телекомунікаційна система
КМУ	–	Кабінет Міністрів України
КК України	–	Кримінальний кодекс України
КП ДПСУ	–	консультаційні пункти Державної прикордонної служби України
КСЗІ	–	комплексна система захисту інформації
КУпАП	–	Кодекс України про адміністративні правопорушення
МВС України	–	Міністерство внутрішніх справ України
МЗС України	–	Міністерство закордонних справ України
Мінінфраструктури	–	Міністерство інфраструктури України
МФ України	–	Міністерство фінансів України
Мінсоцполітики	–	Міністерство соціальної політики України
МОН України	–	Міністерство освіти і науки України
НАДПСУ	–	Національна академія Державної прикордонної служби України імені Богдана Хмельницького
ООДК	–	орган охорони державного кордону
ООС	–	Операція об’єднаних сил
ОРД	–	оперативно-розшукова діяльність
РФ	–	Російська Федерація
СБ України	–	Служба безпеки України
СЗР України	–	Служба зовнішньої розвідки України
Стратегія ІУК	–	Стратегія інтегрованого управління кордонами
ЦК України	–	Цивільний кодекс України
FRONTEX	–	Європейське агентство прикордонної та берегової охорони

ВСТУП

Актуальність теми дослідження. На сучасному етапі відбувається інтенсивне зростання цінності й ролі інформації, інформаційних ресурсів та інформаційних технологій як у забезпеченні прав громадян на вільне перетинання державного кордону, прикордонної безпеки, так і в процесі ухвалення управлінських рішень посадовими особами Державної прикордонної служби України (далі – ДПСУ). У зв'язку з цим особливої актуальності набувають такі напрями діяльності ДПСУ: дотримання прав громадян на інформацію і приватність, забезпечення збереження і захисту інформації, безпечного обігу, використання й опрацювання інформації в інформаційних системах відомчого та міжвідомчого значення ДПСУ, розвиток електронного урядування та електронної ідентифікації осіб.

В умовах динамічного зростання пасажиропотоку на державному кордоні (у 2017 – 97,3 млн осіб, у 2018 – 100,5 млн осіб, у 2019 – 102 млн осіб) відзначається збільшення потреби громадян в реалізації їх права на інформацію у сфері діяльності ДПСУ. Загалом у ДПСУ зафіксовано у 2018 році 27 634 звернень, у 2019 році – 29 065; до Контактного центру надійшло у 2018 році 230 016 дзвінків, у 2019 році – 291 761. Така тенденція потребує подальшого розвитку й оптимізації інформаційної діяльності щодо звернень і запитів, висвітлення інформації, пов'язаної із функціонуванням ДПСУ.

Нормативно-правове регулювання інформаційних відносин має вагоме значення в діяльності органів державної влади, особливо якщо це стосується складових сектору безпеки й оборони, зокрема ДПСУ, яка є розпорядником інформації в межах забезпечення недоторканності державного кордону й охорони суверенних прав України в її прилеглій зоні та виключній (морській) економічній зоні. Підкреслюючи важливість інформації, ми говоримо про її цінність, зокрема маємо на увазі відомості, які мають велике значення, потребують збереження та захисту. Багатогранне «вимірювання» інформації може відображати: її зміст, формування інформаційного забезпечення діяльності, можливість впливу на

свідомість, зміну обставин, забезпечення стану безпеки, важливість для окремих суб'єктів чи сфери діяльності. Різноманітність і динамічність розвитку відносин, пов'язані з обігом такої інформації в діяльності ДПСУ, потребують їх наукового вивчення та узагальнення.

Виконання поставлених перед ДПСУ завдань перебуває у нерозривному взаємозв'язку з прогресуючим розвитком інформаційних відносин і зростанням ролі інформації в управлінській діяльності. Це обумовлено необхідністю ухвалення своєчасних і правильних рішень керівним складом ДПСУ в умовах збільшення правових меж регулювання обігу інформації, забезпечення умов дієвості упровадження основних принципів інформаційних відносин, появи нових сучасних виявів інформаційних відносин (впровадження державного онлайн-сервісу «Дія» як складової «цифрової держави»), реальних і потенційних загроз в охороні державного кордону України, посилення охорони та захисту інформації, розголошення якої може завдати шкоди національній безпеці України.

Розвиток інформаційних відносин у системі охорони державного кордону України та розширення формату обміну інформацією передбачені Стратегією розвитку ДПСУ. Дана Стратегія орієнтована на створення нової системи захисту державного кордону, невід'ємною складовою реалізації якої є приведення механізмів накопичення, опрацювання, зберігання, поширення, охорони й захисту, оцінки й аналізу інформації, розпорядником якої є ДПСУ відповідно до міжнародних і національних вимог. У зв'язку з цим наукового системного правового аналізу потребують елементи інформаційної складової охорони державного кордону, зокрема: модернізація інформатизації та захисту інформації; забезпечення відкритості та прозорості; упровадження електронного урядування, документообігу з використанням електронного цифрового підпису.

Представниками української юридичної науки напрацьовано вагомий теоретичний фундамент, що сприяє підвищенню ефективності правового регулювання суспільних інформаційних відносин. Науково-методологічну основу дисертаційної роботи склали праці відомих правознавців, спеціалістів у сфері дослідження інформаційного права, зокрема: І. В. Арістової, О. А. Баранова,

К. І. Бєлякова, А. М. Благодарного, В. М. Брижка, Ю. П. Бурила, В. Д. Гавловського, М. І. Дімчоглого, Л. О. Євдоченка, В. А. Залізняка, Р. А. Калюжного, А. В. Кардаш, О. Г. Комісарова, О. В. Копана, Б. А. Кормича, І. Ф. Коржа, П. У. Кузнецова, В. А. Ліпкана, Ю. Є. Максименка, О. А. Мандзюка, О. Г. Марценюка, А. І. Марущака, М. М. Мікуліна, В. О. Негодченка, А. М. Новицького, Н. Б. Новицької, В. Г. Пилипчука, О. М. Селезньової, І. М. Сопілко, О. В. Стоєцького, О. К. Тугарової, К. П. Череповського, В. С. Цимбалюка, А. В. Шапки, М. Я. Швеця, Т. А. Шевцова, О. В. Шепети, І. М. Шопіної, О. І. Яременка та інших науковців. Багатоаспектність і комплексний характер інформаційних відносин досліджено в галузі політології (Г. Г. Почепцовим, С. А. Чукутом), теорії держави і права (Н. М. Крестовською, Л. Г. Матвєєвою, Ю. А. Івановим, О. Ф. Скакун, О. О. Тихомировим), адміністративного права (В. Л. Грохольським, Т. О. Коломоєць, В. К. Колпаковим), інших галузей (О. В. Андрушка, О. В. Кохановської, Н. А. Савінової) тощо.

Проблеми правового регулювання інформаційних відносин досліджено у працях зарубіжних авторів, зокрема: І. Л. Бачило, В. М. Боєра, Г. Г. Воробйова, О. А. Гаврилова, В. Д. Єлькіна, Н. Н. Ковальової, В. А. Копилова, В. І. Лапіна, М. А. Лапіної, В. Н. Лопатина, Ю. І. Мигачева, Д. В. Огородова, О. Г. Павельєвої, Л. Л. Попова, И. М. Рассолова, А. Г. Ревіна, Ю. А. Тихомирова, С. В. Тихомирова, М. А. Федотова, С. Г. Чубукової, С. Браман, Дж. Фрулінгера та інших.

Основою дослідження правових засад інформаційної діяльності, інформаційної безпеки та відкритості органів влади в інформаційному суспільстві стали роботи таких учених, як Е. А. Афоніна, В. Ю. Баскакова, О. О. Безвершенка, Н. В. Гудими, Р. Р. Дробожура, С. О. Дорогих, В. М. Желіховського, О. О. Золотар, Н. В. Крука, О. А. Кудіна, А. М. Кузьменка, Ю. П. Лісовської, Н. І. Логінової, Ю. Є. Максименка, Ю. Є. Муравської (Якубівської), С. В. Северина, Є. Б. Тихомирова та інших.

Крім того, базовим підґрунтям для спостережень і висновків слугували узагальнення, висновки і дефініції щодо сутності та змісту інформаційних

відносин у монографічних роботах українських учених: Е. Е. Аблякімова («Адміністративно-правове забезпечення доступу до публічної інформації»), М. Ю. Кузнецової («Органи виконавчої влади України як суб'єкт інформаційних правовідносин»), О. В. Логінова («Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади»), Н. А. Литвин («Адміністративно-правове забезпечення інформаційної діяльності органів Державної фіскальної служби України»), Д. О. Маріц («Інформаційні правовідносини в Україні: теоретичні та практичні аспекти»), Д. О. Мороз («Адміністративно-правові засади діяльності податкової міліції як суб'єкта інформаційних відносин в Україні»), О. М. Селезньової («Теоретико-методологічні засади інформаційного права України як інтегрованої категорії»), І. М. Сопілко («Інформаційні правовідносини за участю органів державної влади України»), Т. В. Субіної («Адміністративно-правове забезпечення інформаційної безпеки в органах Державної податкової служби України»), Д. О. Петрова («Інформаційні правовідносини в Україні») та ін.

Окремі аспекти інформаційного забезпечення прикордонної безпеки досліджено у працях таких учених, як О. В. Ананьїн, С. Я. Білявець, О. В. Боровик, В. Л. Зьолка, В. А. Кириленко, М. О. Король, А. І. Коротушак, Д. А. Купрієнко, Ю. Б. Курилюк, М. М. Литвин, Р. М. Ляшук, Б. М. Марченко, О. Г. Мельников, А. Ф. Мота, В. С. Нікіфоренко, Р. В. Рачок, М. А. Стрельбіцький, Ю. П. Степанова, О. Є. Цевельов, О. Б. Фаріон, С. О. Філіппов, О. М. Царенко, С. І. Царенко та інших.

Теоретичні та методологічні напрацювання зазначених учених мають фундаментальний характер стосовно широкого кола питань інформаційних і прикордонних відносин, проте свідчать про потребу комплексного системного аналізу, узагальнення й обґрунтування напрямків удосконалення в їх інтегрованому поєднанні.

Аналіз норм українського законодавства, у тому числі відомчих нормативних актів ДПСУ, а також вивчення практики їх застосування в діяльності ДПСУ свідчать про наявність значної кількості прогалин у їх

правовому регулюванні. У сучасній науковій літературі відсутнє комплексне узагальнене дослідження особливостей інформаційних відносин у діяльності ДПСУ. Все це утворює суттєві перешкоди та проблеми, обумовлює новизну й актуальність обраної теми дисертаційного дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження спрямовано на реалізацію окремих положень Стратегії розвитку Державної прикордонної служби України, схваленої розпорядженням Кабінету Міністрів України від 23 листопада 2015 р. № 1189-р, Стратегії інтегрованого управління кордонами до 2025 року, схваленої розпорядженням Кабінету Міністрів України від 24 липня 2019 р. № 687-р., Концепції розвитку електронного урядування в Україні, схваленої розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р, Пріоритетних напрямків розвитку правової науки на 2016–2020 рр., схвалених постановою Загальних зборів Національної академії правових наук України від 3 серпня 2016 р.

Дисертація виконана в межах напрямів наукових досліджень Національної академії Державної прикордонної служби України імені Богдана Хмельницького (протокол № 10 від 24 лютого 2016 р.), науково-дослідних робіт Національної академії Державної прикордонної служби України імені Богдана Хмельницького: «Проблеми юридичної відповідальності за правопорушення у інформаційній сфері охорони інформаційних відносин у прикордонній сфері» (219-0107 І), «Методологічний аналіз інституту інформаційних відносин у прикордонній сфері» (219-0108 І). Тему дисертації затверджено рішенням вченої ради Національної академії Державної прикордонної служби України імені Богдана Хмельницького 20 грудня 2016 р. протокол № 10.

Мета і завдання дослідження. *Мета* дисертаційного дослідження полягає в комплексному аналізі теоретичних і організаційних засад нормативно-правового регулювання інформаційних відносин у діяльності ДПСУ, розробленні науково обґрунтованих висновків і пропозицій щодо підвищення ефективності інформаційних відносин і формулювання напрямків удосконалення їх нормативно-правового регулювання.

Досягнення поставленої мети передбачає розв’язання таких завдань:

– окреслити стан наукової розробленості інформаційних відносин у діяльності ДПСУ в сучасній правовій доктрині;

– сформулювати методологічну основу дослідження;

– визначити особливості та запропонувати поняття інформаційних відносин у діяльності ДПСУ;

– установити й проаналізувати елементи структури інформаційних відносин за участю ДПСУ;

– провести співвідношення змісту інформаційної безпеки і захисту інформації як складових прикордонної безпеки;

– окреслити правові підстави інформаційних відносин у діяльності ДПСУ;

– розкрити особливості правового режиму інформації з обмеженим доступом;

– виявити організаційні засади інформаційних відносин в управлінні оперативно-службовою діяльністю ДПСУ;

– узагальнити досвід інформаційної взаємодії в діяльності ДПСУ, визначити її напрямки;

– з’ясувати зміст і розкрити інформаційну відкритість в аспекті комунікації ДПСУ з інформаційною сферою суспільства;

– проаналізувати організаційно-правові аспекти, що впливають на забезпечення приватності в регулюванні інформаційних відносин;

– розглянути особливості порядку реалізації прав громадян на звернення у ДПСУ та запит на публічну інформацію;

– здійснити аналіз інформаційних загроз у сфері охорони державного кордону;

– охарактеризувати правові засоби охорони інформаційних відносин (кримінальна, адміністративна, дисциплінарна та цивільно-правова відповідальність) у функціонуванні ДПСУ;

– надати характеристику організаційно-правовим засадам забезпечення інформаційної безпеки в мережі Інтернет та в інформаційних системах ДПСУ;

– розробити й обґрунтувати рекомендації щодо підвищення ефективності інформаційних відносин у діяльності ДПСУ;

– запропонувати напрямки удосконалення нормативно-правового регулювання інформаційних відносин у діяльності ДПСУ.

Об'єкт дослідження – суспільні відносини, що виникають під час обігу інформації в діяльності Державної прикордонної служби України.

Предмет дослідження – теоретичні та організаційні засади нормативно-правового регулювання інформаційних відносин у діяльності ДПСУ.

Методи дослідження. Методологічна основа дослідження складається із сукупності філософських, загальнонаукових, галузевих і спеціально-наукових методів, які в комплексному застосуванні дали змогу досягти мети дослідження. *Діалектичний метод* надав можливість розглянути інформаційні відносини як комплексне правове явище у пошуку протилежностей сутності, елементах, ознаках у їх взаємозв'язку, досліджуваних відносин, їх аналіз і відмежування, систематизацію, розвиток, формування нових напрямків і тенденцій розвитку (підрозділи 1.1, 1.3, 1.4, 5.1, 5.2). *Феноменологічний метод* дав змогу вивчити окрему складову інформаційну) частину цілісної прикордонної безпеки – інформаційну діяльність, інформаційні повноваження ДПСУ як суб'єкта інформаційних відносин (підрозділи 1.4, 1.5, 2.3), сформувати бачення про нові уявлення, теоретичні аспекти, які утворюють такі інформаційні відносини (підрозділи 2.2, 3.1, 3.2). *Комунікативний метод* забезпечив можливість розглянути організаційно-правовий механізм досліджуваних відносин у взаємозв'язку та взаємодії суб'єктів, їх інформаційних прав та обов'язків у сфері охорони державного кордону (підрозділи 1.4, 2.4, 3.3). *Структурно-функціональний метод* використано для установлення складових структури інформаційних відносин у діяльності ДПСУ (суб'єкт, об'єкт, зміст), системи суб'єктів цих відносин (загальний, особливий (центральний), спеціальні) та взаємозв'язки між цими складовими (підрозділи 1.4, 2.4, 3.3). За допомогою *історичного методу* з'ясовано процес становлення та розвитку законодавчого регулювання інформаційних відносин у діяльності ДПСУ. Установлено

зародження нових видів інформаційної діяльності (інформаційно-аналітичний, кримінальний аналіз) і створення спеціальних суб'єктів ДПСУ (Центр кібербезпеки), котрі здійснюють таку діяльність залежно від обстановки та загроз у сфері охорони державного кордону України (підрозділи 1.4, 4.3). *Формально-логічний метод* надав можливості сформувати поняття, виділити види інформаційних відносин у діяльності ДПСУ, які раніше не були сформульовані у юридичній науці підрозділ 1.3). *Порівняльний метод* дозволив здійснити аналіз, систематизацію, виявлення спільного та відмінного між національним і зарубіжним регулюванням інформаційних відносин прикордонних органів, між ДПСУ та іншими органами державної влади України; визначити загальні особливості та відмінні риси досліджуваних відносин на підставі зіставлення однопорядкових понять, категорій, процесів і фактів; виявити вплив змін інформаційного законодавства на відповідні відносини (підрозділи 1.3, 2.4, 3.1, 3.2, 5.1). За допомогою *методу класифікації та групування* зроблено розмежування окремих категорій та явищ у межах дослідження за самостійними ознаками та властивостями на подібні й відмінні (запропоновано класифікацію інформаційних відносин, інформації у сфері діяльності ДПСУ, виділено правопорушення у межах кримінальної, адміністративної, дисциплінарної та цивільно-правової відповідальності, характерні для досліджуваної проблематики) (підрозділи 1.3, 1.4, 4.2). *Герменевтичний метод* застосовувався для пояснення термінів, текстів нормативно-правових актів, співвідношення їх із практичною діяльністю ДПСУ щодо участі в інформаційних відносинах (підрозділи 1.3, 1.4, 2.1, 2.2, 3.3, 5.2). *Метод спостереження* дозволив відслідковувати факти та події, пов'язані з реалізацією права на інформацію як у міжнародному, так і в загальнодержавному масштабі (а також розпорядником якої є ДПСУ), відзначати зміни в інформаційному законодавстві, у структурі та повноваженнях органів ДПСУ, що призначені для забезпечення інформаційної діяльності (усі розділи дисертації). *Анкетування* дозволило отримати об'єктивну інформацію від військовослужбовців ДПСУ (офіцерів і курсантів НАДПСУ, офіцерів органів та підрозділів охорони державного кордону) з питань правового регулювання обігу

інформації, забезпечення правового режиму інформації й інформаційної безпеки у ДПСУ та проблемних питань у сфері інформаційної діяльності (підрозділи 1.4, 1.5, 2.1, 2.2, 2.3, 3.1, 3.2, 4.2, 4.3, 5.1, 5.2). *Інтерв'ювання (*військовослужбовців-фахівців у сфері інформаційної діяльності та військовослужбовців, що виконують інші завдання, не пов'язані з цією сферою) утворило підґрунтя для емпіричного досвіду, перевірки та підтвердження теоретичних висновків дослідження (підрозділи 3.2, 3.3, 4.3, 5.1). *Контент-аналіз* нормативно-правових актів, рішень судових органів, дослідження подібних та аналогічних питань у науковій доктрині дозволив з'ясувати і виявити загальні закономірності досліджуваних відносин (усі розділи дисертації). *Статистичний метод* надав можливості проаналізувати рівень довіри громадян до ДПСУ, визначити місце Адміністрації ДПСУ у рейтингу інформаційної прозорості органів влади, кількість осіб, що перетинають державний кордон, кількість запитів на інформацію та звернень, що надходять до ДПСУ (підрозділи 3.1, 3.3, 5.1). За допомогою *методу моделювання* підготовлено проєкти змін до законів України «Про Державну прикордонну службу України» і «Про прикордонний контроль», до наказу Адміністрації Державної прикордонної служби України «Відомості про осіб, які перетнули державний кордон України»; складено алгоритм формування інформаційної культури у ДПСУ, Концепцію інформаційного забезпечення ДПСУ, розроблено методичні рекомендації щодо роботи зі зверненнями громадян до ДПСУ (підрозділи 5.1, 5.2). *Метод прогнозування* використано для формування рекомендацій щодо підвищення ефективності досліджуваних відносин, напрямків удосконалення їх нормативно-правового регулювання, висунення та обґрунтування Концепції інформаційного забезпечення ДПСУ, структури Інформаційного кодексу України (підрозділи 5.1, 5.2).

Нормативно-правову основу дослідження становлять Конституція України, закони України, укази Президента України, постанови Кабінету Міністрів України та інші нормативно-правові акти, які регулюють питання інформаційних відносин у сфері діяльності ДПСУ, а також міжнародно-правові акти.

Емпіричною базою дослідження є узагальнення практики застосування чинного законодавства, рішення Колегії Адміністрації ДПСУ за 2018–2019 роки, щорічні (2014–2019) статистичні дані звернень громадян до ДПСУ, звіти щодо роботи із запитами на публічну інформацію у ДПСУ (2011–2019), аналітичні довідки за результатами моніторингу вебсайтів органів виконавчої влади (2019–2020), дані загальнонаціонального дослідження соціологічної служби Центру Разумкова (2019), кількісні дані щодо пасажиропотоку осіб, які перетинають державний кордон України, та затриманих на державному кордоні нелегальних мігрантів (2017–2019), матеріали статистичних даних щодо кількості дзвінків, які надійшли до служби «Довіра» (2016–2019), судова практика ЄСПЛ, судові рішення з Єдиного державного реєстру судових рішень, результати анкетування, проведеного серед персоналу ДПСУ в кількості 620 осіб, реєстр повідомлень щодо операцій з опрацювання персональних даних FRONTEX, участь у міжнародному вебінарі EU Project «Pravo-Justice» «Захист персональних даних: досвід ЄС та України» (16.07.2020), курс «Персональні дані» Національної онлайн-платформи з цифрової грамотності (електронний сертифікат Міністерства цифрової трансформації України від 31.07.2020 р.), наукові, навчальні та довідкові видання.

Дослідження ґрунтувалось на власному службовому досвіді авторки (проходження служби в Державній прикордонній службі України – 22 роки).

Наукова новизна одержаних результатів полягає в тому, що дисертація є одним із перших у вітчизняній юридичній науці комплексним і системним монографічним дослідженням, у контексті якого обґрунтовано теоретичні й практичні проблеми розвитку нормативно-правового регулювання інформаційних відносин у діяльності ДПСУ. У дисертації обґрунтовано низку важливих понять, положень, висновків і пропозицій, які становлять наукову новизну та практичну значущість, основними з яких є такі:

уперше:

– запропоновано авторські визначення понять «інформаційні відносини у діяльності Державної прикордонної служби України», «інформаційна безпека у

прикордонній сфері», «інформаційна діяльність Державної прикордонної служби України», «нормативно-правове регулювання інформаційної складової у діяльності ДПСУ», «правовий режим інформації з обмеженим доступом у діяльності Державної прикордонної служби України»;

– встановлено джерела інформаційного наповнення управлінського рішення в охороні державного кордону: інформаційно-нормативне, інформаційно-управлінське, оперативно-інформаційне, інформаційно-аналітичне, інформаційно-практичне, оперативно-розшукове, інформаційно-консультативне. Розмежовано внутрішні та зовнішні фактори, що впливають на прийняття рішення начальника органу охорони державного кордону України;

– розкрито окремі особливості механізму опрацювання персональних даних і захисту інформаційних прав у діяльності Європейського агентства прикордонної та берегової охорони (FRONTEX), сформовано пропозиції стосовно адаптації їх у діяльності ДПСУ;

– запропоновано конкретні напрямки, спрямовані на вдосконалення інформаційних відносин у діяльності ДПСУ як складової частини системи охорони державного кордону України, до яких віднесено: розвиток відкритості та доступності в діяльності ДПСУ; електронного урядування та електронної ідентифікації; безпеки інформаційних систем ДПСУ; інформаційної культури персоналу ДПСУ;

– підготовлено Методичні рекомендації по роботі зі зверненнями громадян у ДПСУ, з метою сприяння посадовим особам ДПСУ, до обов’язків яких входить робота зі зверненнями громадян, більш чітко й ефективно організувати цю роботу відповідно законодавству України;

– обґрунтовано Алгоритм формування інформаційної культури у ДПСУ, що передбачає розвиток інформаційної культури представників ДПСУ, підвищення обізнаності з теоретичних засад у сфері формування й обігу інформації з урахуванням особливостей завдань, що виконує ДПСУ, з подальшим екстраполюванням у практичну діяльність;

– у складі ДПСУ запропоновано виокремити організаційні структури, призначені для захисту персональних даних, із залученням фахівців юридичних спеціальностей, а також запровадити ведення обліку опрацювання персональних даних;

– підготовлено авторську Концепцію інформаційного забезпечення ДПСУ, що сприятиме підвищенню ефективної реалізації інформаційних відносин та інформаційної безпеки у сфері діяльності ДПСУ;

– сформульовано конкретні пропозиції щодо внесення змін і доповнень до нормативно-правових актів, зокрема до законів України «Про Державну прикордонну службу України» і «Про прикордонний контроль», до наказу Адміністрації Державної прикордонної служби України «Про затвердження Положення про базу даних «Відомості про осіб, які перетнули державний кордон України» у частині, пов'язаній з обігом інформації у сфері охорони державного кордону;

удосконалено:

– теоретичні положення щодо розуміння понять «інформаційні відносини», «володіння інформацією», «офіційна інформація», «інформаційно-правовий статус», «інформаційна політика держави», «інформаційна взаємодія», «інформаційна сфера», «інформаційна відкритість», «інформаційні загрози»;

– критерії класифікації інформаційних відносини та інформації з урахуванням специфіки завдань, що реалізуються ДПСУ;

– наукові підходи до характеристики структури й особливостей інформаційних відносин у діяльності ДПСУ;

– розмежування понять «безпека державного кордону» та «прикордонна безпека»; запропоновано розглядати «безпеку державного кордону» як незмінність лінії державного кордону та надійне збереження територіальної цілісності держави, зазначено, що «прикордонна безпека» охоплює ширші безпекові заходи не тільки на державному кордоні, але і вздовж нього, спрямовані на недопущення та усунення загроз, наслідком чого є безпека державного кордону та реалізація прав усіх суб'єктів, пов'язаних із проходженням

державного кордону. Запропоновано співвідносити «безпеку державного кордону» та «прикордонну безпеку» як частину та ціле відповідно;

– наукові положення щодо елементів правового режиму інформації з обмеженим доступом;

– напрямки, рівні, коло питань, що перебувають у площині інформаційної взаємодії ДПСУ із взаємодіючими прикордонними органами суміжних держав і суб'єктами інтегрованого управління кордонами;

– складові елементи, що відображають інформаційну відкритість ДПСУ з інформаційною сферою суспільства, а саме: врегульовані механізми отримання інформації; оприлюднення інформації у прикордонній сфері через доступні процедури; простота та доступність електронного урядування у ДПСУ; чітке розмежування інформації за порядком доступу до неї; рівень інформаційної культури;

набули подальшого розвитку:

– доведено, що досліджувані інформаційні відносини є складовою системи охорони державного кордону та містять два основних напрями: внутрішньовідомчі інформаційні відносини у діяльності ДПСУ та зовнішні інформаційні відносини ДПСУ з інформаційною сферою суспільства;

– система методів пізнання, які є теоретичною основою дослідження інформаційних відносин у діяльності ДПСУ через призму онтологічного, гносеологічного, аксіологічного та праксеологічного сприйняття дійсності;

– наукові положення щодо визначення інформаційно-правового статусу загальних і спеціальних структурних підрозділів ДПСУ;

– наукові уявлення про особливості механізмів звернення та запиту на публічну інформацію в діяльності ДПСУ;

– аналіз сучасних інформаційних загроз у діяльності ДПСУ дозволив диференціювати їх за такими критеріями: за локалізацією, за наміром, залежно від процесу інформаційної діяльності, за характером вияву, за способом впливу, за способом заподіяння шкоди; обґрунтувати організаційно-правові засади розвитку інформаційної безпеки;

– систематизація інформаційного законодавства у межах Інформаційного кодексу України (запропоновано авторське бачення його структури). Виокремлення статей КК України і КУпАП, що передбачають відповідальність за інформаційні правопорушення у межах окремих розділів;

– пропозиції щодо впровадження у систему освіти Національної академії Державної прикордонної служби України імені Богдана Хмельницького навчальних дисциплін для юридичних спеціальностей – «Інформаційне право» та «Інформаційна діяльність Державної прикордонної служби України», для усіх інших спеціальностей – «Правові основи інформаційної безпеки», що сприятиме удосконаленню нормативно-правового регулювання відносин, об'єктом яких є інформація, в реалізації завдань, що покладаються на ДПСУ.

Практичне значення одержаних результатів полягає в тому, що вони мають як теоретичне, так і практичне значення, а сформульовані теоретичні положення, висновки, пропозиції та рекомендації були використані й можуть у подальшому використовуватись:

– *у науково-дослідній сфері* – для подальших наукових досліджень загальнотеоретичних питань удосконалення правового регулювання відносин, об'єктом яких є інформація у сфері функціонування ДПСУ *(акт впровадження в освітній та науково-дослідній діяльності Національної академії Державної прикордонної служби України імені Богдана Хмельницького від 30 червня 2020 р. № 31/86)*;

– *у нормотворчій сфері* – під час підготовки змін і доповнень до чинного законодавства, зокрема законів України «Про Державну прикордонну службу України», «Про прикордонний контроль» (*акт впровадження Комітету Верховної Ради України з питань правової політики від 30 вересня 2020 року № 04-26/17-2020/172667(222259*), наказу Адміністрації Державної прикордонної служби України від 25.06.2007 № 472 «Про затвердження Положення про базу даних «Відомості про осіб, які перетнули державний кордон України»; при опрацюванні проектів наказів та інструкцій, пов'язаних з обігом інформації у сфері охорони державного кордону (*акт впровадження Адміністрації Державної*

прикордонної служби України від 26 червня 2020 року (Вх. № 37374/0/3-20), акт впровадження Регіонального управління Морської охорони Адміністрації Державної прикордонної служби України від 12 червня 2020 року);

– *у правозастосовній діяльності* – для вдосконалення практики застосування норм, що врегульовують обіг інформації в діяльності ДПСУ, для ефективності впровадження державної інформаційної політики, забезпечення відкритості та прозорості в діяльності ДПСУ, підвищення ефективності отримання, опрацювання та захисту інформації, розпорядником якої є ДПСУ, загалом сприятимуть підвищенню прикордонної безпеки й забезпеченню розвитку інформаційної складової частини системи охорони державного кордону України (*акт впровадження Адміністрації Державної прикордонної служби України від 26 червня 2020 року (Вх. № 37374/0/3-20), акт впровадження Регіонального управління Морської охорони Адміністрації Державної прикордонної служби України від 12 червня 2020 року, акт впровадження Львівського прикордонного загону Західного регіонального управління від 26 травня 2020 року № 44/5519*);

– *в освітньому процесі* – теоретичні положення, висновки та пропозиції можуть бути використані при викладанні таких навчальних дисциплін, як «Актуальні проблеми інформаційного права», «Теорія держави і права», «Інформаційна політика та інформаційна безпека», «Адміністративне право», «Кримінальне право» *(акт впровадження в освітню та науково-дослідну діяльність Національної академії Державної прикордонної служби України імені Богдана Хмельницького від 30 червня 2020 р. № 31/86)*.

Особистий внесок здобувача. Дисертаційне дослідження виконано автором самостійно, основні положення, висновки, рекомендації та пропозиції, що виносяться на публічний захист, обґрунтовано дисертантом на підставі особистого теоретичного та практичного досвіду й наукового пошуку. При використанні матеріалів інших дослідників зроблено відповідні посилання. Ідеї, що належать співавторам, у дисертації не використовувалися.

У колективній монографії «Low and Border: Addressing Security Threats at the Ukrainian Border» дисертантом розроблено основні напрямки удосконалення інформаційних відносин у діяльності ДПСУ.

У науковій статті «Інформаційна безпека держави у прикордонній сфері як об'єкт державної зради» внесок автора полягає у висвітленні суттєвих змістовних характеристик прикордонної інформаційної безпеки як об'єкта кримінально-правового посягання, у визначенні поняття «інформаційна безпека», формулюванні висновків.

У статті «Правовий режим інформації з обмеженим доступом у діяльності Державної прикордонної служби України» внесок автора полягає в аналізі й узагальненні характеристики правового режиму інформації з обмеженим доступом, відокремленні елементів правового режиму інформації з обмеженим доступом у діяльності ДПСУ.

У науковій статті «Питання удосконалення впровадження електронного урядування у Державній прикордонній службі України» внесок дисертанта полягає у визначенні особливостей електронного урядування, окресленні шляхів вирішення проблемних питань щодо впровадження електронного урядування у ДПСУ.

У науковій статті «Особливості застосування дисциплінарної відповідальності за порушення інформаційного законодавства у діяльності Державної прикордонної служби України» внесок автора полягає у систематизації інформаційних правопорушень у межах КУпАП, за які військовослужбовці несуть дисциплінарну відповідальність, у визначенні особливостей дисциплінарної відповідальності військовослужбовців за інформаційні правопорушення, у формулюванні напрямків, що сприятимуть підвищенню правового забезпечення інформаційних відносин та ефективності правового впливу.

У науковій статті «Проблеми та перспективи розвитку консультаційної роботи Контактного центру Державної прикордонної служби України» дисертантом надано теоретичне обґрунтування проблем, що виникають при

здійсненні консультативної роботи Контактного центру, запропоновано шляхи їх вирішення.

У науковій статті «Результативність та ефективність в діяльності органів охорони державного кордону України» проаналізовано й обґрунтовано критерії оцінки ефективності та результативності в діяльності органів охорони державного кордону.

У тезах доповіді «Критерії класифікації злочинів у сфері службової діяльності» розглянуто підстави для критеріїв класифікації злочинів у сфері службової діяльності.

Апробація матеріалів дисертації. Результати наукового дослідження були оприлюднені на міжнародних і всеукраїнських наукових та науково-практичних заходах, зокрема: «Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України» (м. Хмельницький, 10 грудня 2015 р.), «Кібербезпека України: правові та організаційні питання» (м. Одеса, 21 жовтня 2016 р.), «Інформаційна безпека: європейські орієнтири та перспективи для України» (м. Харків, 25 листопада 2016 р.), «Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України» (м. Хмельницький, 8 грудня 2016 р.), «Молодіжний науковий юридичний форум» (м. Київ, 18 травня 2017 р.), «Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України» (м. Хмельницький, 2 листопада 2017 р.), «Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності» (м. Хмельницький, 2 березня 2018 р.), «Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи» (м. Одеса, 13-14 вересня 2018 р.), «Освітньо-наукове забезпечення складових сектору безпеки і оборони України» (м. Хмельницький, 15 листопада 2018 р.), «Актуальні проблеми кримінально-правового, кримінально-процесуального та криміналістичного забезпечення безпеки України» (м. Дніпро, 30 листопада 2018 р.), «Кібербезпека України: правові та організаційні питання» (м. Одеса, 30 листопада 2018 р.), «Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової

діяльності» (м. Хмельницький, 1 березня 2019 р.), «Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи» (м. Одеса, 13-14 вересня 2019 р.), «Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України»(м. Хмельницький, 22 листопада 2019 р.), «Стан та перспективи розвитку адміністративного права України» (м. Одеса, 23 жовтня 2019 р.), «Пріоритетні напрямки розвитку та реформування правоохоронних органів» (м. Херсон, 31 жовтня 2019 р.), «Військова освіта і наука: сьогодення та майбутнє» (м. Київ, 29 листопада 2019 р.), «Українська мова в юриспруденції: стан, проблеми, перспективи» (м. Київ, 28 листопада 2019 р.), «Кібербезпека України: правові та організаційні питання» (м. Одеса, 22 листопада 2019 р.), «Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи» (м. Одеса, 10-11 вересня 2020 р.), «Стратегічні комунікації у сфері забезпечення національної безпеки і оборони : проблеми, досвід, перспективи» (м. Київ, 1 жовтня 2020 р.), «Українська мова в юриспруденції: стан, проблеми, перспективи» (м. Київ, 25 листопада 2020 р.), «Актуальні проблеми інтелектуального, інформаційного та ІТ права» (м. Львів, 12 листопада 2020 р.).

Публікації. Основні теоретичні положення, висновки та пропозиції викладено в 55 наукових публікаціях, з яких: дві монографії (одна одноосібна, одна колективна англійською мовою), 29 статтей – у фахових виданнях (23 з яких опубліковано у фахових виданнях України, 5 – у наукових періодичних виданнях інших держав (одна англійською мовою), розділ у книзі (англійською мовою), 12 – у виданнях, які включені до міжнародних наукометричних баз), одна публікація, яка додатково відображає результати дисертаційного дослідження, а також у 23 тезах доповідей у збірниках матеріалів наукових конференцій.

Структура й обсяг дисертації. Дисертація складається зі вступу, п’яти розділів, які об’єднують 17 підрозділів, висновків, 19 додатків, що розміщені на 84 сторінках, і списку використаних джерел (518 найменувань). Загальний обсяг дисертації становить 566 сторінки, з яких 386 сторінок основного тексту.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНА ХАРАКТЕРИСТИКА ІНФОРМАЦІЙНИХ ВІДНОСИН У ДІЯЛЬНОСТІ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

1.1 Стан наукових досліджень за темою дослідження

Розвиток сучасного інформаційного суспільства, впровадження на основі європейських практик нової системи охорони державного кордону, виникнення нових інформаційних загроз у прикордонній сфері зумовили необхідність розв'язання наукової проблеми у межах окремого напрямку – інформаційних відносин у діяльності Державної прикордонної служби України (далі – ДПСУ). Зміст проблеми спричинений фактичною відсутністю комплексного дослідження теоретичних та організаційних засад цих відносин й у зв'язку з цим породжує необхідність в отриманні нових знань про об'єкт дослідження, виявлення протиріч та формулювання шляхів розвитку (удосконалення) інформаційних відносин у діяльності ДПСУ.

Ураховуючи те, що сутність нормативно-правового регулювання зводиться до упорядкування суспільних відносин, важливо акцентувати увагу на з'ясуванні стану дослідження, особливостях, характеристиці та змісті інформаційних відносин у діяльності ДПСУ.

Отже, з урахуванням комплексного та міжгалузевого характеру проблем, що окреслені у роботі, авторкою досліджені наукові результати фахівців з різних галузей, а саме: теорія держави і права, державне управління, адміністративне, інформаційне, цивільне, кримінальне право, теорія прикордонного управління, прикордонної безпеки тощо.

Якщо XIX століття називали століттям виробництва, XX – століттям управління, то XXI століття, зауважує І. В. Арістова, дійсно є століттям інформації, а інформаційні процеси постають предметом свідомої, цілеспрямованої та

науково обґрунтованої діяльності. Право при цьому відіграє вагоме значення у свідомому проектуванні інформаційних процесів, за допомогою якого не лише регулюються відносини, що складаються, але й відбувається розширення сфери інформаційної діяльності, яке зумовлено суспільними потребами. Тим самим право позначається на втіленні інформаційних процесів, визначаючи та підтримуючи ті напрями, які формують інформаційне суспільство [1, с. 4].

Значний розвиток наукових досліджень як з інформаційних, так і прикордонних відносин сьогодні дозволив генерувати попередньо отримані знання (у вже існуючих дослідженнях) на якісно нові закономірності розвитку інформаційних відносин у межах реалізації форм оперативно-службової діяльності ДПСУ за такими вагомими напрямками: державна інформаційна політика; теорія інформаційних відносин; інформаційне забезпечення в діяльності ДПСУ. Проаналізуємо кожен із них.

Державна інформаційна політика

Інформаційні відносини в діяльності ДПСУ виникають, розвиваються та змінюються відповідно до основних тенденцій державної інформаційної політики. Тільки держава та її правові важелі регулювання, закладені у чинних нормативно-правових актах, визначають фундаментальні засади правових відносин, що стосуються реалізації інформації. Багатоаспектне дослідження проблеми формування і здійснення державної інформаційної політики та якісне забезпечення державного управління інформаційною сферою в умовах становлення та розвитку інформаційного суспільства здійснено І. В. Арістовою у дисертації «Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади» (2002 р.) [2, с. 8].

Авторка вперше запропонувала розглядати державну інформаційну політику в контексті теорії управління як державно-правове явище, динамічний двоєдиний процес – формування (як вироблення стратегічного курсу держави в інформаційній сфері) та реалізація (як державне управління національною інформаційною сферою) [2, с. 8]. У цьому контексті запропоновано суб’єктно-об’єктний підхід до аналізу розуміння змісту державного управління

національною інформаційною сферою, де об’єктом визначена національна інформаційна сфера, суб’єктом – система органів державної влади, що перебувають в інтегративному взаємозв’язку. Сутність інформаційних відносин обґрунтовано як система виробництва – розповсюдження – споживання. Запроваджена ідея поступового перетворення управлінських відносин в інформаційні сприяла доктринальному розширенню інформаційних відносин [2, с. 8].

Запропонований у роботі системний підхід до інформаційної сфери завдяки таким елементам: об’єкт управління – національна інформаційна сфера (єдиний інформаційний простір України); суб’єкт управління – відповідні державні органи всіх гілок влади; взаємозв’язки між суб’єктом та об’єктом управління [2, с. 30] дозволяє розвивати її положення у діяльності ДПСУ.

І. В. Арістова інформаційні відносини розглядає як інформаційні зв’язки між суб’єктами політичної системи суспільства, держави, що виникають під час одержання, використання, зберігання та споживання інформації [3, с. 172]. Таке розуміння виключає інших суб’єктів інформаційних відносин (фізичних та юридичних осіб) та проектує суспільні відносини з приводу інформації на інформаційні зв’язки, залишаючи поза увагою змістовне відображення прав та обов’язків з приводу інформації як законну можливість реалізації та задоволення інформаційного інтересу та потреби.

Вперше К. І. Бєляковим (у 2009 р.) у дисертації «Організаційно-правове та наукове забезпечення інформатизації в Україні: проблеми теорії та практики» було досліджено та обґрунтовано стратегії і тактики державного управління процесами інформатизації суспільства та інформаційною діяльністю в Україні (державної інформаційної політики), розбудову національного інформаційного законодавства, забезпечення інформаційної безпеки як складової національної безпеки, розробку ефективних засобів та методології протидії інформаційним деліктам, розвитку інформаційних ресурсів та процесів, їх цивілізованої інтеграції у всесвітній інформаційний простір, становленню вітчизняного інформаційного ринку і т. ін. [4, с. 8].

Науковець розглядає державну інформаційну політику як регулюючу діяльність державних органів, спрямованої на розвиток національної інформаційної інфраструктури, що охоплює не тільки телекомунікації, інформаційні системи і засоби масової інформації, а всю сукупність виробництв і відносин, пов'язаних із створенням, збереженням, обробкою, демонстрацією, передачею інформації у всіх її видах – інформаційними процесами та технологіями, створення правової бази інформатизації – законодавства, спроможного регулювати виникаючі в суспільстві інформаційні відносини (інформаційне законодавство) [4, с. 14].

Цікавою на наш погляд, є пропозиція К. І. Бєлякова про введення нової галузі знань юридичного циклу – правничої інформаціології, під якою науковець пропонує розглядати міжгалузевий напрям науки про інформаційно-комунікативні процеси та соціально-правові відносини, які виникають при цьому, роль та місце юридичної науки, практики та соціального управління у процесах інформатизації суспільства, інноваційні зміни у правових явищах, породжених ними суспільних наслідків, процесів, тенденцій та відносин, удосконалення засобів і методів адміністративної діяльності та юридичної практики за допомогою інформаційних технологій та ресурсів [4, с. 7]. Така позиція цілком логічна, обґрунтована сучасними темпами розвитку, реаліями та викликами інформаційного суспільства, а також інноваційними процесами.

Загальні тенденції концептуальних і системних теоретико-правових засад формування та реалізації державної інформаційної політики в умовах глобальної інформатизації та розвитку інформаційного суспільства, запровадження концепції е-урядування з обґрунтуванням теоретико-методологічних засад і напрямів підвищення ефективності її правового регулювання досліджені І. М. Сопілко у докторській дисертації «Правові засади державної інформаційної політики України» (2014 р.) [5] та розвинуті у монографії «Правові засади розвитку інформаційного суспільства в Україні» (2015 р.) [6].

У роботі «Правові засади державної інформаційної політики України» державна інформаційна політика розглядається у різних ракурсах: широкому,

вузькому, теоретичному та практичному. Ціннісними для нашого дослідження є зроблені науковцем узагальнення, що державна інформаційна політика це:

процес вироблення, реалізації та контролю за реалізацією та удосконаленням державної стратегії і тактики в інформаційній сфері, що ґрунтується на загальних принципах розвитку ефективного інформаційного суспільства та е-урядування, інформаційної взаємодії державних і недержавних інституцій відповідно до національних інформаційних інтересів;

діяльність уповноважених органів державної влади й управління, громадських організацій, посадових осіб та окремих громадян, яка визначає цілі, функції, принципи, пріоритети інформаційної політики, методи та засоби їх забезпечення;

інформаційна ідеологія держави, що охоплює ідеї, цілі, завдання, функції, методи та принципи, теорії, стратегії, концепції, доктрини, програми тощо, закріплені переважно у формі нормативно-правових актів. У практичному аспекті пропонується під державною інформаційною політикою розуміти діяльність державних і недержавних інституцій зі здійснення ефективного інформаційного впливу на всі сфери суспільного життя [5, с. 14].

Інформаційні відносини у діяльності ДПСУ є невід'ємною частиною державної інформаційної політики (є її продовженням, втіленням засадничих вимог держави в конкретних відносинах), функціонування інформаційного суспільства, що ґрунтується на засадничих вимогах нормативно-правових актів та посідає відповідну нішу в реалізації інформаційних інтересів усіх суб'єктів відповідних відносин прикордонної сфери.

У ході роботи над дослідженням нами також було приділено увагу науковій розробці В. О. Негодченка «Адміністративно-правове забезпечення державної інформаційної політики органами Національної поліції України» (2017 р.), у якій науковець зосередив увагу на суспільних відносинах, що виникають під час діяльності органів Національної поліції України щодо забезпечення державної інформаційної політики [7].

У дисертації сформульовані основні ознаки, які притаманні формам діяльності органів поліції щодо забезпечення державної інформаційної політики: 1) мають публічно-правову природу; 2) регулюються нормами адміністративного та інформаційного права; 3) забезпечуються примусовою силою держави; 4) це завжди зовнішні дії, спрямовані на забезпечення державної інформаційної політики; 5) мають чітко визначену процесуальну форму; 6) тягнуть настання правових наслідків; 7) є обов'язковими для виконання [7, с. 8].

Результатом здійсненого аналізу виступає запропоноване В. О. Негодченком поняття «суб'єкт забезпечення державної інформаційної політики», під яким пропонується розуміти носія передбачених адміністративно-правовими нормами прав і обов'язків щодо формування в межах наданих повноважень державної інформаційної політики та реалізації (з використанням відповідних форм і методів) її положень у сфері забезпечення інтересів людини, суспільства та держави в інформаційній сфері, сприяння розвитку інформаційного простору та забезпечення інформаційної безпеки [7, с. 8]. Виходячи з цього, ДПСУ виступає суб'єктом забезпечення державної інформаційної політики у прикордонній сфері.

Автором запропоновано поділяти інформацію з обмеженим доступом у системі Національної поліції України, на службову та таємну; окреслено основні сфери діяльності органів поліції, у яких циркулює службова та таємна інформація, сформульовано пропозиції щодо недопущення порушень режиму її обігу [7, с. 8]. При цьому поза увагою залишились положення ч. 1 ст. 21 Закону України «Про інформацію», у якому до інформації з обмеженим доступом належить також і конфіденційна інформація. Адже інформація про військовослужбовців і персонал ДПСУ, а також інформація про інших фізичних осіб, що перебуває у відомчому обігу у межах повноважень ДПСУ, належить до конфіденційної.

В. О. Негодченко робить висновок, що на законодавчому рівні недостатньо вичерпно сформульовано перелік напрямів державної інформаційної політики. Викладений у Законі України «Про інформацію» такий перелік не повною мірою враховує весь спектр загроз інформаційній сфері (зокрема, зумовлених веденням

інформаційно-психологічної та торговельно-економічної війни, збройної агресії проти України). Саме тому, науковець запропонував авторське бачення основних напрямків державної інформаційної політики, а саме: 1) дотримання інформаційних прав громадян, створення гарантій їх забезпечення, інформаційної освіти населення; 2) інформатизація органів державної влади та органів місцевого самоврядування, налагодження електронних форм взаємодії з населенням; 3) впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя; 4) забезпечення національної безпеки в інформаційній сфері, зокрема шляхом створення ефективного сектору безпеки і оборони та підвищення обороноздатності держави; 5) захист інформації та інформаційних ресурсів, зокрема в частині забезпечення кібербезпеки; 6) розвиток незалежних засобів масової інформації та формування високоякісного медіапростору. Наведено перелік заходів, що мають реалізовуватися у рамках кожного окремого напряму державної інформаційної політики [7, с. 7].

У напрямку вдосконалення державної інформаційної політики дослідник аргументує необхідність прийняття Закону України «Про державну інформаційну політику», орієнтованого саме на вироблення адміністративно-правового механізму формування та реалізації державної інформаційної політики, у якому мають знайти своє відображення як напрями такої політики, так і заходи, спрямовані на їх реалізацію [7, с. 15].

В. О. Негодченко визначив систему суб’єктів забезпечення державної інформаційної політики в Україні, поділивши їх на загальних суб’єктів – вищі органи державної влади, координаційні та консультативні органи та спеціальних суб’єктів, які складаються з центральних органів виконавчої влади та їх територіальних підрозділів, до яких відніс і ДПСУ. При цьому обґрунтував на прикладі органів поліції, що особливе місце окремого органу виконавчої влади в системі інших суб’єктів забезпечення державної інформаційної політики зумовлено специфікою їх адміністративно-правового статусу [7, с. 16].

Науковець визначив, що сутність взаємодії органів поліції з іншими суб’єктами забезпечення інформаційної політики полягає у спільному визначенні

стратегічних національних інтересів України в інформаційній сфері, виробленні системи заходів щодо забезпечення національної безпеки в інформаційній сфері, веденні постійного моніторингу впливу на національну безпеку процесів, що відбуваються в інформаційній сфері, за результатами якого повинні прийматися рішення про вжиття відповідних заходів реагування [7, с. 10]. Хоча, дозволимо собі зауважити, що питання формування національної стратегії перебувають у віданні вищих органів державної влади, і у такому випадку ці органи можуть очікувати за відповідними запитами від центральних органів влади консультування чи уточнення окремих питань у межах відання останніх. Щодо взаємодії центральних органів виконавчої влади, то це швидше стосується забезпечення реалізації державної інформаційної політики в межах спільного погодження та здійснення окремих її напрямків у межах відомчих повноважень.

Робота Г. Г. Почепцова, С. А. Чукута «Інформаційна політика» (2006 р., 2008 р.) присвячена комплексному дослідженню та висвітленню сутності й основних складових сучасної інформаційної політики, у якій розкриваються питання побудови інформаційного суспільства, проблеми правового регулювання інформаційної сфери, становлення та впровадження системи електронного урядування з урахуванням зарубіжного та вітчизняного досвіду, технологія використання інформаційних стратегій та ведення сучасних інформаційних війн [8].

Інформаційна політика визначає закони функціонування інформаційної сфери. Розуміючи масштабність і важливість останньої, автори навчального посібника у 2006 році написали про майбутню війну як про війну знань і використання маніпулятивних технологій. «Супротивник буде завжди приймати невірні рішення, якщо він буде базуватися на неправильних знаннях». Один із піднапрямків цього напрямку називається «управління сприйняттям»: ми не змінюємо об’єкти, оскільки в багатьох випадках це неможливо, а змінюємо їх сприйняття» [9].

Важливою є теза, що інформаційна сфера стала сьогодні базовою для розвитку всіх інших сфер: економічної, політичної, військової, дипломатичної

[8, с. 29], безперечно й прикордонної, ключовою у якій є забезпечення надійної охорони та захисту державного кордону України.

Г. Г. Почепцов, С. А. Чукут, розглядаючи масштабно інформаційну політику, зазначають, що інформаційна сфера створює цілі країни, вона допомагає їхньому економічному та політичному становленню. Вона збільшує силу сильних, применшує слабкості слабких. Інформаційна сфера стратегічно вигідніша за будь-яку іншу. Вона дає можливість, вкладаючи менший ресурс, отримувати більший результат. Світ починається і закінчується інформацією [8, с. 34].

Пріоритетним для інформаційної безпеки, роблять акцент науковці, є аналіз загроз, які можуть виникнути в інформаційній сфері, і створення умов для запобігання їхньому виникненню. У першу чергу це стосується різноманітних технічних аспектів передавання й обробки інформації [8, с. 12]. Так, саме аналіз ризиків, запроваджений у 2006 році у діяльності ДПСУ, який становить комплекс протидії загрозам на державному кордоні, показав високі практичні результати, що ефективно реалізуються шляхом профілювання ризиків, а у поєднанні з відповідними заходами на регіональному та територіальному рівнях значно підвищує рівень прикордонної безпеки [10].

Отже, наукові напрацювання з інформаційної політики держави дозволили встановити, що вона є визначальним вектором формування, реалізації інформаційних відносин у діяльності ДПСУ. Основні її тенденції впливають на конкретні цілі, межі інформаційних прав та обов’язків, дії, поведінку, взаємозв’язки суб’єктів таких відносин. В основних засадах державної інформаційної політики закладений очікуваний результат, який у загальному зводиться до врегулювання інформаційних відносин, забезпечення виконання завдань, покладених на ДПСУ, інформаційної безпеки громадян і держави.

Теорія інформаційних відносин

Формування теоретико-правових основ інформаційних відносин у сучасному ракурсі здійснено колективом авторів: В. Д. Гавловським, В. В. Гриценко, В. С. Цимбалюком та ін. Результатом спільної роботи стала

перша наукова праця «Інформаційне право» (2004 р.), у якій розглядаються проблеми визначення змісту, сутності й особливостей інформаційного права з урахуванням його об’єкта – суспільних інформаційних відносин. У роботі розроблені такі визначення, основні поняття та категорії: інформаційне суспільство; система правового регулювання соціальних інформаційних відносин; сутність теорії інформаційної безпеки та її напрямки; інформаційна культура. Крім того, досліджена роль інформації в суспільних відносинах та органів публічної влади у формуванні державної інформаційної політики, висвітлені базові принципи правового регулювання суспільних відносин в умовах формування інформаційного суспільства [11].

Не менш важливе значення у розвитку теорії інформаційних відносин мають напрацювання у роботі А. І. Марущака «Інформаційне право: доступ до інформації» (2007 р.), у якій акцентується увага: на теоретичних основах і практичних засадах реалізації права громадян на доступ до інформації; досліджено гарантії реалізації права громадян на доступ до інформації; процедури отримання громадянами інформації (доступу до інформації про діяльність органів державної влади, приватної інформації про фізичну особу) тощо [12].

Цікавим, на нашу думку, є навчальний посібник «Теорія держави і права» (2017 р.) О. О. Тихомиров, М. М. Мікуліна, Ю. А. Іванова та ін., у якому поряд із традиційними темами розглянуті ті, які відображають наявні та перспективні зміни в теорії держави і права, спричинені розвитком інформаційного суспільства та потребами забезпечення інформаційної безпеки. Зокрема, акцентована увага на таких питаннях, як «електронне урядування» в механізмі держави; право в інформаційному суспільстві; інформаційне право і законодавство в Україні; особливості інформаційних правовідносин; особливості інформаційних правопорушень; інформаційні права людини; правові засади інформаційної діяльності органів влади в Україні [13].

Інститут інформаційних відносин в інформаційному праві досліджено в монографії О. М. Селезньової «Теоретико-методологічні основи інформаційного права України» (2014 р.) [14] та відображено у докторській дисертації

«Теоретико-методологічні основи інформаційного права України як інтегрованої категорії» (2015 р.) [15]. Науковець дослідила сутність інформаційних відносин та запропонувала під їх змістом розуміти «визначену сукупність суб'єктивних прав та юридичних обов'язків, що належать суб'єкту інформаційних відносин». При цьому підкреслює, що органам влади притаманна більша кількість обов'язків, а фізичним особам – більшість прав [14, с. 256]. Також О. М. Селезньова розкрила ознаки, притаманні таким відносинам, проаналізувала існуючі підходи до класифікації та сформулювала власні її критерії диференціації інформаційних відносин, розглянула елементи структури інформаційних відносин [14, с. 235]. Висновки та пропозиції науковця є ціннісними орієнтирами в дослідженні інформаційних відносин у діяльності ДПСУ.

Теоретичні проблеми правового регулювання інформаційних відносин в Україні стали предметом дослідження Д. О. Маріц та висвітлені у монографії «Інформаційні правовідносин в України: теоретичні та практичні аспекти» (2018 р.) [16] та дисертаційному дослідженні «Теоретичні проблеми правового регулювання інформаційних відносин в Україні» (2019 р.) [17]. Д. О. Маріц сформулювала концепцію балансу та взаємодії приватних і публічних інтересів у процесі правового регулювання інформаційних відносин з метою належного забезпечення прав на інформацію їх сучасників [18, с. 24], дослідила поняття, правову природу, склад, особливості та механізм правового регулювання інформаційних відносин, розмежувала правопорушення в інформаційній сфері та інформаційних відносинах, визначила види юридичної відповідальності [17, с. 2].

Привертає увагу думка дослідниці про те, що категорії «суспільний інтерес» та «обмеження» (у контексті права на інформацію) є оціночними й взаємопов'язаними. Пояснюється це тим, що за рішенням суду чи розпорядника, у володінні якого перебуває інформація, незаконно обмежена в доступі, перестає бути такою внаслідок встановлення суспільного інтересу до неї [18, с. 25].

Не менш важливим для розкриття теми дослідження є дисертація Н. А. Литвин «Адміністративно-правове забезпечення інформаційної діяльності органів Державної фіскальної служби України» (2018 р.), окремим питанням у

якому розглянуто інформаційні відносини в діяльності Державної фіскальної служби України (далі – ДФС України). Науковець підтримує існуючу позицію, що в більшості робіт як, втім, і в законодавстві, відображений технічний, механістичний підхід до визначення суспільних відносин в інформаційній сфері. Вони визначаються як зберігання, отримання, надання та інші дії з інформацією [19, с. 128]. У зв'язку з цим науковець пропонує під категорією «інформаційні правовідносини» розуміти відокремлену, однорідну групу суспільних відносин, що виникають у процесі обігу інформації в інформаційній сфері в результаті здійснення інформаційних процесів в порядку реалізації кожним суб'єктом інформаційних прав і свобод, а також у порядку виконання обов'язків державними органами щодо забезпечення гарантій інформаційних прав і свобод [19, с. 133]. На наш погляд, формулювання «обіг інформації в інформаційній сфері» варто конкретизувати сферу приватних чи публічних відносин у якій розглядається обіг інформації, наприклад, з урахуванням предмета нашого дослідження «у прикордонній сфері», адже апріорі інформаційні відносини неможливі без інформації.

Тому у своєму дослідженні Н. А. Литвин адаптує його таким чином, інформаційні правовідносини в діяльності органів ДФС України – це суспільні відносини, які виникають у процесі здійснення покладених на органи ДФС України завдань та функцій, а також під час реалізації права на податкову та митну інформацію платниками податків, органами публічного адміністрування та правоохоронними органами [19, с. 148].

Крім того, у своїй роботі науковець комплексно дослідила адміністративно-правове забезпечення інформаційної діяльності органів ДФС України, провела аналіз загальнотеоретичних понять «інформаційна політика органів ДФС України, «інформаційна діяльність органів ДФС України», «інформаційні послуги, що надаються органами ДФС України» тощо [19, с. 39]. Робота Н. А. Литвин суттєво поглиблює теоретичні засади інформаційних відносин.

І. М. Сопілко у монографії «Інформаційні правовідносини за участю органів державної влади України» (2013 р.) ставить під сумнів свободу вибору у

здійсненні прав на інформацію для органів державної влади як суб'єктів інформаційних відносин. Справедливо роз'яснюючи це тим, що отримання інформації не є свобода вибору при здійсненні права на інформацію, а діє лише імперативна норма щодо можливості чи неможливості брати участь в інформаційних відносинах [20, с. 67]. Можливість обирати процесуальні засоби отримання інформації представниками органів державної влади, зокрема під час адміністративно-процесуальної діяльності, оперативно-розшукової діяльності, досудового слідства тощо, не можна вважати свободою вибору того чи іншого виду поведінки щодо отримання інформації. У таких випадках органи державної влади обмежені законом у частині передбаченості підстав для вибору конкретного процесуального засобу отримання інформації [20, с. 68].

Також науковець досліджує питання щодо видів інформації, яка є предметом інформаційних правовідносин за участю органів державної влади України, правові підстави інформаційних правовідносин за участю органів державної влади. Визначає, що особливим видом інформації є інформаційні адміністративні послуги, які задовольняють реалізацію суб'єктивних прав, запитів зацікавлених суб'єктів та доведення публічної інформації про органи влади [20, с. 111].

У роботі Д. О. Мороза «Адміністративно-правові засади діяльності податкової міліції як суб'єкта інформаційних відносин в Україні» (2016 р.) здійснено комплексний теоретичний аналіз правового статусу податкової міліції як суб'єкта інформаційних правовідносин [21, с. 3]. До суб'єктів інформаційних відносин віднесено всіх суб'єктів правовідносин, які є користувачами будь-якої інформації [21, с. 7]. Визначено, що інформація є обов'язковим елементом у системі інформаційних правовідносин. Установлена взаємозалежність ефективності функціонування органів податкової міліції від інформації загалом і правової зокрема. Визначено вимоги щодо підвищення інформаційного забезпечення діяльності податкової міліції [21, с. 16].

Крім того, базовим підґрунтям для спостережень і висновків послужили узагальнення, висновки та дефініції щодо сутності та змісту інформаційних

відносин у роботах українських учених: Ю. П. Бурило [22], Ю. А. Іванова [13], Р. А. Калюжного [11, 24], О. В. Копана [24], Б. А. Кормича [25], О. В. Кохановської [23], М. Ю. Кузнецова [28], О. Г. Марценюка [24], А. І. Марущака [12], М. М. Мікуліна [13], Д. О. Перова [27], О. О. Тихомирова [13], О. В. Сосніна [26], В. С. Цимбалюка [11], М. Я. Швеця [11] та ін. Розроблення усієї сукупності зазначених праць та їх важливі висновки і пропозиції дозволили поглибити пізнання нормативно-правових аспектів у доволі новій інформаційній правовій тематиці в діяльності ДПСУ [29, с. 89].

Інформаційне забезпечення ДПСУ

Інформаційну діяльність ДПСУ у своєму монографічному дослідженні «Охорона національних інтересів України у прикордонній сфері (адміністративно-правовий аспект)» (2015 р.) В. Л. Зьолка розглядає в контексті специфіки інформаційного забезпечення управлінської діяльності органів ДПСУ. Науковець пропонує під інформаційним забезпеченням управління у ДПСУ розглядати як цілеспрямовану діяльність органів і посадових осіб ДПСУ, яка здійснюється з додержанням вимог законодавства щодо за без-печення інформаційної безпеки та полягає у здійсненні процедур щодо пошуку, збирання, обробки, аналізу, зберігання і своєчасної передачі певним суб’єктам управління даних, необхідних для формування і реалізації управлінського впливу, спрямованого на забезпечення ефективної організації охорони та захисту державного кордону, адекватного та оперативного реагування на загрози національній безпеці у прикордонній сфері та ускладнення обстановки на державному кордоні, попередження і розкриття правопорушень законодавства у прикордонній сфері, а також забезпечення ефективної організації діяльності системи ДПСУ та її елементів [30, с. 203]. Отже, у такому розумінні інформаційне забезпечення спрямоване на підтримання інформаційної безпеки у прикордонній сфері завдяки ефективному управлінню, ґрунтованому на оперативній інформаційній діяльності.

З урахуванням специфіки завдань, що виконує ДПСУ, В. Л. Зьолка надає таку характеристику інформації у прикордонній сфері:

специфічна форма взаємозв'язку, взаємодії компонентів системи управління (Адміністрації ДПСУ, регіональних управлінь, органів охорони державного кордону та відділів прикордонної служби), а також система загалом з навколишнім середовищем, наприклад, із суб'єктами інтегрованої охорони державного кордону з метою моніторингу обстановки в країнах, звідки або через територію яких проходять загрози національній безпеці; обмін інформацією з безпекових питань на державному рівні;

обслуговує всі рівні та функції управління – від підготовки та прийняття рішення до підбиття підсумків виконання як у рамках системи органів ДПСУ з метою організації охорони державного кордону, так і за її межами, наприклад, з метою координації дій правоохоронних органів у сфері боротьби з транскордонною злочинністю;

обумовлює вибір системою того чи іншого варіанта поведінки, переведення системи в новий стан, що забезпечує її рух до заданої мети. Так, з метою ефективної протидії загрозам на державному кордоні на основі оцінки результатів оперативно-службової діяльності ДПСУ були проведені організаційні зміни в підрозділах охорони державного кордону. Такими базовими підрозділами стали відділи прикордонної служби ДПСУ [30, с. 185].

Особливості інформаційного забезпечення управління, пише В. Л. Зьолка, визначаються специфікою функцій і всього процесу управління у ДПСУ, до яких відносить: необхідність реалізації управління в рамках забезпечення недоторканності державного кордону й охорони суверенних прав України в її виключній (морській) економічній зоні;

територіальну компактність існування двох об'єктів управління – осіб, що перетинають державний кордон, і службових осіб органів ДПСУ;

швидку зміну обстановки на державному кордоні, динамізм розвитку та тяжкість наслідків у випадку невчасного реагування на її зміни, появу останнім часом нових ризиків і загроз національній безпеці у прикордонній сфері та завдань щодо ефективної протидії їм;

оптимальне співвідношення розповсюдження та обмеження доступу до інформації про діяльність органів ДПСУ щодо поєднання використання інформації з обмеженим доступом, персональних даних поряд з необхідністю виконання вимог інформаційної відкритості для громадянського суспільства, посадових осіб та органів ДПСУ [30, с. 186–187].

Достатньо обґрунтованими є пропозиції дослідника щодо удосконалення окремих питань інформаційних відносин у прикордонному відомстві, а саме:

визначити, що в діяльності ДПСУ надаються інформаційні послуги [30, с. 194];

розробити та закріпити критерії оцінки та доцільності віднесення інформації до категорії службової [30, с. 199];

створити в усіх ланках управління центри правової інформації; розробити та затвердити програму підготовки та перепідготовки фахівців у сфері інформаційно-аналітичної діяльності, до якої включити питання з інформаційного права [30, с. 201];

ефективніше використовувати в цьому плані можливості наявних інформаційно-телекомунікаційних систем ДПСУ [30, с. 201].

Р. М. Ляшук у своєму монографічному дослідженні «Діяльність відділів прикордонної служби Державної прикордонної служби України» (2016 р.) зосередився на інформаційно-аналітичному забезпеченні як однієї із форм діяльності відділів прикордонної служби. На думку автора, інформація є засобом обґрунтування рішень, що приймається начальником відділу прикордонної служби та необхідна для успішного виконання завдань з охорони державного кордону [31, с. 118]. Інформація у даному контексті, пише Р. М. Ляшук, виступає і як предмет, і як об’єкт, і як результат, а оперативність її отримання, повнота та достовірність безпосередньо впливає на можливості прикордонників орієнтуватись у складній ситуації, оцінювати її, прогнозувати зміни, чітко планувати свої подальші дії, й загалом успішно виконувати підрозділами свої функції [31, с. 119]. Автор визначає інформаційну діяльність як комплекс дій з

отримання інформації та її впровадження в охорону державного кордону [31, с. 120].

Дослідник поділяє інформаційно-аналітичну діяльність відділів прикордонної служби на два етапи:

інформаційний (пошук, збирання, зберігання, поширення інформації);

аналітичний (узагальнення, класифікація, аналіз і перетворення інформації у зручні для використання форми, розробка висновків, пропозицій, рекомендацій і прогнозів) [31, с. 136]. Хоча обидва етапи можна охарактеризувати як інформаційні у зв'язку з тим, що відбувається з приводу інформації, її отримання, обробки, оцінки, систематизації тощо. Можливо їх краще диференціювати як накопичення та обробку (систематизацію).

Автор визначає інформаційно-аналітичну діяльність відділів прикордонної служби як діяльність їх посадових осіб і структурних підрозділів із виявлення, збирання, опрацювання, збереження та поширення інформації у сфері охорони державного кордону, що полягає в комплексі організаційних, правових, технічних та інших дій, яка здійснюється відповідно до норм права та з метою виконання функцій відділів прикордонної служби [31, с. 136]. Виникає питання про доцільність застосування терміна «виявлення» у цьому контексті, адже переважно він відображає значення шукати, знаходити, викривати кого-, що-небудь, показувати, робити явним, помітним [32]. Тому, розвиваючи теорію інформаційних відносин, пропонуємо використовувати поняття «пошук».

Окремі наукові напрацювання О. Б. Фаріона «Інформаційне забезпечення стратегічного кримінального аналізу в оперативно-розшукових підрозділах Державної прикордонної служби України» (2017 р.) [33], «Алгоритм опрацювання оперативно-розшукової інформації для забезпечення потреб кримінального аналізу злочинної діяльності» (2013 р.) [34], «Інструментарій визначення типу загроз прикордонній безпеці в процесі проведення стратегічного кримінального аналізу оперативно-розшуковим підрозділом регіонального управління ДПСУ» (2013 р.) [35] присвячені дослідженню інформації, інформаційного та

аналітичного забезпечення у діяльності оперативно-розшукових підрозділів ДПСУ.

Науковець пише, що завдяки інформації отриманої в результаті оперативно-розшукової діяльності, аналізуються факти та явища, які поділяє на високий (час скоєння злочину, місце скоєння злочину, спосіб злочинних дій) та низький рівень важливості (злочинна активність, взаємозв'язки). Автор пропонує оперативно-розшукову інформацію розглядати як різновид соціальної інформації, специфічної за метою та методами її отримання та режимом використання, яка забезпечує конспірацію, надійне зашифровування джерел, можливість перевірки отриманих оперативних даних та їх використання тільки зацікавленими оперативними працівниками [34, с. 201].

О. Б. Фаріон робить висновок, що за допомогою конкретних критеріїв (достовірність, адекватність, повнота й оптимальність, точність, оперативність, лаконічність, значимість, цінність (корисність), відповідність інформації поставленій меті систематизованість і комплексність інформації, новизна інформації), а також сформованого алгоритму кримінальний аналітик опрацьовує отриману оперативно-розшукову інформацію, оцінює ступінь її необхідності для проведення аналітичних досліджень і формує якісну інформацію, необхідну для проведення кримінального аналізу [34, с. 201].

Дослідник доводить, що в умовах розвитку обстановки на державному кордоні кримінальним аналітиком визначається тип загрози та проводиться аналіз впливу зазначених ознак на стан охорони державного кордону. Виникнення загрози на кордоні та стрімка зміна її пріоритетів потребує вчасного внесення коректив у модель охорони державного кордону та опрацювання комплексу заходів протидії злочинності, що є актуальним в умовах сьогодення. При цьому звертає увагу, що пошук ефективних прийомів і способів аналізу даних обстановки, які надходять в оперативно-розшуковий підрозділ, відіграє важливу роль у процесі виявлення загроз на державному кордоні. Результатом такого аналізу інформації є формування пропозиції для прийняття управлінських рішень і концепції у сфері боротьби зі злочинністю на державному кордоні України [35, с. 213].

Процес аналітичного дослідження загроз безпеці державного кордону та суверенних прав України в її виключній (морській) економічній зоні з метою підготовки пропозицій для прийняття управлінських рішень та опрацювання концепцій у сфері боротьби зі злочинністю розглядається О. Б. Фаріоном як стратегічний кримінальний аналіз [33, с. 157], для інформаційного забезпечення якого потрібний постійний доступ до наявних відомчих інформаційних систем та інформаційних ресурсів інших правоохоронних органів; функціонування в єдиній та збалансованій системі інформаційно-аналітичного забезпечення оперативно-розшукової діяльності; постійне оновлення технологій отримання, систематизації та автоматизованої обробки інформації; створення зі складу аналітиків правоохоронних органів єдиних аналітичних центрів або спільних груп для формування та узагальнення комплексу заходів з протидії злочинності [33, с. 162].

Підсумовуюче викладене, слід зауважити, що теоретична основа інформаційних відносин у діяльності ДПСУ зумовлена міжгалузевим характером широкого теоретичного масиву дослідження цих відносин. Відносно об’єкта нашого дослідження, характер наукових розвідок носить стихійний і фрагментарний характер у цій сфері [29, с. 90]. Загалом досліджені вітчизняні роботи дають змогу дійти висновку про відсутність однозначного розуміння не лише інформаційних відносин, але і його змісту, структурних елементів, інформації, інформаційної діяльності, інформаційної безпеки. У межах даного підрозділу ми акцентували увагу на фундаментальних та концептуальних роботах, у зв’язку із неможливістю охоплення всієї літератури за темою роботи у межах даного обсягу та масштабності сучасних інформаційних відносин. Детальний огляд наукових робіт, які створили теоретичну базу для нового сучасного розуміння правової природи, структури, змісту інформаційних відносин з урахуванням особливостей оперативно-службової діяльності ДПСУ, буде здійснено в наступних підрозділах.

Здебільшого теоретична основа даної проблематики зумовлена міжгалузевим характером широкого теоретичного масиву дослідження цих відносин у теорії держави і права (основні закономірності сутності та розвитку

інформаційних відносин, інформаційних правопорушень, інформаційних прав людини, правові засади інформаційної діяльності органів влади в Україні тощо), державне управління (теорії управління інформаційною сферою як державно-правове явище, розвиток і напрямки державної інформаційної політики в умовах становлення інформаційного суспільства тощо), адміністративне (адміністративно-правове регулювання та забезпечення здійснення державної інформаційної політики, інформаційної діяльності ДПСУ), інформаційне (теорія суспільних відносин, об'єктом яких є інформація), кримінальне, адміністративно-деліктне та цивільне право (установлює межі відповідальності за порушення норм інформаційного законодавства), теорія прикордонного управління і прикордонної безпеки (загальні засади інформаційного забезпечення у функціонуванні ДПСУ) тощо.

На підставі проведеного аналізу з'ясовано, що інформаційні відносини у діяльності ДПСУ комплексно не досліджені, тому актуальним є розроблення теоретичних та організаційних засад нормативно-правового регулювання цих відносин, а саме: визначення правової природи, структури та методології дослідження цих відносин; установлення особливостей державної політики у сфері інформаційної прикордонної безпеки; з'ясування стану нормативно-правового регулювання інформаційних відносин у діяльності ДПСУ; характеристика організаційних та правових засад регулювання інформаційних відносин за порядком доступу до інформації; визначення механізму реалізації прав громадян на звернення та запит на публічну інформацію у ДПСУ; узагальнення досвіду інформаційної взаємодії; аналіз та оцінка сучасного стану інформаційних загроз у прикордонній сфері; характеристика правових (дисциплінарні, цивільно-правові, адміністративні та кримінальні) засобів охорони інформаційних відносин у функціонуванні ДПСУ; установлення організаційно-правових засад інформаційної безпеки в мережі Інтернет та в інформаційних системах; вироблення конкретних пропозицій і рекомендацій з підвищення ефективності інформаційних відносин та удосконалення їх нормативно-правового регулювання.

1.2 Методологічні засади дослідження інформаційних відносин у діяльності Державної прикордонної служби України

Останні роки в Україні відбуваються суттєві реформаційні процеси майже в усіх сферах державно-владної діяльності, зокрема й у сфері охорони державного кордону, основне впровадження яких забезпечує ДПСУ. Сучасні пере-форматування у підходах до охорони державного кордону України обумовлені появою нових загроз і викликів на державному кордоні, у тому числі інформаційними, упровадженням інтегрованого управління кордонами, доцільністю підвищення ефективності охорони державного кордону, протидією транскордонній та іншій злочинності, розширенням співробітництва з міжнародними інституціями у сфері прикордонної безпеки, необхідністю врегулювання ситуації у східних регіонах України, підвищенням рівня довіри до ДПСУ тощо. Упровадження відповідних заходів у сфері безпеки державного кордону України здійснюється разом з удосконаленням інформаційної складової: дотримання інформаційних прав суб'єктів прикордонних відносин; процесів, пов'язаних з видами інформаційної діяльності; забезпечення інформаційної безпеки тощо. Аналіз і наукове вивчення сучасних інформаційних відносин у межах розвитку прикордонної сфери потребує використання різноманітних пізнавальних засобів [36, с. 17].

Необхідність у методологічному дослідженні з'являється тоді, коли в науці складається ситуація вибору, для здійснення якого наявний теоретичний та емпіричний матеріал є недостатнім, тоді виникає потреба до нагромадження наукового досвіду та його узагальнення [37, с. 375], а також створення теоретичного підґрунтя для вирішення практичних завдань. З цього приводу варто згадати міркування Р. А. Калюжного, О. В. Копана, О. Г. Марценюка, наведене у монографічній праці «Теоретико-метологічні засади інформаційного права України: реалізація права на інформацію»: «швидкий розвиток інформаційної індустрії передбачає створення чітких правових умов регулювання цих суспільних відносин. На яких засадах буде відбуватися це регулювання, залежить

не тільки від законодавців, а й, перш за все, – від науковців. Безумовно, першочерговим завданням є встановлення теоретико-методологічних засад науки інформаційного права для ефективного регулювання суспільних відносин у сфері інформації та інформатизації» [24, с. 20].

Відсутність розробок, присвячених окремим аспектам досліджуваних інформаційних відносин, а також наявність окремих практичних проблем, пов'язаних з реалізацією інформації у прикордонній сфері, обумовлюють потребу й визнають актуальність обґрунтування методологічних засад щодо аналізу й отримання нових систематизованих знань [36, с. 17].

Методологія вивчається у багатьох наукових працях усіх сфер наукових знань, це пов'язано із тим, що без методології наукового дослідження не може відбуватись пізнання об'єктивної дійсності, формування нових знань про навколишній світ. Теоретичною основою даного підрозділу стали праці, присвячені загальнонауковій методології (В. М. Брижко, В. Т. Бусела, В. Г. Пилипчука, Р. М. Шевчука, П. Ф. Йолона та інших), методології правової науки (Л. В. Авраменко, О. В. Андрушка, І. М. Жаровської, О. В. Зайчука, Н. М. Крестовської, Л. Г. Матвєєвої, Н. М. Оніщенко, Н. А. Орловської, О. В. Петришина, В. Г. Пилипчука, А. М. Притули, П. М. Рабіновича, М. В. Цвік, С. І. Халимона та інших), методології та методам науки інформаційного права (Р. А. Калюжного, О. В. Копана, О. Г. Марценюка, О. М. Селезньової, І. М. Сопілко, В. С. Цимбалюка та інших). Разом з тим до сьогодні відсутня сформована методологія дослідження інформаційних відносин у діяльності ДПСУ [36, с. 18].

Отримання та формування нових знань про інформаційні відносини у сучасному інформаційному суспільстві стає можливим завдяки науковому пізнанню. У результаті цього процесу людської діяльності відбувається усвідомлення об'єктивної реальності з приводу відносин, пов'язаних з інформацією, отриманням, накопиченням, порівнянням та упорядкуванням знань про правове становище, діяльність і поведінку суб'єктів інформаційних відносин,

які є доволі новими у теорії наукової думки й досліджуються у межах становлення та розвитку інформаційного права [36, с. 18].

Теоретичне обґрунтування та систематизація об’єктивних знань про дійсність – це сфера людської діяльності, – тобто наука. У межах наукового пошуку здійснюється опис, пояснення і прогнозування процесів та явищ дійсності, які становлять предмет її вивчення, на основі відомих і тих, що відкриваються нею, законів. Це обумовлюється як суто теоретичними, так і практичними завданнями й потребами суспільного розвитку, досягається у процесі творчої діяльності окремих науковців або їх колективів [39, с. 72].

Для обґрунтованого та всебічного пізнання об’єктивних вимірів інформаційних відносин у діяльності ДПСУ, а також накопичення про них емпіричних знань необхідне використання широкого спектра дослідницького потенціалу. Ґрунтовне дослідження предмета нашого пізнання – інформаційних відносин у прикордонній сфері, з’ясування його сутності, якісних характеристик, динаміки розвитку в усій різноманітності об’єктивної реальності, її закономірних і випадкових виявів, здатність ефективно і швидко реагувати на кардинальні зміни в нашому швидкоплинному сьогоднішньому житті [39, с. 36], – потребує використання системного підходу як напрямку методологічного дослідження [36, с. 18].

Інформаційне право у складі суспільних наук вирішує завдання, які не мають однозначного рішення і вимагають перевірки на адекватність нескінченно складної реальності, що формально дуже важко зробити – потрібні неформальні кроки, які передбачають знання та застосування філософії, аксіології, епістемології, семантико-понятійної точності, герменевтики та наукової методології [40, с. 136].

Система методів досліджень у сукупності з іншими спеціальними засобами і прийомами пізнання тих або інших правових явищ є складним утворенням, дослідницьким інструментарієм усієї юридичної науки [39, с. 36]. Достовірність пізнавальної діяльності залежить від обрання і використання правильного шляху та найбільш адекватних засобів наукового дослідження, тому питання

методологічного забезпечення є першочерговими для теоретичного дослідження у будь-якій предметній сфері [41, с. 25]. Отже, вивчення та дослідження інформаційних відносин у діяльності ДПСУ стає можливим завдяки всебічному використанню властивих для цієї сфери пізнання засобів, які дозволяють відобразити істинність і зв'язки об'єктивної реальності. Таким своєрідним індикатором у науковому дослідженні є методологія, яка сьогодні серед науковців розглядається під різними кутами зору та має різноманітне змістовне наповнення, що свідчить про притаманну особливість об'єктивної істинності кожного предмета наукового пізнання [36, с. 18].

До цього часу, зазначає О. В. Андрушко, серед учених немає єдності до поняття методології, і надалі дискусійними залишаються питання про співвідношення методології з суміжними поняттями (метод, методика, пізнання, логіка тощо), її потенційні можливості для пізнання навколишнього світу, його окремих явищ тощо [42]. Звідси виникає потреба у визначенні змістовного наповнення поняття «методологія» у контексті дослідження інформаційно-правових відносин у діяльності ДПСУ [36, с. 18].

Філософська категорія «методологія» має подвійну природу: 1) сукупність підходів, способів, методів, прийомів і процедур, що застосовуються у процесі наукового пізнання та практичної діяльності для досягнення наперед визначеної мети (отримання об'єктивного істинного знання або побудова теорії, її логічне обґрунтування); 2) галузь теоретичних знань і уявлень про форми і сутність, закони, порядок та умови застосування підходів, способів, методів, прийомів і процедур у процесі наукового пізнання та практичної діяльності [37, с. 374]. Хоча й існує подвійне розуміння методології, але все ж таки це єдине ціле про сутність засобів пізнання, їх застосування у процесі наукового пізнання, які спрямовані на досягнення дослідницьких завдань [36, с. 18].

У Великому тлумачному словнику сучасної української мови методологія розглядається як: вчення про науковий метод пізнання й перетворення світу; його філософська теоретична основа; сукупність методів дослідження, що застосовуються в будь-якій науці відповідно до специфіки об'єкта її пізнання

[43, с. 664], де метод – це спосіб пізнання; прийом або система прийомів, що застосовується в якій-небудь галузі пізнання (науки).

Методологічну роль виконує не лише філософська методологія та методологія науки. Конкретні науки, перебуваючи з філософією у відношенні методологічного забезпечування, також можуть бути методологічними відносно більш вузьких спеціалізованих розділів певної галузі знання [44, с. 34]. Так, теорія держави і права озброює загальними методами дослідження інформаційне право загалом й окремі його інститути, у тому числі інформаційні відносини, що надає методології у загальнонауковому методологічному значенні універсальний взаємодоповнюючий характер. З цього приводу доречним є прислів'я: «Для досягнення мети всі засоби годяться». Наковці, маючи перед собою конкретну наукову мету, застосовують для її досягнення весь досягнутий людством методологічний інструментарій, доречний у цьому науковому дослідженні, або формують власні конкретні засоби. Наприклад І. М. Сопілко як засіб інформаційно-правового пізнання, створення та організації інформаційно-правового знання пропонує застосовувати метод інформаційно-правової теорії [45, с. 232], який раніше у межах методологічного дослідження не згадувався. При цьому обрання методологічних засобів або формування нових повинно бути виправдано й обґрунтовано для відображення об'єктивного стану досліджуваних правових відносин і вироблення дійсних знань про них [36, с. 18].

Методологія науки вивчає весь комплекс явищ, що належать до інструментальної сфери науки та наукової діяльності, їх осмислення та функціонування; досліджує сукупність пізнавальних засобів, що застосовуються в науці, об'єктивні характеристики та властивості науки і наукової праці, які відіграють істотну роль в отриманні об'єктивної істини наукових знань, а також нагромаджує емпіричні уявлення про них [37, с. 374]; має конкретну мету розробити нормативи, схеми й парадигми, скласти приписи та своєрідні рецепти для наукового мислення та дослідження [37, с. 375].

Методологія є теоретичною основою та способом організації пізнавального процесу, що характеризують пізнання з погляду його загальних

форм, можливостей пізнавальних засобів і механізмів, які зумовлюють логічну послідовність наукового дослідження [41, с. 25]. У юридичній енциклопедії методологію юридичної науки визначено як систему підходів, методів і способів наукового дослідження теоретичних засад їх використання під час вивчення державно-правових явищ [46, с. 618].

О. М. Селезньова пропонує під методологією інформаційного права розуміти, сукупність наукових поглядів на сутність, структуру та поділ методів інформаційного права, що передбачають розкриття їхніх характерних особливостей, а також багаторівневу систему певних методів (способів і прийомів), які використовуються в інформаційному праві [47, с. 186].

М. І. Демчогло, В. А. Ліпкан, К. П. Череповський пропонують методологію розглядати у загальному, комплексному розумінні – як множину (а не просту сукупність) методів, що визначають погляди та методики реалізації принципів, прийомів, способів, засобів, практичної та наукової діяльності для отримання істинних, таких, що відображають об’єктивну реальність, відомостей у знаннях для подальшого перетворення чи підтримання у визначеному стані певних явищ буття відповідно до потреб, інтересів певних суб’єктів на певний момент [48, с. 133; 49, с. 114].

З урахуванням наведених вище міркувань з приводу методології науки можна визначити, що методологія дослідження інформаційних відносин у діяльності ДПСУ забезпечує пізнавальну діяльність, обумовлену об’єктивними потребами (дослідження та удосконалення відносин, які існують з приводу інформації, яка пов’язана з функціонуванням ДПСУ), із використанням методологічного філософсько-правового інструментарію, отриманням конкретного результату – нових істинних об’єктивних знань, формулювання висновків про дійсний стан і розвиток цих відносин у межах формування інформаційного суспільства з урахуванням особливостей прикордонної сфери. Отже, методологія дослідження інформаційних відносин у досліджуваній сфері передбачає обрання найбільш доцільних у даному випадку (конкретному

науковому дослідженні) методологічних засобів пізнання та порядок їх застосування [36, с. 19].

Насичення знаннями та з'ясування об'єктивної істини правових відносин з урахуванням особливостей прикордонної сфери можливе лише з використанням багаторівневого підходу. З цього приводу цілком справедливо зазначає А. М. Притула, що не можуть бути достовірними знання, якщо використано лише один метод, тому методологію дослідження утворює сукупність загальнонаукових і спеціально-наукових методів, які забезпечать об'єктивний аналіз [50, с. 14].

Досліджуючи проблеми методології теорії держави і права, І. М. Жаровська визначає методологію юриспруденції як єдність трьох взаємозалежних частин: доктринально-ідеологічної (парадигма дослідницького бачення права, тобто тип праворозуміння), стратегічної (це царина підходів, що зумовлюють загальну спрямованість дослідження права, вибір стратегії його осягнення) та інструментальної (система когнітивних практик, своєрідний набір методологічних інструментів у створенні знань про право) [51, с. 139].

Узагальнюючи результати дослідження методології інформаційного права, В. С. Цимбалюк пропонує розглядати її в контексті методології юридичної науки (правознавства) у трьох аспектах: а) як систему підходів, методів, способів, засобів наукового дослідження правових явищ; б) як вчення (теорії) про їх застосування під час вивчення цих явищ; в) як множину доктринальних, концептуальних та окремих теоретичних положень для теоретичного упорядкування практики суспільних відносин у певній сфері (галузі) людської діяльності за предметною її ознакою, що у своїй єдності утворюють нову якість, яка не притаманна сукупності їх як елементів у системі [52, с. 43].

У межах нашого дослідження зосередимо увагу на ключовому елементі, який розкриває методологічні засади дослідження інформаційних відносин у сфері діяльності ДПСУ, – на методі [36, с. 19].

Метод наукового пізнання створюється та поглиблюється у процесі активного впливу суб'єкта на об'єкт, твориться суб'єктом, визначається властивостями та розвивається в межах природи конкретного об'єкта пізнання,

відповідає закономірностям його розвитку, у нашому випадку суспільних відносин, що виникають під час формування та реалізації інформаційних відносин у діяльності ДПСУ [44, с. 34].

Метод наукового пізнання – це система принципів, правил, норм, прийомів отримання та систематизації нових знань про об'єктивну й суб'єктивну реальність. У діяльнісному, процедурному розумінні метод є послідовністю дій, що спрямовані на досягнення пізнавальної мети, тобто отримання та систематизацію нових знань. У праксеологічному контексті метод «дисциплінує» пошук істини, дає змогу рухатися до пізнавальної мети найкоротшим і найефективнішим шляхом [44, с. 35].

Методи інформаційного права мають подвійне відображення об'єктивної дійсності: об'єктивне (існують незалежно від різних факторів) та суб'єктивне (їх застосування обумовлюється можливістю вибору конкретного методу суб'єктом пізнання) [47, с. 186].

Зважаючи на існуючий методологічний плюралізм і відсутність єдності розуміння з приводу методології, кардинально іншими є погляди науковців щодо різновидів методів пізнання, серед яких практично переважає єдність різновидів методів пізнання, які становлять цілісну методологічну основу дослідження: загальнофілософські, загальнонаукові, групові (міждисциплінарні) і спеціальні методи [14, с. 264; 46, с. 618; 52, с. 42; 53, с. 29].

З урахуванням того, що прикордонні відносини з приводу інформації є складовою інституту інформаційного права, то найбільш близькою до них є система методів пізнання категорій та інститутів саме інформаційного права, розкрита у монографічній праці О. М. Селезньової «Теоретико-методологічні основи інформаційного права України» [14, с. 263–264]: загальнофілософські, загальнонаукові, науково-правові, спеціально-наукові методи.

Загальнофілософські методи використовуються протягом багатьох віків для дослідження різних суспільних явищ, у тому числі і правових. Їх доречно застосовувати при розгляді категорій, постулатів і висуванні нових теорій стосовно інформаційних відносин у діяльності ДПСУ. Зважаючи на те, що

інформаційне право є новою галуззю права для вітчизняної правової системи, застосування саме загальнофілософських методів дає змогу напрацювати онтологічно-теоретичний фундамент інформаційного права і як галузі права, і, власне, як науки [14, с. 263–264].

Основу загальнофілософських методів дослідження інформаційних відносин у прикордонній сфері складають: діалектичний, герменевтичний, феноменологічний, метафізичний, аксіологічний, дуалістичний тощо. Загальнонаукові методи – методи, що застосовуються в усіх або у більшості суспільних наук (наприклад, структурний, функціональний методи, метод сходження від абстрактного до конкретного чи від конкретного до абстрактного, формально-логічні процедури, скажімо, аналіз, синтез і т. д.) [36, с. 19].

Досліджувані інформаційні відносини, будучи частиною інформаційного права, яка є суспільною наукою, дають підстави вважати, що існує певна група методів загального характеру, які доцільно використовувати при дослідженні будь-яких явищ, зокрема правових. Загальнонаукові методи застосовуються під час вироблення нових знань теоретичного змісту, а також під час виведення результатів із практичних даних з метою наукового аналізу. Комплексний характер інформаційного права, а також багатогалузеве значення категорії «інформація», що є предметом вивчення багатьох інших наук, тільки підкреслює її загальність і наукову всеохопленість [14, с. 264].

Інформаційні відносини у прикордонній сфері дали можливості пізнати такі загальнонаукові методи дослідження, як: синергетичний, структурно-функціональний, порівняльний, формально-логічний, метод класифікації та групування, історичний метод, системний метод, статистичний метод, метод опитування тощо [36, с. 20].

Вивчення інформаційних відносин у прикордонній сфері здійснюється у площині комплексної юридичної науки, при дослідженні пов’язаних інформаційно-правових явищ, конструкцій, категорій і т. д. Варто використовувати методи, що застосовуються в юриспруденції для дослідження всіх положень, які входять до предмета її вивчення [14, с. 264]. Тому очевидним

для пізнання цих відносин є використання науково-правових методів або ще їх називають групові, що застосовуються лише у певній групі наук [52, с. 42], наприклад, характерні тільки для юридичних. Такими методами є: догматичний, спеціально-юридичний, порівняльно-правовий, конкретно-соціологічного дослідження, прикладного системного аналізу, вивчення ефективності правових норм, нормативно-аналітичний тощо [36, с. 20].

Спеціально-наукові методи (метод аналізу практики застосування норм інформаційного права, метод тлумачення норм інформаційного права, кібернетичний метод тощо) властиві виключно інформаційному праву. Ця група методів з огляду на предмет інформаційного права та притаманні йому особливості характеризується деталізованістю порівняно з попередньою групою методів, а також дає змогу глибоко дослідити предмет і складові системи інформаційного права [14, с. 264].

З урахуванням зазначених теоретичних положень зупинимось на характеристиці основних методів, які використані в нашому науковому дослідженні. Для цього згрупуємо їх за такими загальнофілософськими властивостями, які дозволять сформувати структуру пізнання інформаційних відносин у діяльності ДПСУ, а саме: онтологічні, гносеологічні, аксіологічні та праксеологічні.

Онтологічне сприйняття стало можливим через застосування методів, що дозволяють з’ясувати сутність досліджуваних відносин.

Так, **діалектичний метод** «допомагає простежити основний характер суспільних відносин при формуванні відносин правових» [54, с. 105]. Він надав можливість розглянути інформаційні відносини як комплексне правове явище у пошуку протилежностей сутності, елементах, ознаках у їх взаємозв’язку тощо, досліджуваних відносин, їх аналіз та відмежування, систематизацію, розвиток, формування нових напрямків і тенденцій розвитку.

Дуалістичний метод використовувався для визнання двоїстого характеру існування досліджуваних відносин, інформаційної та прикордонної складової.

Феноменологічний метод дозволив пізнати окрему складову (інформаційну) частину в діяльності ДПСУ, складову цілісної прикордонної безпеки – інформаційну діяльність, інформаційні повноваження як суб'єкта інформаційних відносин. Сформувати бачення про нові уявлення, теоретичні аспекти, які утворюють такі інформаційні відносини.

Комунікативний метод забезпечив можливість розглянути організаційно-правовий механізм досліджуваних відносин у взаємозв'язку та взаємодії суб'єктів, їх інформаційних прав та обов'язків у сфері охорони державного кордону.

Структурно-функціональний метод був орієнтований на визначення складових структури інформаційних відносин у діяльності ДПСУ (суб'єкт, об'єкт, зміст), установлення системи суб'єктів цих відносин (загальний, особливий (центральний), спеціальні) та взаємозв'язки між цими складовими.

За допомогою **історичного методу** з'ясовано процес становлення та розвитку законодавчого регулювання інформаційних відносин у діяльності ДПСУ. Установлено зародження нових видів інформаційної діяльності (інформаційно-аналітична, кримінальний аналіз) та створення спеціальних суб'єктів ДПСУ (Центр кібербезпеки), що її здійснюють залежно від обстановки та загроз у сфері охорони державного кордону України.

Гносеологічні підстави формують методи, які вивчають процес пізнавальної діяльності, зокрема: герменевтичний метод, порявнільний, метод класифікації та групування.

Формально-логічний метод надав можливості сформувати поняття, виділити види інформаційних відносин у діяльності ДПСУ, які раніше не були сформульовані у юридичній науці.

Порівняльний метод спрямовувався на проведення аналізу, систематизації, виявлення спільного та відмінного між національним і зарубіжним регулюванням інформаційних відносин прикордонних органів, між ДПСУ та іншими органами державної влади України. Дозволив визначити загальні особливості та відмінні риси досліджуваних відносин, на підставі

зіставлення однопорядкових понять, категорій, процесів, фактів тощо. Виявити вплив змін інформаційного законодавства на відповідні відносини.

Метод класифікації та групування відіграв значне пізнавальне значення щодо мети дослідження, з його допомогою вдалось розмежувати окремі категорії та явища у межах дослідження за окремими ознаками, властивостями, на подібні та відмінні (запропонована класифікація інформаційних відносин, інформації у сфері діяльності ДПСУ, розмежовані види юридичної відповідальності, що посягають на досліджувані відносини тощо).

Герменевтичний метод застосовувався для пояснення термінів, текстів нормативно-правових актів, співвідношення їх із практичною діяльністю ДПСУ щодо участі в інформаційних відносинах.

За допомогою ***аксіологічного*** підходу з'ясована цінність, якості та властивості інформаційних відносин у діяльності ДПСУ, їх правова оцінка впливу на задоволення інформаційних потреб, інтересів та прав суб'єктів прикордонних відносин, а також оцінка їх суспільної користі для забезпечення прикордонної безпеки.

Основою аксіологічного підходу став метод інформаційно-правової теорії (І. М. Сопілко), що дозволив з'ясувати цінність інформації у сучасному суспільстві та у прийнятті управлінських рішень посадовими особами ДПСУ. Визначити, що інформація є категорією фундаментальною як у процесі управління підпорядкованими підрозділами, так і під час установлення взаємозв'язків з громадянами України, іноземними громадянами, особами без громадянства, що перетинають державний кордон, з іншими органами державної влади, іноземними прикордонними структурами у процесі здійснення взаємодії, у тому числі й інформаційної.

Праксеологічні компоненти надають інструментарій для з'ясування взаємозв'язку отриманих знань з практикою, конкретним видом людської діяльності. Для з'ясування праксеологічного контексту нами використовувались такі методи, як: спостереження, анкетування, інтерв'ювання, діяльнісний, контент-аналіз, статистичний, моделювання, прогнозування.

Метод спостереження дозволив протягом усього періоду здійсненого дослідження відслідковувати факти, події, пов'язані із реалізацією права на інформацію як у міжнародному, так і загальнодержавному масштабі, а також розпорядником якої є ДПСУ, відслідковувати зміни в інформаційному законодавстві, у структурі та повноваженнях органів ДПСУ, що призначені для забезпечення інформаційної діяльності.

Анкетування дозволило отримати об'єктивну інформацію від військовослужбовців ДПСУ (офіцерів і курсантів Національної академії Державної прикордонної служби України імені Богдана Хмельницького (далі – НАДПСУ), офіцерів органів та підрозділів охорони державного кордону) з питань правового регулювання обігу інформації, забезпечення правового режиму інформації й інформаційної безпеки у ДПСУ та проблемних питань у сфері інформаційної діяльності.

Інтерв'ювання (військовослужбовців-фахівців у сфері інформаційної діяльності і військовослужбовців, що виконують інші завдання, не пов'язані із цією сферою) утворило підґрунтя для емпіричного досвіду, перевірки та підтвердження теоретичних висновків дослідження.

Діяльнісний метод дозволив пов'язати та розкрити зміст (правосуб'єктність) інформаційних відносин, її суб'єктів із видами інформаційної діяльності, особливостями реалізації прав цих суб'єктів з приводу інформації у діяльності ДПСУ.

Контент-аналіз нормативно-правових актів, рішень судових органів, дослідження подібних та аналогічних питань у науковій доктрині. Такий метод дозволив з'ясувати та виявити загальні закономірності досліджуваних відносин.

Статистичний метод надав можливості поєднати теоретичні знання та практику втілення інформаційних відносин через статистичні показники у діяльності ДПСУ. Проаналізувати окремі аспекти реального стану досліджуваних інформаційних відносин.

Для праксеологічної гуманітарної інтерпретації юридичної науки застосовані математичні методи моделювання та прогнозування.

Метод моделювання допоміг у формулюванні та відтворенні моделі властивостей, структури, взаємозв'язків між елементами інформаційних відносин, фіксуванні отриманих результатів дослідження інформаційних відносин у конкретній сфері діяльності ДПСУ. За допомогою цього методу сформований алгоритм формування інформаційної культури у ДПСУ, проект Інформаційної концепції ДПСУ, методичні рекомендації у роботі зі зверненнями громадян у ДПСУ.

Метод прогнозування використано для формування пропозицій щодо внесення змін у законодавство для покращання організації здійснення інформаційної діяльності ДПСУ, висунення та обґрунтування Концепції інформаційного розвитку (безпеки) ДПСУ.

Методологічний підхід до вивчення теоретичних засад інформаційних відносин у діяльності ДПСУ зумовлює такі особливості: створює теоретичну основу для формування нових змістовно якісних знань відповідно до сучасних умов розвитку інформаційних відносин у прикордонній сфері; формує логічні засади процесу опрацювання великого обсягу інформації, теоретичного та практичного значення, пов'язаної з інформаційною діяльністю ДПСУ; обумовлює дослідження чіткими теоретичними та практичними цілями; результат дослідження залежить від оптимально обраного методологічного інструментарію, що залежить від світогляду науковця, специфіки прикордонної сфери та очікуваних результатів дослідження; є фундаментом для вироблення та уніфікації понятійного апарату інформаційних відносин; забезпечує всебічність отримання інформації про інформаційні відносини у прикордонній сфері; вибір методологічного інструментарію залежить від конкретного науковця, а отже має суб'єктивний характер, при чому існує об'єктивно і не залежить від волі дослідника [36, с. 20].

Отже, на підставі зазначеного можна узагальнити, що наукове дослідження інформаційних відносин у діяльності ДПСУ здійснюється на підґрунті методологічних засад, обрання яких обумовлено специфікою сфери пізнання та спирається на методологічний плюралізм. Методологічне дослідження створює

умови для пізнання та відображення об’єктивної дійсності цих відносин, а також теоретичне підґрунтя для вирішення практичних завдань у діяльності ДПСУ. Дослідження показало, що методологія інформаційних відносин у діяльності ДПСУ є доволі складним і несформованим на сьогодні у межах науки інформаційного права явищем, яке можливо пізнати через систему методів, на підставі яких здійснюється розкриття теоретико-правових засад інформаційних відносини у прикордонній сфері. У даному підрозділі ми сформулювали систему методів через онтологічне, гносеологічне, аксіологічне та праксеологічне сприйняття дійсності, які є теоретичною основою дослідження інформаційних відносин у діяльності ДПСУ, що логічно спирається на методи, характерні для науки інформаційного права, які не є вичерпними.

1.3 Правова природа інформаційних відносин у діяльності Державної прикордонної служби України

Інформаційні відносини як предмет інформаційного права мають не довготривалий період державно-правового визнання, як і інформаційне право ага-лом, але фактично інформаційні відносини існують вже не одне тисячоліття, як і історія розвитку людства. Адже інформаційна діяльність відома давно [14, с. 9]. «Інформація як предмет уваги і побуту людини супроводжує усі її дії та відносини. Це своєрідне середовище існування людини, не менш важливе, ніж повітря, земля» [55, с. 85]. Про глибинні коріння інформаційних відносин, а саме про епоху їх зародження, пишуть автори підручника «Основи інформаційного права», та пов’язують їх із зовнішнім вираженням спілкування між людьми мовою у формі звуків, жестів, пізніше за допомогою малюнків (на скелях, у печерах), ще пізніше письмо: літери, знаки, література [2, с. 16]. Інформація та її обіг у різних її виявах та конфігураціях, доступних людському розумінню, є необхідною умовою існування та еволюції людини, розвитку суспільства і держави.

Інформація в історії розвитку цивілізації завжди відігравала значну роль і виступала засадою для прийняття рішень на всіх рівнях та етапах еволюції суспільства. В історії суспільного розвитку відокремлюють п’ять інформаційних революцій, пов’язаних з кардинальними змінами у сфері виробництва, обробки та обігу інформації, які призвели до радикальних перетворень суспільних відносин [56]. Перша інформаційна революція (пов’язана з винаходом письменності), друга інформаційна революція (обумовлена винаходом друкарства), третя інформаційна революція (обумовлена відкриттям електроструму, завдяки чому з’явився телеграф, телефон, радіо), четверта інформаційна революція (пов’язана з винаходом обчислювальної техніки). Зараз ми переживаємо п’яту інформаційну революцію, пов’язану з формуванням та розвитком транскордонних глобальних інформаційно-телекомунікаційних мереж, які охоплюють усі країни та континенти, і найяскравішим прикладом цьому є Інтернет. Зміст цієї революції полягає в інтеграції в єдиному інформаційному просторі по всьому світу програмно-технічних засобів, засобів зв’язку і телекомунікацій, інформаційних запасів або запасів знань як єдиної інфраструктури, у якій активно діють юридичні та фізичні особи, органи державної влади та місцевого самоврядування. Указані зміни впливають на життя держави, суспільства та особи [56].

Усі здобутки інформаційного розвитку ми використовуємо повсякденно в обігу інформації в усіх сферах приватного та публічного життя: письмо, зображення, друковані джерела, зв’язок, збереження, обробка та передача інформації за допомогою електронної техніки. Причому різновиди та можливості останньої зростають дуже швидкими темпами. Усі ці надбання активно впроваджуються та використовуються під час охорони державного кордону.

Розвиток можливостей людства отримувати, накопичувати, передавати інформацію за значно маленький обсяг часу, майже миттєво, перебуваючи у будь-якій точці земної кулі, має як свої позитивні, так і негативні сторони. Майже вся інформація може потрапити у мережу Інтернет, швидко передаватись засобами зв’язку та за допомогою електронних носіїв, тобто стати доступною широкому загалу майже миттєво. Інформація стала й засобом маніпулювання свідомістю,

яка сьогодні досягла форми інформаційної війни в усьому світі, тому необхідно визначити чіткі правові межі регулювання та захисту інформаційних відносин, у тому числі здійснити їх правову оцінку та наукове обґрунтування. Усі ці аспекти підкреслюють важливість та актуальність дослідження правової природи інформаційних відносин у діяльності ДПСУ.

Інформаційні відносини у прикордонній сфері, на нашу думку, також виникли разом із розумінням та усвідомленням людей щодо необхідності захисту території, де вони проживають, її окраїн, у сучасному розумінні – державних кордонів. Саме своєчасні та достовірні дані про можливі напади ворожих племен, народів допомагали вчасно захистити та зберегти державність (незалежність, свою територію, діючу владу та життя без війни). Із розвитком суспільних і державних відносин інформаційний простір у прикордонній сфері значно ускладнюється та потребує диференціації. На сучасному етапі розвитку такі відносини пов’язані із формуванням, накопиченням, одержанням, зберіганням, використанням, наданням, обміном, поширенням, охороною та захистом інформації у сфері охорони державного кордону. Сьогодні інформаційні відносини у сфері охорони державного кордону України виходять за національні межі, стосуються державних інтересів і інтересів суміжних держав, також фізичних і юридичних осіб, які перетинають державний кордон, здійснюють різну діяльність у прикордонній смузі, на території контрольованого прикордонного району чи на державному кордоні України, а також безпосередньо стосуються персоналу ДПСУ (військових і цивільних осіб, що виконують обов’язки у службових межах).

Інформація як предмет інформаційного права пронизує всі сфери відносин сучасних держаних органів влади. Безумовно не є виключенням і сфера охорони державного кордону. Відповідно до статті 5 Закону України «Про інформацію» кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів [57]. Дане положення відповідає частині 2 статті 34 Конституції України, яка визначає, що «кожен має право

вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір».

Розвиток державно-правових відносин та об'єктивна необхідність їх нормативно-правового врегулювання зумовлюють виникнення, зростання, накопичення та сприйняття значної кількості інформації про різні сфери суспільних відносин, використання різноманітних сучасних носіїв інформації, її оброблення та автоматизації. Особливої актуальності за останні роки набули відносини щодо обігу інформації у сфері охорони державного кордону, зокрема сьогодні, коли ми стоїмо на порозі відкриття для нашої держави європейських кордонів і впровадження Стратегії інтегрованого управління кордонами, яка спрямована на підвищення ефективності управління державним кордоном, запровадження ефективних інструментів співпраці та координації на внутрішньовідомчому, міжвідомчому, міжнародному рівнях, а також з приватним сектором, що передбачено досягти завдяки: оперативному обміну інформацією; вдосконаленню міжвідомчого ІТ-обміну інформацією; забезпеченню технічного, криптографічного та кібернетичного захисту інформації в інформаційно-телекомунікаційних системах; підвищенню рівня обізнаності представників суб'єктів інтегрованого управління кордонами у сфері дотримання прав людини тощо [59]. Такі цілі зумовлені, перш за все, веденням гібридної, у тому числі інформаційної війни проти України Російською Федерацією (далі – РФ). Тому серед основних завдань Стратегії розвитку Державної прикордонної служби України визначено – створення системи інтегрованого управління безпекою державного кордону, яку планується забезпечити шляхом розвитку інформаційної складової частини системи охорони державного кордону [59].

У нормативних документах стратегічного планування розвитку ДПСУ [59] частину інформаційних відносин у межах формування нової системи захисту державного кордону України, пов'язаного із сучасними загрозами та виконанням узятих державою зобов'язань перед Європейським Союзом (далі – ЄС), названо як «інформаційна складова» частина системи охорони державного кордону, яка згадується в контексті: інформаційної взаємодії; системи аналізу та оцінки

інформації; формування баз даних; функціонування інформаційно-телекомунікаційних систем «Гарт», «Аркан»; системи електронного документообігу; захисту інформації; усебічного удосконалення обладнання, призначеного для передачі інформації; інформаційно-аналітичного забезпечення [59]; аналізу ризиків; міжвідомчого обміну інформацією між суб'єктами інтегрованого управління кордонами; організації діяльності контактних пунктів [59]. Отже, така складова відображає внутрішню інформаційну діяльність у межах функціонування прикордонного відомства, спрямованого на забезпечення безпеки державного кордону, розвиток та функціонування його на відповідному європейському рівні, не допускаючи при цьому вияву будь-яких загроз, підтримання інформаційної взаємодії.

Поінформованість громадян про діяльність органів державної влади є важливим елементом демократизації суспільства, можливістю користуватися в повному обсязі послугами, що надаються органами влади, реалізовувати свої права, а також здійснювати громадський контроль. Особливої актуальності набуває інформація, що пов'язана з діяльністю ДПСУ, зокрема з умовами перетинання державного кордону України тощо. Громадяни, які мають намір перетнути державний кордон, як правило, долають значний шлях, щоб дістатися пунктів пропуску, і вразі отримання відмови в перетинанні (через неналежно оформлені документи або їх відсутність) втрачають свій час, гроші, а іноді і правомірну вигоду. Саме тому, громадяни повинні оперативно отримувати інформацію про діяльність ДПСУ, у першу чергу, про порядок і правила перетинання державного кордону України. Крім цього, значення та роль інформації у втіленні форм оперативно-службової діяльності сьогодні настільки важливі, що без неї (актуальної, оперативної інформації) неможливо здійснення управління її органами, підрозділами та реалізація завдання щодо охорони державного кордону України. Забезпечення цього стає можливим завдяки участі ДПСУ, її органів і підрозділів в інформаційних відносинах, які мають свої характерні особливості.

Виникнення, зміна та припинення інформаційних відносин регулюється інформаційними нормами, або в теорії інформаційного права застосовується термін інформаційне законодавство України (нормативно-правовими актами, прийнятими ВРУ) у формі законів і постанов нормативного змісту [2, с. 32], та підзаконними нормативними актами, що приймаються відповідними державними органами влади [2, с. 54]). Ураховуючи особливості прикордонної сфери, зазначимо, що на регулювання інформаційних відносин впливають також норми міжнародного права. Так, основними відомостями щодо встановлення правил національного прикордонного законодавства (перетинання державного кордону, в'їзд, виїзд, порядок перебування та проведення різних робіт у прикордонній смузі або контрольованому прикордонному районі) є двосторонні угоди про встановлення проходження лінії державного кордону України та встановлення і функціонування (здійснення міжнародного сполучення) пунктів пропуску через державний кордон та з інших питань [60, 25]. Тобто інформаційні відносини у прикордонній сфері стосуються інтересів та інформаційних прав суміжних держав, фізичних і юридичних осіб, які можуть перетинати державний кордон або здійснювати різну дозволену законодавством діяльність уздовж державного кордону України та персоналу ДПСУ [61, с. 35].

В. А. Копилов зазначає, що будучи різновидом правових відносин, інформаційні правові відносини виражають усі основні ознаки правового відношення [62, с. 13]. Змістом правових відносин, підкреслюють Н. М. Керестовська та Л. Г. Матвєєва, є суб'єктивні юридичні права й обов'язки їх учасників, а правові відносини є юридичним виразом економічних, політичних, майнових, культурних та інших суспільних відносин [53, с. 430].

Безліч відносин (зв'язків) постійно виникає між людьми та їх об'єднаннями, які потребують врегулювання шляхом установлення певних правил поведінки їх учасників. Відносини, що врегульовані нормами права, є правовідносинами. Правові відносини є результатом дії приписів норм права на відносини між різними суб'єктами. Відповідно до цього, робить висновок С. Л. Лисенко,

відносини у суспільстві, що врегульовані нормами права, називаються правовими відносинами, або правовідносинами [63, с. 211].

О. Ф. Скакун характеризує правові відносини як специфічний вид суспільних відносин, що складаються між людьми чи колективами як суб'єктами права з приводу соціального блага або забезпечення яких-небудь інтересів, перебувають у формі соціальних зв'язків – економічних, організаційних, політичних, сімейних тощо [64, с. 389]. У теорії права присутня думка, що «правові відносини є найбільш поширеною і виразною формою реалізації права, втілення в життя його приписів» [53, с. 431]. Найбільш значущим поділом форм реалізації права є: дотримання, виконання та використання норм права [40, с.408; 53, с. 413; 63, с. 189].

Якщо «правові відносини» являють собою врегульовані правовими нормами суспільні відносини між різними суб'єктами з приводу реалізації їх прав і задоволення інтересів, то «інформаційні правові відносини» є винятковими суспільними взаємозв'язками між споживачами та володільцями (розпорядниками) різноманітних знань, які здобувають у результаті отримання та усвідомлення відомостей, що становлять зацікавленість у кожному окремому випадку, причому дії з такими даними (інформаційна діяльність) знаходяться виключно в правовому регулюванні різних сфер суспільних відносин, а зміст інформації може і не мати юридичного контексту [65].

Правові відносини виникають, змінюються або припиняються скрізь, де діє право [41, с. 334], принципова особливість яких полягає у тому, що вони завжди пов'язані з інформацією. Базовий нормативно-правовий акт, що регулює інформаційні відносини в Україні – Закон України «Про інформацію», поширюється на відносини, які виникають у всіх сферах життя і діяльності особи, суспільства та держави, пов'язані із інформацією. Так, у преамбулі цього Закону закріплено, що він урегульовує відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [57]. Тобто це є будь-яка інформація, різноманіття (зміст) якої в сучасному світі неможливо охопити і визначити правовими засобами, лише вплив і поводження із нею

суб'єктів інформаційних відносин регулюються правовими нормами. Держава, регулюючи інформаційні відносини, надає їм правової форми.

Інформаційні відносини пов'язані з основними правилами інформаційної діяльності, зокрема щодо отримання відповідних відомостей, їх поширення та зберігання тощо. Більш чітко регулюється, охороняється інформація, володільцем і розпорядником якої є органи державної влади, зокрема й у сфері охорони державного кордону України – ДПСУ.

На підставі ґрунтовного аналізу інформаційно-правових відносини, Л. П. Коваленко визначив їх як суспільні відносини, які регулюються нормами права, виникають, розвиваються та припиняють свою дію в інформаційному просторі між суб'єктами права, які наділені інформаційними правами й обов'язками [66, с. 274]. При цьому автор називає такі ознаки інформаційно-правових відносин: вони існують практично в усіх сферах суспільної життєдіяльності; юридична природа інформаційно-правових відносин передбачає наявність особливого суб'єкта, у власності або в розпорядженні якого є інформація або інформаційний ресурс; основним об'єктом інформаційно-правових відносин є інформація; інформаційно-правові відносини відкриті для всіх учасників; інформаційні відносини характеризуються високим рівнем динамічності, оскільки періодично з'являються нові інформаційні явища, які потребують правового регулювання [66, с. 275]. Такий підхід гармонійно поєднує зміст правових відносин із особливостями інформаційної сфери.

О. М. Селезньова називає інформаційні правові відносини одним із видів правових відносин [14, с. 209], обґрунтовуючи це наявністю в інформаційних відносинах ознак, притаманних іншим правовим відносинам, а саме: інформаційні правовідносини є особливим різновидом суспільних відносин, об'єктом яких є інформація; інформаційні правовідносини є ідеологічними відносинами, які існують у формі зв'язків між суб'єктами; інформаційні правовідносини є наслідком дії права, виникають після прийняття відповідної норми; інформаційні правовідносини є свідомим волевиявленням суб'єктів інформаційного права; інформаційні правовідносини виявляють себе як односторонні, двосторонні та

багатосторонні зв'язки між суб'єктами інформаційного права; інформаційні правовідносини обумовлені можливістю державного примусу [47, с. 210].

Досліджуючи інформаційні правові відносини за участю органів державної влади, І. М. Сопілко зазначає, що інформаційні відносини пов'язані з можливостями отримувати та надавати органами державної влади України інформацію [20, с. 23].

В. А. Копилов зважаючи на сутність основних об'єктів правовідносин у системі інформаційного права, особливості та юридичні властивості, поділяє їх на дві складові: інформаційна сфера – це інформація, її різні види і форми подання; та її юридична модель, інформаційні процеси й інформаційні відносин, які виникають під час здійснення цих процесів [62, с. 9]. Тобто визначає наявність статичної та динамічної сторін інформаційних відносин.

Науковець зазначає такі особливості інформаційних відносин: виникають, здійснюються та припиняються в інформаційній галузі у процесі обігу інформації; опосередковують державну політику визнання, дотримання і захисту інформаційних прав і свобод людини і громадянина в інформаційній сфері; відображають особливості застосування публічно-правових та цивільно-правових методів правового регулювання при здійсненні інформаційних прав і свобод з урахуванням специфічних особливостей і юридичних властивостей інформації та інформаційних об'єктів [62, с. 51].

При цьому *цивільно-правовий аспект* інформаційних відносин пов'язує з особливостями реалізації інформаційних прав і свобод, у першу чергу майнових прав і прав власності на інформаційні ресурси в інформаційній сфері, здійснення яких визначається особливостями інформації як об'єкта правовідносин. А *публічно-правовий аспект* інформаційних відносин пояснює необхідністю забезпечення гарантій здійснення інформаційних конституційних прав і свобод громадян, державного управління інформаційними процесами формування і використання державних інформаційних ресурсів, створення і застосування державних інформаційних систем і засобів їх забезпечення, а також засобів і

механізмів інформаційної безпеки для досягнення головної мети – забезпечення гарантій здійснення інформаційних прав і свобод [62, с. 51].

Інформаційні правові відносини, наголошує О. О. Кульчій, по суті є суспільними відносинами, які виникають під час інформаційної діяльності [67, с. 35]. Таке розуміння відображає зв'язок з нормами Закону України «Про інформацію», де визначено, що ним врегульовані відносини з приводу створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [57, преамбула], а основними видами інформаційної діяльності є ті ж самі процеси [57, ст. 9]. Узагальнюючи, О. О. Кульчій наголошує, що інформаційні відносини є реальними суспільними відносинами, оскільки саме правовідносинами вони стають на підставі врегулювання нормами інформаційного законодавства [67, с. 35].

Ураховуючи погляди В. А. Копилова, О. О. Кульчій та згаданого вище положення Закону України «Про інформацію», інформаційні відносини ототожнюються з інформаційною діяльністю, інформаційними процесами або розглядаються як форми втілення у реальні правові відносини. Аналогічні судження відслідковуються у поглядах таких науковців, як О. А. Гаврілова, В. Д. Елькіна, С. Г. Чубукова.

О. А. Гаврілов уособлює інформаційні правові відносини із об'єктивними зв'язками, які складаються між суб'єктами правових відносин та інформаційною діяльністю. Так, він зазначає, що: поняття «інформаційні відносини» відображає об'єктивні зв'язки між окремими індивідами, їх колективами й об'єднаннями, підприємствами, державними органами і установами з приводу виробництва, розповсюдження та споживання інформації; інформаційні відносини тісно пов'язані з інформаційною діяльністю, яка являє собою сферу суспільного виробництва, пов'язану з виробництвом інформації, наданням інформаційних послуг і підготовкою інформаційних продуктів. Саме у процесі цієї діяльності виникають різноманітні інформаційні відносини [68, с. 38].

С. Г. Чубукова, В. Д. Елькін підкреслюють, що інформаційні правові дносини формуються на основі інформаційних процесів [69, с. 54], до яких

належать: створення інформації; збирання інформації (сприйняття і перетворення); передача інформації між різними елементами інформаційної системи; обробка інформації; зберігання інформації; тиражування інформації; поширення інформації [69, с. 55]. На нашу думку, увесь інформаційний процес у діяльності ДПСУ можна узагалінено відобразити таким чином: надходження інформації з різних джерел, сприйняття інформації, її перетворення (диференціація) для подальшої передачі компетентним посадовим особам з подальшою фіксацією та обробкою у відповідних базах даних, забезпечення її зберігання з дотриманням правого режиму інформації (якщо це інформація з обмеженим доступом), у разі якщо йде мова про відкриту публічну інформацію, то здійснюється її поширення **(додаток Б).**

І. Л. Бачило робить висновок, що «для права в його доктринальній та нормативній частинах об'єктами є, з одного боку, предмет – інформація в доступних для права формах; а з іншого – інформаційні відносини, які виникають з приводу даного предмета» [55, с. 95]. Цілком слушним є твердження І. В. Арістової про те, що поняття інформаційних відносин ще остаточно не закріпилося у правовій науці. У своїй науковій праці науковець формулює таке визначення інформаційних відносин, під якими пропонує розуміти процес цільового, однозначно усвідомленого перерозподілу в суспільстві відомостей про особу, предмети, факти, події, явища і процеси незалежно від форми їх подання [70, с. 260], що за зовнішнім уявленням подібно до диференціації досліджуваних відносин. Пізніше у своєму дисертаційному дослідженні з приводу організаційно-правових засад державного управління національною інформаційною сферою України І. В. Арістова обґрунтує необхідність розгляду інформаційних відносин між об'єктом і суб'єктом державного управління національною інформаційною сферою через те, що під час становлення та розвитку інформаційного суспільства управлінські відносини у вузькому тлумаченні перетворюються в інформаційні відносини у їх широкому тлумаченні. Розглядаючи «інформаційні відносини» під таким ракурсом, науковець пропонує таке визначення цього поняття: інформаційні відносини – це інформаційні зв'язки між суб'єктами політичної

системи суспільства, держави, що виникають під час одержання, використання, зберігання та споживання інформації. Інформаційні відносин дослідниця пропонує розгляд-дати з урахуванням стандартного циклу руху інформації у вигляді найпростішої формули: виробництво–розповсюдження–споживання [5, с. 20]. На наш погляд, сьогодні така «формула» інформаційних відносин є складнішою, ніж зазначені механічні процеси, це ще й інтелектуальна діяльність, пов'язана з аналізом інформації, розмежування приватної й публічної інформації тощо, які є невід'ємною важливою складовою цих відносин та детермінантом руху інформації.

Інформаційними відносинами, на думку І. В. Безверхньої та Л. В. Перевалової, можна вважати суспільні відносини, які виникають з приводу одержання, перероблення, використання або зберігання інформації [71]. Аналогічний погляд розділяють і інші науковці, зокрема О. О. Тихомиров, М. М. Мікуліна, Ю. А. Іванов [4, с. 196]. Такий підхід до означення суспільних відносин в інформаційній сфері у роботі Д. В. Огородова згадується як технічний, механістичний. Тобто «одержання, перероблення, використання або зберігання інформації» відображають певні процеси, динамічні явища, технічний підхід [72, с. 68]. Н. А. Литвин зазначає, що такий підхід не повною мірою виражає саме правову специфіку, тому для цілей правового регулювання конструкція відносин в інформаційній сфері не може бути заснована на копіюванні даної формули. Переносити технічний підхід у правову сферу просто неправильно: право має власні механізми впливу на суспільні відносини. Тому, незважаючи на зовнішню простоту і удавану зручність зазначеної конструкції «одержання, перероблення, використання або зберігання інформації», її механічне перенесення на правову сферу має істотний недолік, оскільки не береться до уваги різновид важливих відносин – статичні відносини в інформаційній сфері [19, с. 128]. Варто підтримати таку позицію у зв'язку із тим, що у зазначеному випадку процесам надається перевага, хоча відносини відбуваються не заради них, а все ж пріоритетними є інформаційні права, інтереси, потреби, з приводу яких суб'єкти і вступають у ці правовідносини. А інформаційні процеси і діяльність є виявом

гарантії, засобом, формою, механізмом реалізації цих відносин і задоволення інформаційних інтересів і потреб.

Відносини урегульовані за допомогою загальнообов'язкових, формально визначених, гарантованих державою правил поведінки, через їх суспільну значущість А. І. Марущак називає інформаційними, інформаційно-правовими або інформаційними правовідносинами. Упорядкування цих відносин пов'язується із необхідністю розмежування прав та обов'язків їх учасників, а саме з визначенням правового статусу відповідних суб'єктів [12, с. 110].

Досліджуючи проблематику інформаційних відносин, В. М. Боєр і О. Г. Павельєва, визначають інформаційні правові відносини як різновид відносин, що виникають у суспільстві, і роблять висновок, що інформаційні правовідносини – це соціальні відносини з приводу створення, володіння та користування інформацією, що складається в інформаційній сфері, урегульовані інформаційно-правовими нормами [73, с. 45]. При цьому вони сформулювали такі ознаки інформаційних правовідносин: конкретний об'єкт – інформація (не залежно від форми); форма правомірної поведінки; інформаційно-правові норми; поєднання суб'єктивних прав і обов'язків кореспондуючого характеру, коли реалізація права одним суб'єктом знаходиться в безпосередній залежності від виконання відповідного обов'язку іншим суб'єктом; суб'єктами правовідносин можуть бути тільки особи, що володіють правосуб'єктністю; суб'єктивні права й обов'язки, що реалізуються учасниками інформаційних правовідносин, перебувають під захистом держави, підкріплені системою державних гарантій і заходами юридичної відповідальності. Науковці зауважують, що відносини з приводу інформації, які не відповідають зазначеним ознакам (інформаційні відносини побутового характеру), не можуть розглядатися як правові відносини [73, с. 45].

Н. М. Ковальова, характеризуючи інформаційні відносини, розставляє акцент на їх нормативному закріпленні та взаємозв'язках суб'єктного складу і визначає їх як відносини між різноманітними учасниками – громадянами, редакціями газет, телестудіями, підприємствами, організаціями, фірмами й

іншими, у яких останні беруть участь як носії прав і обов'язків, установлених нормами інформаційного права, називаються інформаційно-правовими відносинами або інформаційними правовідносинами [74, с. 40].

На основі системно-структурного аналізу інформаційної сфери Ю. П. Бурило з'ясовує, що інформаційні відносини (об'єктом яких є інформація) входять до її складу, поряд із інформаційно-інфраструктурними відносинами (об'єктом яких виступають засоби зв'язку, інформатизації та інформаційної безпеки), та поділяє досліджувані відносини на дві групи: ті, що мають публічне значення, та приватні інтереси [22, с. 5].

Д. Маріц, підкреслюючи відсутність законодавчого визначення поняття «інформаційні відносини» за наявності низки нормативно-правових актів вітчизняного законодавства й оперування законодавцем цим поняттям у низці законів [75, с. 64], узагальнює своє бачення цього терміна – це відносини, які регулюються нормами приватного та публічного права, які виникають, змінюються і припиняються між суб'єктами суспільних відносин на підставі юридичних фактів [75, с. 67]. Таке визначення можна застосувати і до іншого виду відносин, воно не враховує особливості відносин, що відбуваються з приводу інформації.

Л. П. Коваленко підкреслює суттєву ознаку інформаційних правовідносин – їх інформаційний характер, що зумовлюється змістом інформаційних правовідносин, які виникають, змінюються і припиняються саме при формуванні, розповсюдженні й використанні інформації, необхідної для існування держави, забезпечення потреб суспільства та територіальних громад [76, с. 4].

Особливим є підхід О. В. Кохановської щодо сутності та поняття інформаційних правовідносин, і взагалі до інформаційного права загалом. Науковець, піддає обґрунтованій критиці теорію інформаційного права як окремої галузі права, а інформаційні відносини, наголошує О. В. Кохановська, мають свою специфіку залежно від того, до якої галузі права вони належать за своєю правовою природою. О. В. Кохановська пропонує розмежовувати поняття «інформаційних правовідносин» і «правовідносин у сфері права на інформацію».

Термін «інформаційні правовідносини» пропонує використовувати, по-перше, як узагальнюючий для усієї сфери інформаційних правовідносин, і по-друге, як конкретизуючий щодо тих інформаційних цивільних правовідносин, які не пов'язані з інформацією, як з особистим немайновим, не пов'язаним з майновими, благом. Розглядаючи інформаційні правовідносини через призму цивільно-правових відносин, науковець стверджує, що інформаційні правовідносини за своєю природою є приватноправовими відносинами, і можуть характеризуватися через предмет і метод цивільного права [23, с. 6]. Протилежною є думка Ю. А. Тихомирова, який розглядає інформаційне право виключно як частину публічного права [77, с. 137].

На наш погляд, варто підтримати у цьому питанні більш універсальний погляд, сформульований О. М. Селезньовою, яка підкреслює, що система інформаційних відносин включає і приватні, і публічні інтереси й потреби, а конкретному інформаційному правовідношенню притаманна одна із зазначених характеристик [14, с. 211]. Інформаційним правовідносинам у прикордонній сфері властивий публічно та приватно-правовий характер, це пов'язано з тим, що інформаційні процеси у цій галузі відбуваються у зв'язку з діяльністю органу державної влади – ДПСУ, але охоплюють і приватні інтереси осіб, що прямують через державний кордон, звертаються із запитами, зверненнями тощо.

Р. А. Калюжний, О. В. Копан і О. Г. Марценюк висловили свою думку з приводу поняття інформаційних відносини – це є суспільні відносини у сфері інформації: її одержання; використання; поширення; правового захисту; права власності на неї; боротьби з комп'ютерною злочинність та договірні відносини у сфері інформатики [24, с. 23]. Б. А. Кормич оперує поняттям «інформаційні правовідносини», виходячи з елементарного етимологічного алгоритму, – суспільні відносини з приводу інформації, які урегульовані правом. Виходячи із цього, формулює таке визначення інформаційних правовідносин – це «врегульовані інформаційно-правовою нормою інформаційні відносини, сторони яких виступають носіями взаємних прав та обов'язків, установлених і гарантованих інформаційно-правовою нормою» [25, с. 55–56]. Крім цього,

зауважує науковець, це не будь-які суспільні відносини, що виникають з приводу інформації чи інформаційних процесів, а ті, що визначають параметри і характеристики інформаційних процесів (їх види, форми, засоби, змістовне наповнення). При цьому, виділяє два базових інформаційних процеси: процес документування та публічного оголошення (розповсюдження) інформації [25, с. 36].

Н. А. Литвин розуміє інформаційні правовідносини як відокремлену, однорідну групу суспільних відносин, що виникають у процесі обігу інформації в інформаційній сфері в результаті здійснення інформаційних процесів у порядку реалізації кожним суб'єктом інформаційних прав і свобод, а також у порядку виконання обов'язків державними органами щодо забезпечення гарантій інформаційних прав і свобод [19, с. 133]. При цьому зазначає, що для інформаційних правовідносин, які реалізуються в рамках права, характерні такі специфічні ознаки: існують в інформаційній сфері; відображають особливості застосування різних методів правового регулювання залежно від об'єкта правовідносин; опосередковують державну політику дотримання, захисту, визнання інформаційних прав і свобод суб'єкта правовідносин в інформаційній сфері [19, с. 133].

Проаналізовані наукові думки з приводу змісту й особливостей інформаційних правовідносин свідчать, що багато хто з науковців, зокрема І. В. Безверхня, В. М. Боєр, В. Д. Елькін, Р. А. Калюжний, О. В. Копан, О. Г. Марценюк, О. Г. Павельєва, Л. В. Перевалова, С. Г. Чубукова, інформаційні правові відносини розкривають, дотримуючись нормативно закріпленої моделі в Законі України «Про інформацію». З урахуванням усього теоретичного масиву, опрацьованого нами, сформулюємо ознаки, які, на наш погляд, притаманні інформаційним відносинам:

інформаційні відносини є різновидом суспільно-правових відносин, які охоплюють сфери приватного та/або публічного життя;

врегульовуються нормами інформаційного законодавства або у поєднанні із галузевим нормами (адміністративного, цивільного, кримінального тощо), чи

окремої, як зазначає О. Т. Басараб, (специфічної) сфери правового регулювання – прикордонної сфери [78, с. 371];

є інформаційною складовою національної та державної безпеки;

вони мають подвійні засади виникнення та функціонування: юридична (правова норма) й інформаційна (конкретна інформація) складові;

відображають ступінь державного визнання, дотримання і захисту інформаційних інтересів, прав і свобод людини та громадянин, суб'єктів публічної адміністрації в інформаційній сфері;

інформаційний інтерес та потреба є мотивом виникнення та реалізації інформаційних відносин;

спрямовані на забезпечення та підтримання інформаційної безпеки особи, держави, суспільства, дотримання інформаційних прав суб'єктів цих відносин;

це особливі, з приводу інформації, відносини, які складаються між її суб'єктами: окремими індивідами, їх колективами й об'єднаннями, державними органами, установами, підприємствами;

втілюються в інформаційних процесах або діяльності, щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, обміну та захист інформації.

Отже, **інформаційні відносини** можна розуміти як урегульовані нормами інформаційного або у поєднанні з галузевим (чи окремою правовою сферою) законодавством суспільні відносини, що відбуваються з приводу задоволення інформаційних потреб, прав, інтересів усіх суб'єктів цих відносин, а також забезпечення інформаційної безпеки.

Класифікація інформаційних відносин. «Питання класифікації будь-яких правових відносин є важливою методологічною передумовою, оскільки передбачає розподіл наявних інформаційних правових відносин за певними ознаками» [17, с. 240]. Різноплановість інформаційних відносин у прикордонній сфері обумовлює їх своєрідність. Досліджувані відносини мають комплексний інтегрований характер, зумовлений інформаційними потребами суб'єктів у цій сфері та реалізацією завдань прикордонного відомства – забезпечення

недоторканності державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні [79, ст. 1].

В. Г. Хахановський, І. В. Мартиненко, В. М. Смаглюк, М. Я. Швець, О. І. Грищенко, Ю. І. Ігнатушко називають інформаційну сферу відмінною, унікальною та особливою, порівнюючи з іншими галузями права [80, с. 48]. Багатогранність і складність інформаційних відносин О. М. Селезньова пов'язує з комплексним характером інформаційного права, що зумовлює «регламентацію інформаційних відносин не лише нормами галузі інформаційного права, але й забезпечення врегулювання джерелами інших галузей права» [14, с. 212]. Зі свого боку І. М. Сопілко вказує на необхідності упорядкування інформаційних відносин та підкреслює, що особливої актуальності це питання набуває у правовідносинах за участю органів державної влади. Його вирішення на науково-теоретичному рівні буде позитивно впливати на нормотворчу діяльність щодо визначення інформаційних повноважень органів державної влади, а також знижуватиме рівень конфліктних ситуацій у процесі правозастосування [20, с. 74–75]. У межах нашого дослідження варто ще додати, що таке упорядкування дозволить поглибити з'ясування особливостей правової природи інформаційних відносин у сфері функціонування ДПСУ, належного застосування її посадовими особами норм інформаційного законодавства та розвиток теорії інформаційного права.

Багатогранність, міжгалузевий характер інформаційних відносин, а також їх правове регулювання приватноправовими та публічно-правовими нормами зумовили в доктрині інформаційного права з урахуванням різноманітних критеріїв визначити класифікації цих відносин. Хоча І. В. Хоменко пропонує застосовувати два головних критерії для класифікації: на підставі суттєвих ознак досліджуваних об'єктів – природний та на підставі не суттєвих ознак досліджуваних об'єктів – штучний [81, с. 62–63]. Таку позицію Д. О. Маріц піддає критиці та зауважує, що «такий підхід може бути виправданим для чітко визначеного об'єкта, а не правових відносин» [82, с. 127]. При цьому у досліджуваних відносинах досить важко відзначити суттєві та несуттєві ознаки, тому в теорії інформаційного права науковці пропонують ураховувати багато

критеріїв, які іноді є однаковими (схожими), а іноді особливими в окремій сфері правового регулювання.

Так, за цілями [83, с. 216; 84, с. 11], за функціями [14, с. 20] та за функціональним призначенням розмежовують: регулятивні й охоронні [82, с. 132]. При цьому, крім регулятивних (урегульовують інформаційні відносини) та охоронних (забезпечення безпеки для усіх учасників цих відносин, гарантування реалізації інформаційних прав), також необхідно розглядати превентивно-захисні (ужиття запобіжних заходів і методів для перешкоджання та недопущення впливу інформаційних загроз).

За співвідношенням прав і обов'язків учасників інформаційно-правові відносини розглядають: вертикальні і горизонтальні [14, с. 20–23; 83, с. 67]. В основі такого розподілу (вертикальні, горизонтальні) Д. О. Маріц застосовує критерій за характером зв'язків [82, с. 132]. Крім вертикальних і горизонтальних, у теорії адміністративного права виділяють реорганізаційні та діагональні відносини. Реорганізаційні як різновид горизонтальних відносин виникають за ініціативою осіб у разі їх звернення до публічної адміністрації (запит на публічну інформацію). Діагональні, пов'язують суб'єкт і об'єкт управління, які знаходяться в різних галузях управлінської системи [85, с. 49], наприклад обмін інформацією між суб'єктами інтегрованого управління кордонами.

За таким критерієм, як сфера поширення інформаційних правовідносин, О. І. Яременко поділяє їх на внутрішньоорганізаційні та зовнішні [86, с. 159–160], О. М. Селезньова – на внутрішньоорганізаційні, внутрішньодержавні, зовнішньодержавні [14, с. 20–23]. Для досліджуваної теми характерні відносини внутрішньовідомчого (які пов'язані із забезпеченням управління службовою діяльністю, пошуком інформації про факти чи спроби неправомірного перетинання державного кордону, здійсненням інформаційно-аналітичної діяльності; захистом і збереженням інформації) та змішаного спрямування (як внутрішньо- так і зовнішньодержавного) у зв'язку з тим, що знати особливості

перетинання державного кордону України необхідно як громадянам України, так і іноземцям та особами без громадянства (далі – ОБГ).

Розподіляючи інформаційні відносини на матеріальні та процесуальні, науковці об'єднують їх за змістом [82, с. 132; 83, с. 89; 84, с. 11], за призначенням [14, с. 23]. Причому зазначають М. А. Лапіна, А. Г. Ревін, В. І. Лапін, матеріальні відносини реалізуються за допомогою процесуальних [83, с. 90].

За тривалістю у часі: постійні та тимчасові [86, с. 159–160]. Варто підтримати позицію О. М. Селезньової, яка пропонує даний критерій доповнити таким видом, як періодичні інформаційні правовідносини, що мають місце протягом певного строку і припиняються, але після спливу деякого часу знову створюються, і знову припиняються [14, с. 215]. Так, наприклад іноземний громадянин в'їжджає на територію України на певний період, а через певний час виїжджає. При в'їзді та виїзді громадянин повідомляє під час прикордонного контролю встановлені відомості, які підлягають перевірці. Такі відносини можна віднести до періодичних.

О. І. Яременко[86, с. 159], Д. О. Маріц [82, с. 132]пропонують поділяти інформаційні відносин за галузевою сферою. Хоча такий критерій класифікації О. М Селезньова піддає критиці і зауважує, що він підкреслює комплексність інформаційного права як галузі законодавства. І пропонує розподіляти за цим критерієм на інформаційні правовідносини, урегульовані нормами інформаційного законодавства, та інформаційні правовідносини, урегульовані нормами інших галузей законодавства, зі зміною критерію – на «залежно від виду галузі законодавства, яка здійснює регламентацію інформаційних відносин» [14, с. 214]. Ще, на нашу думку, варто додати, що інформаційні правовідносини можуть бути регламентовані окремою правовою сферою, наприклад, у межах забезпечення охорони державного кордону ДПСУ.

Отже, з урахуванням аналізу [87, с. 62–68] різних наукових позицій О. М. Селезньової [14, с. 20–23]. Д. О. Маріц [82, с. 132]. І. М. Рассолова [84, с. 13], М. Ю. Кузнецової [88, с. 201], Л. Л. Попова [89, с. 53],

О. П. Климентьєва і Д. О. Перова [90, с. 82] стосовно класифікації інформаційних відносин, нами сформульовано конкретні критерії класифікації інформаційних відносин у діяльності ДПСУ.

На підставі проведеного наукового аналізу сучасної доктрини зазначимо про відсутність єдиного підходу до класифікації інформаційних правовідносин через різноманітність сучасної інформації (в державно-правових межах), складність і багатогранність інформаційних відносин, а також відсутність законодавчо закріплених видів інформаційних відносин. У зв'язку із цим, для досягнення поставленої мети, а саме – з'ясування правової природи інформаційних відносин в діяльності ДПСУ, запропонуємо власну їх класифікацію.

1. Залежно від напрямку діяльності вони поділяються:

на *внутрішньовідомчі*: інформаційні відносини пов'язані із забезпеченням управління службою, проходженням служби, порядком і підставами реалізації прав та обов'язків військовослужбовцями та персоналом ДПСУ; забезпеченням соціального захисту персоналу; порядком і підставами звільнення зі служби; пошуком та отриманням різної інформації про факти чи спроби неправомірного перетинання державного кордону; інформуванням органів охорони державного кордону про факти проведення господарської чи іншої діяльності у прикордонній смузі та контрольованому прикордонному районі; інформаційно-аналітичною діяльністю; захистом і збереженням інформації та ін.;

внутрішньодержавні: пов'язані з висвітленням результатів діяльності відомства; інформуванням про організацію та функціонування ДПСУ; координуванням та взаємодією; перевіркою Уповноваженим ВРУ з прав людини дотримання законодавства України щодо захисту персональних даних, місць тримання осіб в органах охорони державного кордону; мотивуванням до проходження служби (навчання) у ДПСУ; координацією діяльності військових формувань і відповідних правоохоронних органів, пов'язаною із захистом державного кордону України, а також взаємодією з органами державної влади, органами місцевого самоврядування та громадськими організаціями під час

здійснення покладених на ДПСУ завдань; інформаційним забезпеченням демократичного цивільного контролю тощо;

зовнішньодержавні (проведення роботи з питань делімітації та демаркації державних кордонів; усебічна взаємодія з прикордонними службами іноземних держав та робота прикордонних представників, спільне патрулювання; обмін інформацією про обстановку на спільному кордоні через діяльність Контактних пунктів у пунктах пропуску через державний кордон) [91, с. 58];

змішаного спрямування (як внутрішньо- так і зовнішньодержавного): інформування про порядок та підстави перетинання державного кордону (громадянами України, іноземними громадянами, особами без громадянства, міжнародними делегаціями тощо) за різних умов на різних ділянках державного кордону (з тимчасово окупованою територією); урегулювання окремих питань, пов'язаних із перетинанням державного кордону з громадянами України, іноземними громадянами та особами без громадянства, їх консультування (Контактний центр ДПСУ служба «Довіри», робота зі зверненнями (запитами) громадян); своєчасне доведення змін щодо порядку перетинання державного кордону в засобах масової інформації та ін.).

2. За функцією: регулятивні (урегульовують, упорядковують інформаційні відносини у сфері охорони державного кордону, інформаційну взаємодію тощо); охоронні (визначають умови, підстави застосування та заходи державного впливу до правопорушників); превентивно-захисні (є окремою групою інформаційних відносин, пов'язаних із забезпеченням правового режиму інформації).

3. За видом норм, що врегульовують інформаційні відносини: матеріальні (закріплюють правове становище суб'єктів інформаційних відносин (права, обов'язки, відповідальність); процесуальні (забезпечують втілення матеріальних норм у реальних правових відносинах; установлення правил, процедур дотримання правового режиму інформації тощо).

4. За тривалістю у часі: короткочасні, постійні, періодичні і за запитом.

Короткочасні відбуваються у зв'язку із порядком надання інформація у стислі терміни після прийнятого рішення (факту, події, що відбулися), про

важливі події та зміни, актуальні при перетинанні державного кордону (наприклад, організація пропуску через державний кордон на період Великодніх свят), про повсякденні результати діяльності прикордонного відомства, ситуація в Контрольних пунктах в'їзду-виїзду зоні проведення Операції об'єднаних сил (далі – ООС) (Антитерористичної операції (далі – АТО) (висвітлюється в засобах масової інформації (далі – ЗМІ) з повідомлень прес-центру ДПСУ (у т. ч. он-лайн конференції) та на офіційному сайті ДПСУ) [91, с. 59].

Постійні інформаційні відносини, пов'язані із формуванням баз даних, наприклад відповідно до наказу Адміністрації ДПСУ «Положення про базу даних «Відомості про осіб, які перетнули державний кордон України» [92]. Але постійними вони є для ДПСУ, уповноважені підрозділи якої забезпечують наповнення інформацією, її обробку та захист. Стосовно громадян, які перетинають кордон, інформація у базі зберігається протягом 5 років, але якщо громадянин постійно виїжджає за кордон та в'їжджає на територію України, такі відносини можуть носити і постійний характер.

Періодичні мають місце у зв'язку із поданням час від часу інформації у сфері діяльності ДПСУ: звіти про діяльність відомства (кількість пропущених у встановленому порядку через державний кордон, затриманих за незаконне перетинання (спробу) державного кордону осіб, складено протоколів про адміністративні правопорушення, кількість затриманих нелегальних мігрантів, кількість відпрацьованих запитів на інформацію, фінансовий звіт про витрачання коштів). Періодичність може бути за місяць, три місяці, шість місяців, за рік тощо [91, с. 59].

На виконання вимог законів України «Про звернення громадян», «Про доступ до публічної інформації» громадяни України, іноземні громадяни звертаються із індивідуальним зверненням, запитами з питань перетинання державного кордону, особистих питань та діяльності прикордонного відомства, як правило, щодо правомірності дій посадових осіб ДПСУ, роз'яснення норм законодавства, отримання персональних даних чи публічної інформації тощо у межах компетенції відомства. Крім цього, військовослужбовці та працівники

ДПСУ мають право звертатись зі зверненнями (запитами) про порядок проходження військової служби, з питань соціального захисту військовослужбовців тощо. Запити надходять до Адміністрації ДПСУ, інших підпорядкованих структурних підрозділів від вищих органів державної влади: Адміністрації Президента України, ВРУ, Кабінету Міністрів України (далі – КМУ), від інших органів державної влади, органів місцевого самоврядування, установ, організацій та підприємств [91, с. 59].

5. Залежно від суб'єктного складу однією стороною інформаційних правовідносини виступає ДПСУ із: міжнародними публічними суб'єктами (при узгодженні прикордонних питань з суміжними державами або державами – партнерами, укладенні відповідних угод з прикордонних питань тощо); посадовими особами, органами державної влади та місцевого самоврядування України; громадянами України; іноземними громадянами (або особами без громадянства); персоналом ДПСУ [91, с. 61].

6. За зв'язками: вертикальні (у зв'язку із підпорядкованістю носять імперативний характер); горизонтальні (із суб'єктами, не пов'язаними службовими відносинами, можуть носити як імперативний, так і диспозитивний характер, залежить від співвідношення прав та обов'язків у відносинах); реорганізаційні (запит на отримання публічної інформації, інформації про перетинання державного кордону щодо запитувача інформації) та діагональні відносини (обмін інформацією між суб'єктами інтегрованого управління кордонами, у роботі спільних контактних пунктів).

7. За видами та характером норм, що регламентують інформаційні відносини: Конституція України (визначає основні інформаційно-правові засади таких відносин); загальні або базові нормативно-правові акти (визначають основні положення інформаційного права); спеціальні нормативно-правові акти (врегульовують інформаційну діяльність у межах повноважень ДПСУ); програмні (стратегічні) документи ДПСУ (формулюють основні напрямки розвитку відомства на близьку та середню перспективи з урахуванням актуальних загроз і потреб розвитку сфери охорони державного кордону).

Проаналізовані теоретичні обґрунтування поняття, ознак і класифікації інформаційних відносин дозволили визначити їх характерні особливості в діяльності ДПСУ:

вони є різновидом суспільних відносин, притаманних сфері охорони державного кордону, специфічність яких обумовлюється динамічними процесами, пов'язаними з охороною державного кордону, забезпеченням контролю за його перетинанням, підтриманням прикордонного режиму й утриманням державного кордону;

врегульовані нормами інформаційного, адміністративного, кримінального та інших галузей права, а також нормами законодавства у прикордонній сфері;

носять публічний характер у зв'язку із тим, що відбуваються за участі та ресурсів органу публічної адміністрації, – ДПСУ;

абсолютний характер цих відносин означено конкретизацією одного із суб'єктів – розпорядника інформації у сфері охорони державного кордону, де інший суб'єкт конкретно не визначений;

характер і мета таких відносин обумовлюється інформаційною потребою з приводу інформації, що пов'язана або створюється у процесі виконання завдань ДПСУ;

стосуються інтересів української держави, іноземних держав, фізичних і юридичних осіб, які перетинають державний кордон або здійснюють різну діяльність уздовж чи безпосередньо на державному кордоні України, а також стосуються інтересів персоналу ДПСУ;

є інформаційною складовою прикордонної безпеки, що загалом є визначальним фактором державної та національної безпеки;

мають подвійну спрямованість: внутрішню та зовнішню. До внутрішніх належать інформаційні відносини, пов'язані зі здійсненням особовим складом відомства завдань, реалізацією їх правового статусу. До зовнішніх належать відносини, пов'язані з інформацією, необхідною для суб'єктів, які перетинають державний кордон, або перебувають у прикордонній смузі або контрольованому прикордонному районі.

Логічним завершенням цього підрозділу стає визначення авторського бачення інформаційних відносин у діяльності ДПСУ, яке сформульоване на підставі огляду теоретичного його осмислення у науковій доктрині та сформованого власного розуміння особливостей досліджуваної сфери. Отже, під **інформаційними відносинами у діяльності ДПСУ** пропонуємо розуміти різновид суспільних відносин у сфері охорони державного кордону, які урегульовані нормами (інформаційного, адміністративного та інших галузей) законодавства, а також нормами законодавства у прикордонній сфері, які обумовлені реалізацією прав, потреб і процесів щодо інформації, що пов'язана з діяльністю або створюється у процесі виконання завдань ДПСУ.

1.4 Структура інформаційних відносин за участю Державної прикордонної служби України

Дослідження юридичної структури інформаційних відносин дозволяє розкрити внутрішню побудову та з'ясувати взаємозв'язок елементів цієї структури, а отже поглибити пізнання та сформувати закономірності розвитку цих відносин у діяльності ДПСУ. Хоча переважно така будова містить небагато, три або чотири елементи, у юридичній думці відбуваються розходження щодо її змісту, причому практично всі науковці дотримуються єдності щодо двох елементів, таких як суб'єкт та об'єкт.

О. О. Кульчій називає традиційними такі елементи: суб'єкт правовідносин; юридичний зміст правовідносин, який виявляється в суб'єктивних правах і юридичних обов'язках названих суб'єктів (учасників) правовідносин; об'єкт правовідносин [67, с. 35]. А. І. Марущак, визначає, що зміст інформаційних правовідносин складають суб'єктивні права і обов'язки [12, с. 116]. В. М. Боер і О. Г. Павельєва додають ще до цих елементів «способи реалізації прав та обов'язків» [73, с. 52]. В. А. Копилов відносить до основних елементів інформаційних правовідносин такі складові, як: об'єкт (те, у зв'язку з чим або з

приводу чого виникають правовідносин); суб'єкти (учасники правовідносин); правовий статус (права, обов'язки та відповідальність суб'єктів); поведінка (визначені правовою нормою дії або бездіяльність суб'єктів) [62, с. 47]. Прихильником такої позиції є український учений Б. А. Кормич [25, с. 56].

На наш погляд, найбільш раціональною є позиція В. М. Карташова [93, с. 477], О. П. Климентьєва і Д. О. Перова [90, с. 82], Н. А. Литвин [19, с. 137], Д. Маріц [75, с. 66], О. М. Селезньової [94, с. 184], І. М. Сопілко [20, с. 61], які розглядають інформаційні правовідносини як єдність таких елементів: **суб'єкт, об'єкт та зміст** (взаємні права та обов'язки учасників правовідносин).

Суб'єктний склад інформаційних правовідносин

Багато наукових праць (І. В. Діордіца, К. Р. Калюжного, І. Ф. Коржа, К. С. Полетило, В. А. Ліпкана, Ю. Є. Максименко та ін.) присвячені суб'єктам інформаційних правовідносин, переважно стосуються фізичних осіб та забезпечення їх інформаційних прав. Органи державної влади як суб'єкти інформаційних правовідносин досліджені І. В. Арістовою, О. А. Барановим, К. І. Бєляковим, Ю. П. Битяком, Р. А. Калюжним, Л. П. Коваленко, Н. А. Литвин, В. С. Цимбалюком, Є. О. Резченком, І. М. Сопілко та багатьма іншими науковцями. Розкриті питання правового становища, поняття та видів суб'єктів інформаційно-правових відносин не вичерпують усіх аспектів правового становища органів державної влади у цих відносинах. Крім цього, розвиток інформаційного суспільства, розширення меж відкритості діяльності органів охорони державного кордону ДПСУ та необхідність охорони їх службової інформації потребують детального аналізу та визначення правового становища їх як суб'єктів інформаційних відносин, що досі залишається поза увагою наукового пізнання.

Характеризуючи інформаційні відносини в діяльності ДПСУ, у попередньому підрозділі нами було визначено таку їх особливість як абсолютний характер (одна сторона визначена – ДПСУ, друга не конкретизована). Отже, один суб'єкт цих відносин є орган держаної влади – ДПСУ, інший (інші) будь-які особи (суб'єкти) інформаційних відносин (фізичних та юридичних осіб, об'єднання

громадян та суб'єкти владних повноважень [57, ст. 4]). У межах предмета нашого дослідження вони набувають певної конкретизації, а саме: які мають відповідний інтерес (реалізують право на запит на публічну інформацію, розпорядником якої є ДПСУ) чи зобов'язання (наприклад, особи що перетинають державний кордон подають відповідну інформацію під час паспортного контролю) щодо інформації у сфері охорони державного кордону. У зв'язку із цим варто відмежувати загального (не наділені владними повноваженнями) та спеціального (особливого) суб'єкта інформаційних правовідносин (що наділені владними повноваженнями) у сфері охорони державного кордоні.

У науковій доктрині існує думка про розподіл суб'єктів інформаційних відносин на споживачів і виробників, де споживачі інформації реалізують конституційне право на пошук та одержання інформації будь-якого виду й форми, за винятком інформації, що обмежена у доступі, порядок одержання якої регламентується чинним законодавством. Споживачі вступають у правовідносини з тими виробниками інформації, інформаційних об'єктів, які діють відповідно до покладених на них обов'язків щодо створення й поширення інформації (це в основному державні підприємства, установи організації й органи місцевого самоврядування), а також із виробниками інформації – авторами робіт або власниками інформаційних об'єктів. Правовідносини, у які вступають користувачі й виробники інформації, регулюються інформаційними нормами, які містяться в законах та інших нормативних актах, залежно від виду оброблюваної інформації [95, с. 376].

У цьому контексті варто зазначити, що споживач більше стосується матеріального блага, товарів, речей, що потребують ужитку, споживання, використання. Так, у Законі України «Про захист прав споживачів» споживач трактується як фізична особа, яка придбає, замовляє, використовує або має намір придбати чи замовити продукцію для особистих потреб, безпосередньо не пов'язаних з підприємницькою діяльністю або виконанням обов'язків найманого працівника [96, п. 22, ст. 1].

А виробником визнається суб’єкт господарювання, який: виробляє товар або заявляє про себе як про виробника товару чи про виготовлення такого товару на замовлення, розміщуючи на товарі та/або на упаковці чи супровідних документах, що разом з товаром передаються споживачеві, своє найменування (ім’я), торговельну марку або інший елемент, який ідентифікує такого суб’єкта господарювання; або імпортує товар [96, п. 4 ст. 1]. У Законі України «Про інформацію» згадується про споживачів, яким надається інформаційна продукція, що має матеріалізований результат інформаційної діяльності і лише у контексті цивільного законодавства [57, ст. 23]. А матеріальний вияв фіксування, наприклад письмовий документ, це лише змістовне відображення інформації, а цінність несуть дані, знання, відомості, що знаходяться у ньому. Інформація щодо сфери охорони державного кордону може бути отримана не тільки шляхом матеріального закріплення (письмово, в електронній формі), але й усно (на особистому прийомі посадовими особами ДПСУ громадян), у тому числі телефонному режимі (звернення до Контактного центру ДПСУ (служби «Довіри»). На наш погляд, необхідно використовувати категорії набувачі або користувачі інформації до осіб, які мають право звернутись до посадових осіб ДПСУ для отримання публічних чи персональних даних відповідно до норм чинного законодавства. Про ДПСУ в межах нашого дослідження можна говорити як про особливий суб’єкт, або ще як використовує Н. А. Литвин у своєму дисертаційному дослідженні – центральний орган, відносно характеристики суб’єктного складу інформаційних відносин в діяльності органів ДФС України [19, с. 138]. Отже, ДПСУ як особливий чи центральний суб’єкт у досліджуваних відносинах обумовлюється встановленим правовим становищем усієї ДПСУ та її структурних підрозділів, виключно на які покладається виконання завдань щодо забезпечення недоторканності державного кордону, реалізації форм оперативно-службової діяльності (далі – ОСД), а тому й володіння, користування та розпоряджання інформацією у цій сфері.

Визначальну роль для ДПСУ як суб’єкта інформаційних відносини відіграють основні принципи діяльності, такі як: поєднання гласних, негласних і

конспіративних форм і методів діяльності, відкритість для демократичного цивільного контролю [79, ст. 3]. Специфічною особливістю діяльності ДПСУ як суб'єкта інформаційних відносин є оптимальне співвідношення розповсюдження та обмеження доступу до інформації про діяльність органів та підрозділів ДПСУ [30, с. 187]. Крім того, ДПСУ може вступати в інформаційні відносини з іншими суб'єктами: фізичними особами; юридичними особами; громадськими об'єднаннями; іншими суб'єктами владних повноважень. Як ми вже визначили, їх інформаційна правосуб'єктність має загальні підстави та зміст, на відміну від ДПСУ, яка є розпорядником інформації і визначається особливостями її загального правового статусу.

Суб'єктна характеристика ДПСУ пов'язана з поняттям «розпорядник інформації» в особі правоохоронного органу спеціального призначення у сфері охорони державного кордону. Поняття «розпорядники інформації» охоплює суб'єктів, які мають визначені у статті 13 Закону України «Про доступ до публічної інформації» обов'язки стосовно оприлюднення та надання публічної інформації, що знаходиться у їхньому володінні [97, ст. 13], до переліку яких належить ДПСУ. Розпорядники публічної інформації, відповідно до згаданого вище Закону, є тими суб'єктами, що забезпечують реалізацію права на доступ до інформації. Тобто під поняттям «розпорядник інформації» розуміється не особа, яка має право розпорядження інформацією, а особа, під контролем якої знаходиться публічна інформація [98]. Неоднозначним є розуміння опитаних респондентів щодо того, «хто є розпорядником інформації у сфері діяльності ДПСУ?» 63,2 % обрали ДПСУ, 12,6 % – військовослужбовці ДПСУ, 11,7 % – Міністерство внутрішніх справ України (далі – МВС України), 7,3 % – особи, що надали свої персональні дані для обробки, по 2,6 % висловили, що це є Президент України й КМУ **(додаток В)**. При цьому варто відмітити що більшість вважає правильно

Опитані у ході анкетування респонденти (усього 610 осіб), серед яких 45,9 % офіцерського, 40,2 % рядового і 13,9 % сержантського (старшинського)

складу ДПСУ. При чому сержантський (старшинський) та рядовий склад опитаних є курсантами 4 курсу НАДПСУ, які через кілька місяців після проведеного у межах цього дослідження анкетування отримують офіцерські звання та будуть призначені на відповідні офіцерські посади, тому нам важливо було з'ясувати не тільки знання та розуміння тих чи інших аспектів інформаційних відносин у діяльності ДПСУ досвідчених офіцерів, але й наскільки розуміють та знають їх курсанти-випускники, на скільки вони готові до реалізації норм інформаційного законодавства у подальшій практичній діяльності в органах охорони державного кордону. Термін перебування на службі респондентів до 5 років (52,8 %), до 20 років (14,7 %), більше 20 років (14,7 %), до 15 років (10,4 %), до 10 років (7,4 %). Анкетуванням було охоплено 620 осіб.

Ураховуючи міждисциплінарний характер інформаційних відносин і важливість їх у діяльності прикордонників різних спеціальностей, опитані були фахівці з широкого кола, зокрема: правоохоронна діяльність 22,3 %, право 14 %, автомобільний транспорт 13,1 %, філологія 13,1 %, безпека державного кордону 10,5 %, телекомунікації та радіотехніка 10 %, військове управління (за видами збройних сил) 7 %, психологія 6,5 %, національна безпека (сфера прикордонної діяльності) 3,5 % **(додаток В)**.

З'ясуємо, що розуміється під «володінням»? Відповідно до статті 1 Закону України «Про доступ до публічної інформації» публічною інформацією є відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена у процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень [99]. Тобто тут під володінням розуміється не юридична правомочність, що є складовою права власності (володіння, користування, розпорядження), а характеристика фактичного стану, тобто факт контролю суб'єкта над певною інформацією як нематеріальним об'єктом (інформація зберігається у суб'єкта в зафіксованому на матеріальному носії вигляді або іншим чином доступна йому). Тому термін

«розпорядник» лише позначає, що інформація знаходиться у фізичному контролі суб'єкта, а не те, що він має право розпоряджатися і визначати долю інформації на свій розсуд [99].

Органи та підрозділи ДПСУ як суб'єкти інформаційних правовідносин

Охорона державного кордону важлива функція будь-якої держави, її забезпечення потребує впровадження сучасних інноваційних підходів з урахуванням вимог часу та існуючих загроз прикордонній безпеці. Розвиток інформаційного суспільства обумовлює необхідність здійснення якісних перетворень у діяльності органів охорони державного кордону з урахуванням інформаційної відкритості та забезпечення інформаційної безпеки. Органи охорони державного кордону реалізують свої повноваження як суб'єкти інформаційних правовідносин під час безпосереднього виконання поставлених перед ДПСУ завдань, у межах визначеної ділянки щодо забезпечення недоторканності державного кордону України [100, п. 2]. Поява нових викликів у сфері безпеки державного кордону України обумовила нагальну потребу в розвитку інформаційної складової ДПСУ, що передбачено Стратегію розвитку ДПСУ [59].

Органи охорони державного кордону України є суб'єктами інформаційних правовідносин, мають власний рівень правосуб'єктності, що визначається нормативно-правовими актами, які врегульовують інформаційні прикордонні відносини. Особливість правового статусу цих органів як державно-владних суб'єктів визначається тим, що вони уповноважені діяти лише у спосіб, передбачений законом. У цьому їх суттєва різниця від приватноправових суб'єктів суспільних (зокрема інформаційних) відносин, які повноважні діяти у межах, не заборонених законом [20, с. 107].

Закон України «Про інформацію» закріплює право кожного на інформацію, що передбачає можливості вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів [57, ст. 5]. Під кожним необхідно розуміти суб'єктів інформаційно-правових відносин, до яких Закон України «Про інформацію»

відносить фізичних та юридичних осіб, об'єднання громадян та суб'єктів владних повноважень [57, ст. 4]. Із цієї норми незрозуміло до яких суб'єктів відносяться органи та підрозділи ДПСУ, до юридичних осіб чи суб'єктів владних повноважень, які в згаданому Законі розмежовані.

Закон України «Про доступ до публічної інформації» до суб'єктів владних повноважень відносить органи державної влади, інші державні органи, органи місцевого самоврядування, органи Автономної Республіки Крим (далі – АРК), інших суб'єктів, що здійснюють владні управлінські функції відповідно до законодавства та рішення яких є обов'язковими для виконання [97, п. 1, ч. 1, ст. 13]. Ще одне значення терміна «суб'єкт владних повноважень» розкрито в Кодексі адміністративного судочинства України, під яким розуміються органи державної влади, органи місцевого самоврядування, їх посадові чи службові особи, інші суб'єкти при здійсненні ними публічно-владних управлінських функцій на підставі законодавства, у тому числі на виконання делегованих повноважень, або наданні адміністративних послуг [97, ч. 7 ст. 4]. Ці дві законодавчі норми хоча і стосуються регулювання різних сфер правових відносин, але разом з тим, пов'язують суб'єктів владних повноважень зі здійсненням управлінських (адміністративних) функцій та реалізацією законодавчих актів, які є ключовими у характеристиці суб'єкта владних повноважень.

Автори Науково-практичного коментаря Кодексу адміністративного судочинства України під владними управлінськими функціями, що здійснюються на основі законодавства, розуміють будь-які владні повноваження у рамках діяльності держави чи місцевого самоврядування, що не належать до законодавчих повноважень чи повноважень здійснювати правосуддя [101, п. 19]. Є. І. Білокур функції управління розглядає як основні базові види, напрямки управлінської діяльності, тобто з точки зору змісту та спрямованості управлінської діяльності [102, с. 35]. При цьому зазначає, що зміст цих функцій може полягати як у впливі на керованих суб'єктів (організація, регулювання, координація), так і в необхідній допоміжній діяльності, не пов'язаній з безпосереднім впливом на поведінку людей, наприклад планування. Через

реалізацію функції управління суб'єкти виконавчої влади здійснюють управлінські процеси, досягають поставленої мети [103, с. 12].

Серед існуючої різноманітності видів управлінських функцій ми зазначимо ті функції, які реалізуються силами прикордонного загону та стосуються теми нашого дослідження, а саме: правове регулювання, нагляд і контроль.

Функція регулювання дозволяє впорядкувати поведінку підпорядкованих суб'єктів (персонал ДПСУ) та правові відносини, у які вступає відповідальна посадова особа органу охорони державного кордону. Реалізуючи цю функцію, начальник прикордонного загону видає накази та розпорядження з організації охорони державного кордону у межах наданих повноважень (про встановлення режиму в пунктах пропуску через державний кордон України, уводить посилену охорону державного кордону, виносить постанови щодо обмеження мореплавства та заборони виходу в море українських невійськових суден і плавзасобів у територіальному морі та внутрішніх водах України та з інших питань для запобігання незаконному перетинанню державного кордону України тощо) [100, п. 6, Р. ІІІ], забезпечує охорону державної таємниці [100, п. 4, Р. ІІІ].

Нагляд передбачає спостереження за додержанням законності у відповідних суспільних відносинах, які здійснюються компетентним на те органом, із застосуванням наданих йому законом (підзаконним нормативним актом) повноважень і спрямовані на попередження, виявлення і припинення порушень, а також притягнення порушників до відповідальності [104, с. 36]. Нагляд за додержанням прикордонного режиму, режиму в пунктах пропуску, режимом державного кордону та інших питань, віднесених до компетенції ДПСУ, здійсняються у повсякденній діяльності прикордонного загону, завдяки чому забезпечується охорона визначеної ділянки державного кордону України та суверенних прав України в її виключній (морській) економічній зоні [100].

Завдяки контролю надходить інформація про дійсний стан справ щодо виконання завдань, з подальшим прийняттям рішення про відповідну корекцію у системі управління [103, с. 128]. У нормативно-правових актах, які врегульовують питання охорони державного кордону недостатньо розмежовані поняття

«контроль» та «нагляд». Переважно використовується термін «контроль»: контроль за плаванням і перебуванням українських та іноземних невійськових суден і військових кораблів у територіальному морі та внутрішніх водах України [79, ст. 9]; контроль за дотриманням прикордонного режиму [79, п. 11 ст. 19]; контроль за режимом у пункті пропуску [79, п. 13 ст. 19]. Поняття «нагляд» застосовується лише відносно дотримання законності в діяльності ДПСУ [79, ст. 32].

Традиційно прийнято вважати прерогативою у державі прокурорський нагляд, але оскільки функції прокуратури були обмежені у зв'язку з конституційною реформою, то органи прокуратури сьогодні здійснюють «класичний» нагляд за місцями тримання іноземців та осіб без громадянства у спеціальних приміщеннях і пунктах тимчасового тримання органів охорони державного кордону [105, ст. 26]. Загалом співвідношення контролю та нагляду сьогодні залишаються дискусійними серед науковців та чітко не розмежовані в законодавстві, але дане питання виходить за межі цього наукового дослідження.

Проаналізовані нормативні та теоретичні положення, пов'язані із поняттям «суб'єкт владних повноважень», дозволили визначити таку логічну послідовність: суб'єкт владних повноважень – органи державної влади – владні управлінські функції – владні повноваження. Отже, здійснення управлінських функцій є характерним для органів охорони державного кордону, що дає нам підстави вважати їх суб'єктами владних повноважень, а у контексті Закону України «Про інформацію» – суб'єктами інформаційних відносин [106, с. 73].

Наказ МВС України, яким затверджено «Положення про орган охорони державного кордону ДПСУ», закріплює, що орган охорони державного кордону є юридичною особою [100, п. 4, Р. IV]. З цього приводу, Цивільний кодекс України визначає юридичну особу як організацію, що створена і зареєстрована у встановленому законом порядку та визначає правові межі функціонування, – наділяється цивільною правоздатністю і дієздатністю, може бути позивачем і відповідачем у суді [107, ст. 80]. Згідно з ч. 2 ст. 81 Цивільного кодексу України (далі – ЦК України), органи охорони державного кордону є різновидом

юридичних осіб публічного права, тобто мають публічно-правову природу діяльності [107, ст. 81]. Це обумовлює виконання даними органами публічних повноважень. Статус юридичної особи публічного права більше властивий для органу охорони державного кордону як учасника цивільно-правових відносин.

Закон України «Про доступ до публічної інформації» у сфері доступу до публічної інформації визначає таких суб'єктів: *запитувачі* інформації (фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи, крім суб'єктів владних повноважень); *розпорядники* інформації (суб'єкти владних повноважень); *структурний підрозділ або відповідальна особа* з питань доступу до публічної інформації розпорядників інформації [97, ст. 12].

У межах ДПСУ функціонують структурні підрозділи, які спеціально призначені для забезпечення окремих напрямків інформаційної складової у сфері охорони державного кордону України. Оприлюднення публічної інформації за результатами функціонування ДПСУ здійснюється Управлінням апаратної роботи, посадовими особами відділу з питань взаємодії із ЗМІ та зв'язків з громадськістю Адміністрації ДПСУ, прес-службами регіональних управлінь та прес-секретарями органів ДПСУ. При цьому розповсюджувати інформацію про діяльність ДПСУ у засобах масової інформації дозволяється лише посадовим особам відділу з питань взаємодії із ЗМІ та зв'язків з громадськістю Адміністрації ДПСУ, прес-служб та прес-секретарям органів ДПСУ. Інші представники відомства надавати інформацію про діяльність ДПСУ у ЗМІ можуть лише за безпосереднім погодженням або за участю перерахованих вище осіб. У разі їхньої відсутності посадова особа, що надає ЗМІ інформацію за вказівкою керівника органу ДПСУ, повинна провести експертну оцінку щодо відсутності в ній відомостей з обмеженим доступом. Розповсюджувати інформацію про ДПСУ в ЗМІ з власної ініціативи посадовим особам органів ДПСУ категорично забороняється [108].

Організація та здійснення інформаційно-аналітичної діяльності, звітності про результати оперативно-службової діяльності ДПСУ, обмін відкритою статистичною інформацією покладається на Департамент інформаційно-аналітичного та документального забезпечення [109].

Окремою частиною центрального підпорядкування Адміністрації ДПСУ є Головний центр зв'язку, автоматизації та захисту інформації, який забезпечує функціонування та безпеку інформаційних систем ДПСУ. У зв'язку з необхідністю протистояти сучасним кіберзагрозам у прикордонній сфері у 2018 році у складі Головного центру зв'язку, автоматизації та захисту інформації було створено спеціальний структурний підрозділ – Центр кібербезпеки [110], який відповідальний за інформаційну безпеку та захист інформації, розпорядником якої є ДПСУ, також обробляє і зберігає інформацію у відомчих інформаційних системах, на основі використання сучасних інформаційних технологій.

Надання громадянам відповідей на питання консультаційного характеру в межах компетенції ДПСУ здійснює Контактний центр (служба «Довіри») [111].

Підрозділи документального забезпечення ведуть документування управлінської діяльності, організацію діловодства з документами, діловодства за зверненнями громадян, запитами на публічну інформацію згідно із постановою КМУ «Деякі питання документування управлінської діяльності» від 17.01.2018 р. № 55 та затвердженою наказом Адміністрації ДПСУ Інструкцією з діловодства в ДПСУ від 17.05.2004 р. № 400 та іншими керівними документами [112, п. 13.4].

Інформаційно-аналітичні підрозділи складаються з сектору інформаційного забезпечення та сектору аналізу ризиків. Ці підрозділи забезпечують обіг інформації шляхом її прийняття, оброблення, відбір за якісними та корисними показниками, формування статистичних даних тощо. Увесь обсяг інформації щодо оперативно-службової діяльності надходить, зберігається та передається підрозділами інформаційно-аналітичного забезпечення ДПСУ.

У межах функціонування ДПСУ здійснюється чіткий розподіл інформаційної діяльності за окремими напрямками: оприлюднення публічної інформації; надання консультування та прийняття заяв, звернень; забезпечення обігу оперативно-службової інформації; документування, робота з управлінськими, внутрішньоорганізаційними та індивідуальними документами; обробка електронної інформації; забезпечення захисту інформації. Така

інформаційна діяльність спеціальних суб'єктів пронизує всю структурну вертикаль ДПСУ. Чіткий розподіл інформаційної діяльності дозволяє в повному обсязі реалізовувати не тільки визначені у ст. 9 Законі України «Про інформацію» види інформаційної діяльності, але і забезпечити потреби ДПСУ у сфері безпеки державних кордонів та інформаційних прав усіх учасників прикордонних відносин.

На запитання «Чи мали Ви досвід роботи у ДПСУ з оприлюднення публічної інформації про ДПСУ, забезпечення безпеки та функціонування інформаційних систем, інформаційно-аналітичної діяльності, роботи із запитами і зверненнями громадян?» 60,1 % військовослужбовців ДПСУ відповіли «ні», а 39,9 % – «так» **(додаток В)**. Такі результати свідчать про те, що з розвитком інформаційного суспільства інформаційна діяльність набуває фахової спрямованості у функціонуванні органів влади.

Отже, проаналізовані положення дають нам підстави вважати, що з огляду на особливості інформаційного законодавства органи охорони державного кордону є суб'єктами інформаційно-правових відносин як суб'єкти владних повноважень, розпорядники інформації. Підтвердження такого статусу відображено в Інструкції «Про забезпечення доступу до публічної інформації у Державній прикордонній службі України», яка затверджена наказом Адміністрації ДПСУ [113]. Відповідно до цієї Інструкції «кожен з органів ДПСУ є розпорядником публічної інформації, яка отримана або створена ним у процесі здійснення своїх повноважень та перебуває в його володінні [113, п. 1.3]. Крім того, ДПСУ регулює всі інформаційні процеси, здійснює інформаційну діяльність, забезпечує функціонування та контроль інформаційно-телекомунікаційних технологій, обмін інформацією у межах інтегрованого управління кордонами та загалом реалізує державну інформаційну політику у прикордонному просторі.

Згідно зі ст. 5 Закону України «Про інформацію» можливості органів охорони державного кордону як учасників інформаційних відносин окреслюються питаннями одержання, використання, поширення, зберігання та захисту

інформації, яка є необхідної для забезпечення недоторканності державного кордону України на ділянці відповідальності. Загалом інформаційно-правові відносини, суб'єктом яких є ДПСУ, достатньо різноманітні та характеризуються динамічністю, стрімким розвитком, багатогранністю і залежністю від об'єктивних умов охорони державного кордону [91, с. 62].

Зміст інформаційних відносин (правосуб'єктність)

Суб'єктами інформаційних правовідносин, установлює І. В. Арістова, є особи, які беруть участь у конкретних правовідносинах і які є носіями інформаційних обов'язків та прав [6, с. 67]. Правосуб'єктність суб'єктів інформаційних правовідносин О. А. Баранов уособлює із потенційною здатністю бути учасником інформаційних правовідносин, а суб'єкт інформаційних правовідносин, є реальним учасником конкретних правовідносин [114, с. 49]. Л. П. Коваленко підсумовує, що наявність в особи правосуб'єктності є підставою визнання її суб'єктом інформаційних правовідносин. Суб'єктивні юридичні права й обов'язки у сфері інформаційної діяльності роблять осіб потенційно можливими учасниками інформаційних правовідносин [76, с. 7]. Під суб'єктами правовідносин в інформаційній сфері Д. Шпенов пропонує розуміти носіїв передбачених інформаційно-правовими нормами прав і обов'язків, що здатні ці права реалізовувати, а покладені обов'язки виконувати [115, с. 94].

І. М. Сопілко, досліджуючи інформаційні правовідносини за участю органів державної влади в Україні, піднімає проблемність їх правового регулювання з приводу отримання та надання інформації [20, с. 107]. На наш погляд, органи охорони державного кордону є учасниками ширшого кола правовідносин, які визначаються інформаційною правосуб'єктністю.

Суб'єктами інформаційних правовідносин стають у ході реалізації своїх юридичних прав та обов'язків, яких вони набувають при вступі у правовідносини. Характерною ознакою суб'єктного складу інформаційних правовідносин є визначення місця та ролі суб'єкта владних повноважень [76, с. 7]. Отже, органи охорони державного кордону реалізують свої повноваження як суб'єкти інформаційних відносин, під час безпосереднього виконання поставлених перед

ДПСУ завдань у межах визначеної ділянки, в інтересах забезпечення недоторканності державного кордону України та є повноправними учасниками інформаційних правовідносин відповідно до закріпленої нормативно-правовими актами інформаційної правосуб'єктності.

З урахуванням розвитку інформаційних правовідносин Є. О. Резченко вказує на проблемність правового регулювання інформаційних відносин в Україні, що потребує вирішення. Науковець наголошує на необхідності розробки та прийняття закону, що урегульовуватиме інформаційне забезпечення органів державної влади [116, с. 7]. До базових положень запропонованого Закону України «Про інформаційне забезпечення органів державної влади» Є. О. Резченко пропонує включити систему прав, обов'язків та відповідальності у сфері інформаційного забезпечення органів державної влади [116, с. 8].

Системне закріплення інформаційних прав та обов'язків учасників інформаційних відносин було у перших редакціях Закону України «Про інформацію», сьогодні ці статті із поточної редакції виключені. Тому підтримуємо позицію Є. О. Резченко щодо необхідності систематизації інформаційних прав та обов'язків органів державної влади. Науковець пропонує визначити такі права: право на формування програм інформаційного забезпечення; право на отримання відомостей про інформаційні системи, мережі, інформаційні ресурси та послуги з чіткими правами та відповідальністю; право органів державної влади щодо створення інформаційного забезпечення, розповсюдження інформації та інформаційних послуг; створення системи інформаційного забезпечення, технологій і засобів їх реалізації в порядку, що передбачено законами України «Про інформацію» та «Про захист інформації в автоматизованих системах» [116, с. 9].

Обов'язки органів державної влади в законі Є. О. Резченко вважає, що доцільно викласти у вигляді низки норм, відповідно до яких вони зобов'язані: формувати інформаційні ресурси відповідно до їх компетенції; видавати інформацію з державних ресурсів іншим державним органам, організаціям і фізичним особам в обумовлені строки; ефективно використовувати національні

інформаційні ресурси в процесі державного управління; забезпечувати схоронність та підтримку державних інформаційних ресурсів в актуальному стані; забезпечувати схоронність державної, комерційної, службової таємниці під час формування та використання інформаційних ресурсів [116, с. 9].

Здатність ДПСУ виступати учасником інформаційних відносин обумовлено відповідним інформаційно-правовим статусом, установлення якого є похідним від загальнотеоретичного розуміння правового статусу та нормативно-правового закріплення становища ДПСУ в механізмі держави й визначення її ролі в інформаційних правовідносинах. Реальний зміст досліджуваного правового статусу можливо розкрити за допомогою його структури або елементів. У юридичній теорії можна зустріти різні конструкції структури (елементів) правового статусу органу публічної влади.

У теорії держави і права правовий статус розглядається переважно через призму становища індивіда в суспільстві та державі, але відмінність поглядів щодо його елементів не знайшли єдиного розуміння серед науковців. Можна відокремити такі підходи до конструкцій правового статусу: права, свободи, обов'язки [117, с. 409]; суб'єктивні юридичні права, законні інтереси, юридичні обов'язки, гарантії здійснення прав і обов'язків [64, с. 62]; принципи правового статусу; громадянство; права і свободи людини; обов'язки людини [4, с. 278]; правові норми та принципи, що встановлюють даний статус; правосуб'єктність; громадянство (або інше відношення до країни перебування – без громадянства, іноземне громадянство або підданство); права, свободи та законні інтереси індивіда; обов'язки індивіда; юридична відповідальність. Причому серцевину, основу правового статусу, на думку Н. М. Крестовської, Л. Г. Матвєєвої, становлять права, свободи та обов'язки [53, с. 204].

У теорії адміністративного права адміністративно-правовий статус центрального органу влади розкривається за допомогою таких елементів, як: призначення, порядок утворення, реорганізація, ліквідація та місце в системі цих органів; завдання; структура [118]; становище керівника у системі управління, його повноваження, відповідальність [119, с. 32]; повноваження заступників;

утворення та правові підстави діяльності підпорядкованих підрозділів [85, с. 98–99]; межі нормотворчої діяльності [85, с. 100].

Проаналізовані погляди щодо елементів правового статусу дозволили визначити, що ключовими у ньому залишаються права й обов'язки, інші елементи доповнюють змістом правове становище органу у зв'язку з ускладненням і розвитком державно-правових відносин. Кожен орган виконавчої влади, діючи від імені та за дорученням держави, має певний правовий статус, виступає носієм відповідних повноважень юридично-владного характеру, реалізація яких забезпечує йому досягнення мети виконавчо-розпорядчої діяльності [120, с. 23]. З урахування теми нашого дослідження ще варто додати, що реалізація повноважень ДПСУ як учасника інформаційно-правових відносин здійснюється як у класичних (відносини з права власності на інформацію, реалізацією інформаційних прав), так і пов'язаних з техніко-технологічною складовою [14, с. 212] (відносини у сфері електронного урядування, документообігу, застосування інформаційно-телекомунікаційних систем, автоматизованих систем управління) відносинах.

Інформаційно-правовий статус ДПСУ визначений нормативно-правовими актами, які закріплюють її роль, місце, а також правові межі та можливості участі в інформаційно-правових відносинах, тобто знаходить свій вияв через інформаційну правосуб'єктність. Правосуб'єктність складається з низки взаємопов'язаних елементів. Однак у науці не досягнуто єдності розуміння відносно структури даної правової категорії. Одні дослідники ототожнюють її з правоздатністю, інші розглядають у ній два елементи – правоздатність і дієздатність, треті додають до цього ще й деліктоздатність і конкретні права й обов'язки, які виникають безпосередньо із закону [121, с. 101].

Ю. Нечипорук підкреслює, що суб'єктами інформаційного правовідношення є особи, які наділені інформаційною правосуб'єктністю, яка складається з інформаційної правоздатності (можливості мати інформаційні права й обов'язки) та інформаційної дієздатності (здатності своїми діями набувати інформаційних прав і створювати інформаційні обов'язки) [122, с. 42].

Реалізувати інформаційно-правовий статусу органів виконавчої влади, як зазначає М. Ю. Кузнецова, означає реалізувати їх відповідні суб'єктивні права й обов'язки в інформаційних правовідносинах [123, с. 133]. В. О. Качур визначає правосуб'єктність як соціально-юридичну властивість суб'єкта права, що полягає у його здатності мати права та обов'язки і вчиняти дії, що мають правові наслідки. При цьому пропонує вважати правосуб'єктність однією із соціально-юридичних властивостей суб'єкта права поряд з правовим статусом, правовим становищем тощо [124, с. 27]. Так, «правосуб'єктність» та «правовий статус» окремі правові категорії, але їх пов'язують такі структурні елементи, як права та обов'язки, без яких не може бути і суб'єкта інформаційно-правових відносин в особі ДПСУ.

Інформаційні права й обов'язки як елементи інформаційно-правового статусу ДПСУ визначають межі інформаційної діяльності у вигляді правових можливостей і дотримання, виконання та здійснення необхідних дій відповідно до законодавства, а чітко врегульований механізм втілення у реальні інформаційно-правові відносини у сфері охорони державного кордону відповідних прав та обов'язків дозволяє ДПСУ вчиняти дії, пов'язані з інформацією, що мають правові наслідки. Отже, зміст інформаційно-правового статусу ДПСУ тісно пов'язаний з інформаційною правосуб'єктністю.

На нашу думку, такі елементи правового статусу, як призначення, порядок утворення, реорганізація, ліквідація та місце в системі державно владних органів, структура ДПСУ (окрім її системно-структурних підрозділів, призначених для обробки, захисту інформації тощо), перебувають у межах адміністративно-правового статусу ДПСУ. Зі свого боку, інформаційно-правовий статус розкривають такі його елементи: правові підстави участі у правовідносинах з приводу інформації; завдання інформаційної діяльності; система спеціальних підрозділів, діяльність яких спрямована на забезпечення та реалізацію інформаційних потреб ДПСУ; інформаційна правосуб'єктність (права й обов'язки) посадових осіб ДПСУ щодо інформаційної діяльності [125, с. 51].

Інформаційно-правовий статус ДПСУ закріплений у Конституції України та чинних нормативно-правових актах. Конституція України визначає основні

інформаційні права суб'єктів інформаційних відносин (зокрема фізичних осіб), чим обумовлює встановлення відповідних обов'язків (забезпечення прав) у органів державної влади. Норми Основного закону визначають такі обов'язки ДПСУ в інформаційній сфері: інформаційна безпека України повинна бути серед пріоритетних напрямків діяльності всіх структурних органів і підрозділів ДПСУ як найважливіша функція держави [126, ст. 17]; організацію роботи слід здійснювати з урахуванням установленого обмеження обігу інформації в державі (державна або інша захищена законом таємниця) [126, ч. 3 ст. 32]; забезпечувати дотримання інформаційних прав інших суб'єктів інформаційних правовідносин, зокрема фізичних осіб: свобода особистого і сімейного життя [126, ч. 1 ст. 32]; таємниця листування, телефонних переговорів, телеграфної та іншої кореспонденції [126, ст. 31]; право громадянина не зазнавати втручання в його особисте та сімейне життя шляхом збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, знайомитися в органах державної влади, органах місцевого самоврядування, установах та організаціях із відомостями про себе [126, ч. 3 ст. 32]; право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір [126, ст. 34].

Також важливими у правовому регулюванні інформаційних відносин та визначенні в них ролі ДПСУ є базові закони з інформаційного прав та у сфері охорони державного кордону. Діяльністю ДПСУ, спрямованою на реалізацію основних напрямків державної інформаційної політики, є: забезпечення доступу кожного до інформації; забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; створення умов для формування в Україні інформаційного суспільства; забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень; створення інформаційних систем і мереж інформації, розвиток електронного урядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки

України; сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору [57, ст. 3].

У Законі України «Про Державну прикордонну службу України» серед основних функцій ДПСУ визначено «ведення розвідувальної, інформаційно-аналітичної та оперативно-розшукової діяльності в інтересах забезпечення захисту державного кордону України згідно із законами України «Про розвідувальні органи України» та «Про оперативно-розшукову діяльність»» [79, ч. 1 ст. 2]. З цієї норми можна зрозуміти, що інформаційно-аналітична діяльність здійснюється тільки в межах оперативно-розшукової діяльності, оскільки за правову основу визначені закони, що врегульовують не інформаційну, а оперативно-розшукову діяльність. Дана функція продубльована і як обов'язок ДПСУ у п. 10 ст. 19 Закону України «Про Державну прикордонну службу України». Обов'язком ДПСУ також є надання за запитами компетентних органів влади відомостей, що зберігаються в інформаційних системах, у тому числі банках даних, стосовно осіб, які в період одержання допомоги по безробіттю перетинали державний кордон України або перебували за межами України [79, п. 23-1 ст. 19].

До прав в інформаційній сфері ДПСУ належать: створення і використання в інтересах забезпечення охорони державного кордону України інформаційних системи, банків даних щодо осіб, які перетнули державний кордон України, осіб, які вчинили правопорушення, яким згідно із законодавством не дозволяється в'їзд в Україну тощо [79, п. 10 ст. 20]; здійснення автоматизованого обміну інформацією про транспортні засоби, що перетнули державний кордон України, з терторіальними органами МВСУ [79, п. 19 ст. 20]. Права та обов'язки ДПСУ з приводу здійснення діяльності, пов'язаної з інформацією, сьогодні не відображають весь спектр інформаційних правовідносин, учасником яких є прикордонне відомство.

Інформаційно-правовий статус є багатоелементною й багатоаспектною категорією та юридичним закріпленням положення ДПСУ в інформаційному суспільстві. Інформаційно-правовий статус ДПСУ є частиною його

адміністративно-правового статусу у сфері забезпечення недоторканності державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні як суб'єкта інформаційно-правових відносин.

Межі діяльності ДПСУ пов'язані з інформацією, охоплюють набагато більше напрямків, ніж це визначено у Законі України «Про Державну прикордонну службу України», а отже і інформаційно-правовий статус є ширшим від закріплених його меж у цьому Законі. Вважаємо, що доцільно виділяти окрему інформаційну функцію в діяльності ДПСУ у зв'язку з розвитком і збільшенням обсягів діяльності, пов'язаної з інформацією у сфері охорони державного кордону.

Сьогодні питання інформаційної правосуб'єктності органів охорони державного кордону, як і загалом органів державної влади, чітко не визначені й несистематизовані. Відносно суб'єктів владних повноважень, у тому числі органів охорони державного кордону, їх інформаційна правосуб'єктність передбачена у значній кількості нормативно-правових актів, що, як правило, закріплюють обов'язки щодо оприлюднення офіційної публічної інформації, надання відповідей за запитами (зверненнями) та захисту інформації з обмеженим доступом, забезпечення захисту інформації тощо. Загалом, визначення та конкретизація інформаційних прав та обов'язків органів охорони державного кордону перебуває у системній залежності та зв'язку з актуальною потребою упорядкування інформаційного законодавства, що буде нами детально висвітлено у розділі 5.

Об'єктом інформаційних відносин у сфері діяльності ДПСУ, як і будь-яких інших інформаційних відносин, є інформація, що містить відомості, пов'язані з формуванням, використанням, поширенням, збереженням та охороною даних щодо функціонування органів охорони державного кордону, їх особового складу, порядком перетинання державного кордону України, здійсненням діяльності в прикордонному просторі, настанням відповідальності за порушення норм інформаційного законодавства.

У сучасному світі інформація має велику багатоманітність і потребує чіткого правового розмежування. Особливої актуальності набуває диференціація інформації, яка пов’язана з діяльністю державних органів влади. Поняття та види інформації знайшли відображення у багатьох наукових працях з різних наукових спеціальностей, юридичного, технічного та іншого спрямування. Але нас насамперед цікавить інформація та її види, розпорядником якої є ДПСУ. Частково дана проблематика досліджувалась у працях: В. М. Брижака, О. М. Гальченка, В. Л. Зьолки, Р. А. Калюжного, О. В. Копана, О. Г. Марценюка, А. І. Марущака, В. С. Цимбалюка, М. Я. Швеця та багатьох інших. Окремо необхідно виділити дослідження інформації, яка є предметом інформаційних правовідносин за участю органів державної влади Т. В. Гаман, І. М. Сопілко, О. О. Тихомирова, О. І. Яременко та інші. Але при цьому характеристика змісту та видів інформації, розпорядником якої є ДПСУ, не отримала належного наукового вивчення [98].

Інформація як об’єкт інформаційних відносин є складною, динамічною і досить різноманітною, про що свідчить пошук законодавця у визначенні її оптимальних різновидів, а також наявності різних наукових поглядів і підходів.

Інформація, як визначено у Законі України «Про інформацію», це – будь-які відомості та (або) дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [57, ч. 4, ст. 1]. За цим Законом інформація за змістом поділяється на такі види:

інформація про фізичну особу;

інформація довідково-енциклопедичного характеру;

інформація про стан довкілля (екологічна інформація);

інформація про товар (роботу, послугу);

науково-технічна інформація;

податкова інформація;

правова інформація;

статистична інформація;

соціологічна інформація;

інші види інформації [57, ст. 10]; з

а порядком доступу: відкрита інформація та інформація з обмеженим доступом [57, ст. 20]. Окремо цим Законом відокремлена масова інформація, що поширюється з метою її доведення до необмеженого кола осіб [57, ч. 1 ст. 22].

Досліджуючи види інформації за законодавством України, Ю. О. Гелич зауважує, що за таким поділом неможливо визначити єдиний критерій для подібної класифікації інформації, оскільки багато понять пересікаються за змістом, наприклад, правова інформація та податкова тощо [127, с. 85].

Попередня редакція Закону України «Про інформацію» від 06.01.2011 р., визначала поняття «галузі інформації як сукупності документованих або публічно оголошених відомостей про відносно самостійні сфери життя і діяльності суспільства та держави», і визначала такі галузі інформації: політична, економічна, духовна, науково-технічна, соціальна, екологічна, міжнародна [128, ст. 17]. Стаття 18 закріплювала такі основні види інформації: статистична інформація; адміністративна інформація (дані); масова інформація; інформація про діяльність державних органів влади та органів місцевого самоврядування; правова інформація; інформація про особу; інформація довідково-енциклопедичного характеру; соціологічна інформація; податкова інформація [128, ст. 18].

За зовнішніми ознаками досліджувану нами сферу інформаційних відносин можна віднести за таким підходом до адміністративної інформації та інформації державних органів. Під адміністративною інформацією (даними) розуміються офіційні документовані дані, що дають кількісну характеристику явищ і процесів, що відбуваються в економічній, соціальній, культурній, інших сферах життя і збираються, використовуються, поширюються та зберігаються органами державної влади, органами місцевого самоврядування, юридичними особами відповідно до законодавства з метою виконання адміністративних обов’язків та завдань, що належать до їх компетенції [128, ч. 1 ст. 19-1]. Інформація про діяльність державних органів влади та органів місцевого самоврядування розглядається як офіційна документована інформація, яка створюється у процесі поточної діяльності законодавчої, виконавчої та судової влади, органів місцевого

самоврядування [128, ч. 1 ст. 21]. Попередня редакція Закону України «Про інформацію» від 06 січня 2011 р. надавала більше можливостей віднесення досліджуваної сфери до одного з видів інформаційних відносин, на відміну від поточної редакції цього Закону. Тому продовжимо наш пошук у наукових джерелах, у багатьох із яких підкреслюється складність і відсутність одностайної класифікації інформаційних відносин у зв'язку із законодавчою невизначеність та їх особливою роллю в державі і суспільстві.

Інформацію в органах державного управління Т. В. Гаман класифікує за різними підставами й ознаками: офіційна і неофіційна; горизонтальна і вертикальна; за змістом і цільовим призначенням; можливими соціальними наслідками; ступенем доступності; за джерелом виникнення і напрямком руху; за ознакою щодо середовища формування; за засобом вираження; за ступенем стабільності і визначеності, а також на основі її співвідношення з часом (інформація про минуле, у режимі реального часу, прогнози на майбутнє) [129, с. 308].

Вважаємо, що розподіл інформації на офіційну та неофіційну є недоречним, у зв'язку з тим, що інформація, якою володіє державний орган влади завжди є офіційною. Ця позиція обґрунтована тим, що такі поняття, як «офіційна інформація», «офіційні джерела» пов'язуються з діяльністю органів державної влади [39, с. 104; 130, с. 102], із законною діяльністю [131], спеціально уповноваженим компетентним органом, державним службовцем чи посадовою особою на підставі службового обов'язку [53, с. 402].

Ознаку офіційності можна виокремити також із суміжних категорій. Так, зокрема офіційним документом є документ, який має юридичну силу. Офіційними документами вважаються перш за все урядові документи, матеріали, постанови, декрети, заяви, стенограми офіційних засідань, дані державної та відомчої статистики, архіви і поточні документи різних установ, організацій, ділова кореспонденція, протоколи судових органів, прокуратури, нотаріату тощо. Основними атрибутами офіційного документа вважається підпис посадової особи та/або реєстрація у встановленому порядку. До неофіційних документів належать

особисті матеріали, виконані на основі власних спостережень [132]. Виходячи з цього, вважаємо, що в розпорядженні ДПСУ знаходиться тільки офіційна інформація, а неофіційна не пов'язана з діяльністю органів державної влади. Навіть коли інформація отримана з неофіційних джерел, наприклад від негласних джерел у ході оперативно-розшукової діяльності ДПСУ, з моменту її фіксування вона набуває офіційного характеру [98].

Нормативно закріплено, що «офіційна інформація органів державної влади та органів місцевого самоврядування» (офіційна інформація) – це офіційна документована інформація, створена у процесі діяльності органів державної влади й органів місцевого самоврядування, яка доводиться до відома населення в порядку, установленому Конституцією України [133, ст. 1]. Тобто офіційна інформація має дві основні ознаки: публічності та оприлюднення. У Законі України «Про доступ до публічної інформації» публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом [97, ч. 1 ст. 1]. У ст. 6 Закону України «Про доступ до публічної інформації» визначено, що публічна інформація може бути з обмеженим доступом (конфіденційна, таємна, службова) [134]. Тоді втрачається сенс публічності у такій інформації, якщо вона обмежена у доступі до неї та зважаючи на те, що публічний означає такий, що оприлюднюється; відбувається в присутності публіки, людей; призначений для широкого відвідування, користування; громадський. Отже, уся інформація, яка знаходиться у володінні ДПСУ, тобто пов'язана зі сферою охорони державного кордону та її забезпеченням, є офіційною, а та її частина, що має відкритий доступ, – публічною [98]. На підтримку нашого міркування знаходимо визначення публічної інформації у докторській дисертації Д. О. Маріц, під яким науковець розглядає офіційну відкриту інформацію, яка зберігається на відповідному матеріальному носії, електронному ресурсі, що передбачає вільний

доступ до такої інформації або надається на підставі запиту у визначений строк згідно з принципом відкритості і прозорості діяльності суб'єктів владних повноважень [17, с. 249].

З урахування конкретної сфери діяльності ДПСУ у її інформаційних джерелах визначено такі види інформації, якими володіє розпорядник (ДПСУ) за змістом: інформація про фізичну особу; інформація довідково-енциклопедичного характеру; науково-технічна інформація; правова інформація; статистична інформація; соціологічна інформація; інші види інформації [135]. Цей перелік не є виключним і, на наш погляд, потребує детального аналізу.

Відомості про особу в діяльності ДПСУ складають велику частину всієї інформації у розпорядженні відомства. Такий вид інформації стосується осіб: які перетинають державний кордон, порушують прикордонне законодавство, можуть перетнути кордон (але яким заборонено його перетинання, знаходяться в базах даних правоохоронних органів України, Інтерполу тощо); сприяють охороні державного кордону (членів добровільних громадських формувань з охорони громадського порядку і державного кордону); усіх військовослужбовців та працівників ДПСУ [98].

Інформація довідково-енциклопедичного характеру пов'язана із систематизованими, документованими, публічно оголошеними або іншим чином поширеними відомостями про діяльність ДПСУ. Така інформація може бути про результати оперативно-службової діяльності, основні терміни та категорії у прикордонній сфері, обстановку в контрольних пунктах в'їзду-виїзду на лінії розмежування, порядок перетинання державного кордону її громадянами, іноземцями, дітьми тощо. Вона може бути відображена в енциклопедіях, словниках, довідниках, буклетах, повідомленнях та оголошеннях (наприклад, про оголошення початку та умови вступу до НАДПСУ), картографічних матеріалах, електронних базах та банках даних, архівах різноманітних довідкових інформаційних служб, мереж та систем, а також звітах про діяльність ДПСУ (наприклад, «Стратегічний бюлетень прикордонної безпеки. Біла книга») та автоматизованих інформаційно-телекомунікаційних системах [57, ч. 2 ст. 12].

До науково-технічної інформації ДПСУ належать будь-які відомості та/або дані про досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської та громадської діяльності у прикордонній сфері, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [57, ч. 1 ст. 15]. Науково-технічна інформація спрямована на підтримання всіх сфер і напрямків діяльності ДПСУ, підтримання взаємозв'язків з іноземними прикордонними службами, взаємодіючими органами України, розвитком технічного забезпечення прикордонних підрозділів, міжнародного технічного співробітництва в межах проекту Twinning тощо. Такий вид інформації міститься в монографіях, збірниках, періодичних виданнях, навчальній літературі, дисертаціях, звітах про науково-дослідну роботу та інших джерелах [136].

Спеціалізованими установами у формуванні науково-технічної інформації є НАДПСУ та Головний експертно-криміналістичний центр. Організацію та координацію заходів, пов'язаних із науковою та науково-технічною діяльністю в НАДПСУ, здійснює окремий підрозділ – науково-дослідний відділ.

Правову інформацію утворюють будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо [57, ч. 1 ст. 17]. Формами закріплення правової інформації є Конституція України, система законодавчих і підзаконних нормативно-правових актів, міжнародних договорів та угод, норм і принципів міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань [57, ч. 2 ст. 17].

Правова інформація є соціально важливою інформацією, яка відображає нормативні (загальнообов'язкові) або індивідуальні вимоги до поведінки (діяльності) суб'єктів, що відповідають інтересам суспільства та забезпечуються й охороняються державою [137, с. 32]. Під правовою інформацією також розуміють зміст даних (повідомлень), використання яких допомагає вирішити те або інше правове завдання чи сприяє його вирішенню [138, с. 10]. Принциповою вимогою

такого виду інформації є її необхідність доведення до персоналу ДПСУ та інших зацікавлених осіб й усвідомлення її усіма суб'єктами як основного та єдиного механізму урегулювання прикордонних відносин. Правова інформація у сфері охорони державного кордону формує бажану для ДПСУ поведінку суб'єктів, які перетинають (намагаються перетнути) державний кордон України, проживають у контрольованих прикордонних районах або здійснюють діяльність у прикордонній смузі для забезпечення прикордонної безпеки, поведінки працівників (належне виконання обов'язків) ДПСУ [98].

До правової інформації, яка знаходиться у володінні і під контролем ДПСУ, належать будь-які відомості і про юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику у сфері охорони державного кордону, підзаконні нормативно-правові акти, прийняті уповноваженими особами ДПСУ та інше [98].

Статистична інформація містить відомості, що надають кількісну характеристику явищам і процесам, які відбуваються у сфері діяльності органів і підрозділів охорони державного кордону. Ця інформація надається в документованій формі та підлягає систематичному оприлюдненню (за винятком тієї, яка обмежена в доступі). Статистична інформація у прикордонній сфері є різновидом інформації, розпорядником якої є ДПСУ, що являє собою сукупність відомостей, які відображають результати оперативно-службової діяльності за певний період (кількість пропущених через державний кордон осіб, кількість осіб, що отримали відмову у пропуску, скільки виявлено нелегальних мігрантів тощо) та інша статистична інформація [98].

Соціологічна інформація у сфері діяльності ДПСУ передбачає різноманітні задокументовані відомості про суспільство, суспільні відносини в межах виконання завдань. Така інформація отримується з імміграційної картки іноземця, бази даних «Відомості про осіб, які перетнули державний кордон України», під час вивчення та узагальнення соціологічних даних про населення, що проживає в прикордонних районах, анкетування персоналу ДПСУ тощо [98].

Перелік видів інформації у статті 10 Закону України «Про інформацію», якою володіє ДПСУ, не є вичерпними, оскільки закінчуються пунктом «інші види інформації». Цим допускається можливість виникнення нових видів інформації, тоді вони будуть підпадати під зазначену норму законодавства [14, с. 235].

Довідково-енциклопедична, науково-технічна, правова, статистична, соціологічна інформація надається за запитами на інформацію, які подано поштою, факсом, телефоном, електронною поштою та особисто до громадської приймальні Адміністрації ДПСУ [139].

Окремий розподіл інформації на види, розпорядником якої є ДПСУ, передбачає критерії «за порядком доступу»: відкрита інформація та інформація з обмеженим доступом (конфіденційна, таємна та службова інформація) [97, ст. 20, 21]. Тобто всі види інформації за змістом можуть бути обмежені в доступі, що визначено характером виконуваних завдань із забезпечення прикордонної безпеки держави [98].

У законодавстві закріплені інші види інформації, зокрема Закон України «Про державну статистику» (ст. 1) визначає такі види: адміністративні дані – дані, отримані на підставі спостережень, проведених державними органами (за винятком органів державної статистики), органами місцевого самоврядування та іншими юридичними особами відповідно до законодавства та з метою виконання адміністративних обов’язків і завдань, віднесених до їх компетенції [140, ст. 1]; конфіденційна інформація – статистична інформація, яка належить до інформації з обмеженим доступом і знаходиться у володінні, користуванні або розпорядженні окремого респондента та поширюється виключно за його згодою відповідно до погоджених з ним умов [140, ст. 1].

У юридичній доктрині сформувалися різні підходи до класифікації інформації, зокрема Б. А. Кормич класифікує інформацію за наскрізним критерієм (одна і та ж сама інформація може одночасно класифікуватися за декількома підставами), а саме: порядок або режим доступу до інформації; порядок реалізації права на інформацію; спосіб поширення інформації; вид інформації за змістом

[141, с. 299]. Усі підстави крім останньої, відображають динамічні процеси, які можуть відбуватись з інформацією у різних її виявах.

А. І. Марущак, підкреслюючи не універсальність законодавчої класифікації інформації, пропонує свою класифікацію: приватноправового характеру – публічно-правового; обігоздатна – необігоздатна; загальнодоступна – нерозкрита (з обмеженим доступом); приватна – офіційна; для комерційного використання – для вільного, звичайного, наукового, освітянського використання [12, с. 19].

І. М. Сопілко слушно зауважує, що класифікація інформації має не лише суто теоретичне, а й значне практичне значення [20, с. 75]. А. В. Погорілецька умовно існуючу інформацію, залежно від осіб, у розпорядженні яких вона знаходиться, поділяє на приватну, тобто інформацію, що знаходиться у володінні конкретної приватної особи, офіційну – інформацію, що знаходиться у володінні державного органу влади та органів місцевого самоврядування, і публічну інформація – інформація, отримана або створена у процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації [142, с. 131–132].

В. М. Плішкін пропонує всю інформацію поділяти на такі види: відповідно до сфери виникнення: елементарна нежива природа; біологічна (світ тварин і рослин); соціальна (людське суспільство); залежно від способу передачі та сприйняття: візуальна (передається і сприймається візуальними образами); аудіальна (звуками); тактильна (відчуттями); смакова (запахами); машинно-орієнтована (сприймається і обробляється ЕОМ); за соціальною орієнтацією в науці виділяють масову (інформація, яка адресується найширшому колу споживачів), особисту (орієнтована на точно визначеного індивідуума або певну групу осіб) і спеціальну інформацію (розрахована на спеціалістів, може бути науковою або художньою, технічною або гуманітарною і т. ін. Спеціальну інформацію часто поділяють за сферами людської діяльності за галузевим принципом). Крім того, зазначає В. М. Плішкін, інформацію умовно поділяють на

естетичну (пов'язується із виникаючим у природі різним сполученням звуків, запахів, світла, кольорів і тіней) та семантичну (виникає в результаті різної діяльності людей). У правоохоронній сфері прикладом семантичної інформації може бути повідомлення про вчинений злочин. Інформація, яка зібрана на місці злочину, також є семантичною. Вона – результат криміналістичної діяльності працівників органів внутрішніх справ) [143, с. 320].

Задіяні в анкетуванні респонденти зазначили, що під поняттям «інформація» у сфері діяльності ДПСУ вони розуміють відомості, пов'язані із порядком функціонування органів охорони державного кордону та порядком перетинання державного кордону (61,5 %), відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді у сфері діяльності ДПСУ (55,8 %), дані про факти (кількість) перетинання державного кордону (53,5 %), інформація про джерела та зміст норм права, що врегульовують діяльність ДПСУ (47,8 %), дані про результати (показники) діяльності посадових осіб (підрозділів) ДПСУ (46 %), інформація про персонал відомства (40,7 %), об'єкт інформаційних відносин у діяльності ДПСУ (28,3 %). Отже, отримані результати свідчать про практичне (повсякденне) розуміння інформації у сфері діяльності ДПСУ її представників, а не законодавчо закріплене, на яке надали найменше відповідей (28,3 %). На запитання «З яким видом інформації Вам частіше доводилось стикатись у своїй службовій діяльності?» із запропонованих варіантів 33,6 % обрали – «інформація про фізичну особу», 26,1 % вказали «інформація довідково-енциклопедичного характеру», 31 % зазначили науково-технічну інформацію, 49,1 % – правову інформацію, 32,7 % – статистичну інформацію, 19 % – соціологічну інформацію; 57,2 % – відкриту й 33,6 % – інформацію з обмеженим доступом **(додаток В)**.

Інформація у прикордонній сфері має зовнішній (про порядок перетинання державного кордону) та внутрішній (функціонування прикордонного відомства) напрямок. Зовнішня інформація є доступною та відкритою для широкого загалу суб'єктів правових відносин. До неї можна віднести дані, що містяться: у

нормативно-правових актах про правовий статус, структуру, повноваження ДПСУ, про порядок та особливості перетинання державного кордону в пунктах пропуску через державний кордон (закони України «Про Державну прикордонну службу України», «Про прикордонний контроль» та інші); відомостях про результати діяльності органів охорони державного кордону України, що постійно висвітлюються в засобах масової інформації, на офіційному сайті Адміністрації ДПСУ, в аналітичних звітах тощо.

Нормативне закріплення умов перетинання державного кордону міститься, в законах України «Про державний кордон України», «Про прикордонний контроль», постанові КМУ «Про затвердження Правил перетинання державного кордону громадянами України» та інших нормативно-правових актах. Крім того, таку інформацію можна отримати в засобах масової інформації, які висвітлюють діяльність прикордонного відомства. Також доступним для інформування громадян є офіційний сайт Адміністрації ДПСУ, а саме розділ «Перетинання кордону». У ньому міститься інформація за окремими розділами: порядок перетинання державного кордону громадянами України; виїзд за кордон неповнолітніх дітей – громадян України та інші. Закон України «Про звернення громадян» дає можливість отримувати інформацію шляхом подання заяви або клопотання з приводу реалізації особистих прав і законних інтересів.

Внутрішня інформація частково переплітається із зовнішньою, але має деякі особливості, пов’язані із характером виконуваних завдань і забезпеченням управління підпорядкованими підрозділами. Така інформація може бути обмежена у доступі [57, ст. 21], яка стосується всього персоналу та виконання службових обов’язків (службова), окремого військовослужбовця (працівника) ДПСУ (конфіденційна) чи окремих посадових осіб (таємна).

За колом суб’єктів: масова (для необмеженого кола суб’єктів: перелік діючих пунктів пропуску через державний кордон і пунктів контролю [144]), для обмеженого кола суб’єктів (службова інформація, або інформація, доступна для осіб, що мають доступ до державної таємниці), індивідуальна (персональна інформація, наприклад, про місце проживання військовослужбовця, інформація

про перетинання фізичною особою державного кордону України, про наявність або відсутність стосовно фізичної особи тимчасового обмеження у праві виїзду з України або в'їзду в Україну).

Інформація про внутрішню діяльність ДПСУ міститься у таких джерелах, як: нормативно-правові акти, які регламентують діяльність ДПСУ та порядок і правила перетинання державного кордону України; повідомлення компетентних посадових осіб держави про організаційні та штатні зміни в діяльності прикордонної служби (наприклад, звернення Президента України до народу з повідомленням про безвізовий режим з країнами ЄС); публікації, розміщені на офіційному сайті ДПСУ, її органів і підрозділів; повідомлення та роз'яснення прес-служби Адміністрації ДПСУ та відповідних посадових осіб відомства; публікації, розміщені в офіційних друкованих джерелах «Прикордонник України», «Кордон» тощо; у матеріалах за результатами звернень громадян та з повідомлень, отриманих від служби «Довіра» (надання громадянам України, іноземцям та особам без громадянства відповідей на питання консультаційного характеру в межах компетенції ДПСУ) [91, с. 59-60].

Уся інформація, пов'язана із діяльністю ДПСУ, поділяється за правовим режимом доступу на інформацію відкриту й обмежену (службова, таємна, конфіденційна). До відкритої інформації у прикордонній сфері належить будь-яка інформація про перетинання державного кордону, про його охорону та діяльність ДПСУ у разі, якщо вона не віднесена законом до інформації з обмеженим доступом. До інформації з обмеженим доступом Законом України «Про інформацію» належить: конфіденційна, таємна та службова інформації [57, ч. 1 ст. 21]. Детально особливості інформації у прикордонній сфері відкритої та з обмеженим доступом буде розглянуто в наступних підрозділах цього дослідження.

Інформація, пов'язана із діяльністю ДПСУ, закріплюється у відповідних формах. Класичною і найбільш історично-тривалою формою є документування у вигляді службової документації, відповіді на різноманітні запити тощо. Більш сучасною та зручною формою є електронні носії та мережа Інтернет, поширена

усно в засобах масової інформації; поширення в офіційних друкованих виданнях (наприклад, газети «Урядовий кур'єр», «Прикордонник України»). Разом зі зручністю електронного спілкування (отримання, обміну, направлення запиту інформацією) сьогодні існують проблеми нормативного та організаційного характеру щодо ідентифікації особи, збереження та захисту інформації, що потребує окремого обговорення у напрямку вдосконалення.

Важливою для сучасного демократичного суспільства та забезпечення цивільного контролю є отримання інформації про діяльність органів державної влади. У ДПСУ інформація звітного характеру має такі напрямки: про стан охорони державного кордону (прикордонної служби, прикордонного контролю, Морської охорони, прикордонної авіації, аналіз ризиків); щодо здійснення державної регуляторної політики у межах діяльності відомства (розроблення, відстеження, планування діяльності з підготовки проектів регуляторних актів, недопущення прийняття регуляторних актів, які є недоцільними, непослідовними або не узгоджуються чи дублюють чинні регуляторні акти; оприлюднення проектів регуляторних актів на офіційному веб-сайті ДПСУ (наприклад, наказ Адміністрації ДПСУ, Міністерства фінансів України (далі – МФ України), Міністерства інфраструктури України (далі – Мінінфраструктури) від 27 квітня 2012 р. № 291/506/228 «Про затвердження Порядку подання авіа перевізникам або уповноваженим ними особами попередньої інформації про пасажирів, імпортні та транзитні вантажі, які перевозяться повітряними суднами, органам охорони державного кордону та митним органам») [145] та інше; виконання міжнародних Угод, забезпечення Європейської інтеграції, результати співпраці з урядами іноземних країн та міжнародними організаціями, залучення міжнародної технічної допомоги; фінансовий звіт про витрачання бюджетних коштів; стан роботи з громадськістю (проведення громадських обговорень, консультацій, сприяння діяльності громадських об'єднань: Громадської ради Адміністрації ДПСУ, Об'єднаної профспілкової організації ДПСУ, Всеукраїнської організації ветеранів-прикордонників); стан роботи з персоналом (інформування про порядок прийняття на службу за контрактом, вступу на навчання у НАДПСУ, охорона

здоров’я персоналу, забезпечення житлом, спортивні досягнення, інформація для учасників АТО/ООС, дотримання люстрації влади) [98].

За державно-правовим та суспільним схваленням інформація може бути позитивна та негативна.

Позитивна – це інформація про діяльність та результативність прикордонного відомства про належне виконання завдань, попереджувальна інформація про зміни в законодавстві щодо порядку та правил перетинання державного кордону України. Останні роки актуальною є інформація про запровадження в діяльності ДПСУ сучасних європейських методів, способів і засобів охорони державного кордону, міжнародна співпраця, у тому числі у межах проекту Twinning (технічної співпраці).

Негативна, містить відомості про порушення прикордонного законодавства, виявлені факти протиправної діяльності посадових осіб ДПСУ, у тому числі і про корупційні явища, інформація про черги на державному кордоні при проведенні прикордонного контролю з різних причин та інше.

Поширення інформації має важливе не тільки національне, але і транскордонне значення, саме тому інформацію у сфері охорони державного кордону доречно розглядати за територіальним значенням: міжнародного значення (про узгодження особливостей перетинання державного кордону із суміжною державою, проведення спільного патрулювання, прикордонного контролю); загальнодержавної вагомості (правила та порядок в’їзду-виїзду з території України, установлений режим у пунктах пропуску через державний кордон України, порядок виїзду з території України дітей); регіонального значення (запровадження додаткових тимчасових обмежень на ділянці відповідальності прикордонного загону); локального (місцевого) характеру (порядок роботи місцевого пункту пропуску через державний кордон України та спрощене його перетинання місцевими громадянами).

Отже, проаналізоване вище дозволило нам сформулювати такі критерії для розмежування інформації в діяльності ДПСУ:

1. За характером: офіційна, публічна.

2. За напрямком діяльності: внутрішня і зовнішня.

3. За доступністю: відкритого і обмеженого (службова, таємна, конфіденційна) доступу.

4. За сутністю: правила перетинання державного кордону; факти перетинання державного кордону; результати діяльності посадових осіб (підрозділів) ДПСУ тощо.

5. За результатами службової діяльності ДПСУ: звіт про результати охорони державного кордону; реалізація державної регуляторної політики в межах діяльності відомства; виконання міжнародних угод; фінансовий звіт про витрачання бюджетних коштів; стан роботи з громадськістю; стан роботи з персоналом.

6. За очікуваним результатом: зменшення правопорушень на державному кордоні; мінімізація відмов у пропуску внаслідок поінформованості громадян щодо умов перетинання державного кордону; недопущення протиправної діяльності серед персоналу ДПСУ тощо.

7. За способом доведення: усна проста, усна візуалізована, письмова проста, письмова під підпис (про отримання повідомлення); електронна.

8. За формою вираження: мовна, документальна, електронна, аудіо, візуальна, он-лайн.

9. За формою візуалізації: текстова, числова, графічна, зображення, інтерактивна мапа [98].

10. За територіальним спрямуванням: міжнародного, державного, регіонального та локального значення.

11. За державно-правовими та суспільним схваленням: позитивна та негативна.

Інформація усіх видів має самостійну цінність, створює основу для нормативних документів як на міжнародному, державному, так і регіональному рівнях. Вона має свої специфічні закономірності функціонування і розвитку, здатна до випереджального впливу на державну прикордонну політику, виступає безпосередньою причиною, що визначає вибір того чи іншого варіанта

управлінського рішення [129, с. 308] Адміністрації ДПСУ, а також дій прикордонних органів і підрозділів. Розподіл інформації на види обумовлює відповідні види інформаційних ресурсів, а відповідно і режим доступу до них [24, с. 58]. Отже, чинне інформаційне законодавство України містить положення, які визначають зміст і правові ознаки різноманітної інформації як об'єкта суспільних відносин. Державна прикордонна служба України володіє та розпоряджається інформацію, вступаючи при цьому в різноманітні інформаційні відносини. Саме тому диференціація інформації, розпорядником якої є ДПСУ, має важливе як теоретичне, так і практичне значення [98].

Отже, проведений нами аналіз структури інформаційних відносин у діяльності ДПСУ дозволив нам визначити, що інформаційні відносини розкривають такі елементи, як: суб'єкт інформаційних правовідносин; зміст (інформаційно-правовий статус суб'єкта); об'єкт інформаційних правовідносин. Ці елементи мають специфічні особливості, пов'язані з діяльністю ДПСУ в забезпеченні охорони державного кордону України.

Суб'єкт відносин у цій сфері є загальний та особливий (центральний). До загального суб'єкта належать фізичні та юридичні особи, громадські організації тощо, який мають інтерес чи право, пов'язане з інформацією у сфері діяльності ДПСУ. Особливим суб'єктом є всі структурні підрозділи та посадові особи ДПСУ. У межах ДПСУ функціонують спеціальні суб'єкти (Управління апаратної роботи, Департамент інформаційно-аналітичного та документального забезпечення, Головний центр зв'язку, автоматизації та захисту інформації, Контактний центр (служба «Довіра»), підрозділи документального забезпечення, інформаційно-аналітичні підрозділи), правовий статус яких обумовлюється призначенням, – безпосереднє здійснення інформаційної діяльності за окремими напрямками: оприлюднення публічної інформації; надання консультування та прийняття заяв, звернень; забезпечення обігу оперативно-службової інформації; документування, робота з управлінськими, внутрішньоорганізаційними та індивідуальними документами; обробка електронної інформації; забезпечення захисту інформації.

Структурна побудова спеціальних суб'єктів ДПСУ інформаційних відносин відповідає вимогам безпеки державних кордонів та інформаційних прав усіх учасників прикордонних відносин. Суб'єкти інформаційних правовідносин реалізують свій інформаційний статус у межах інформаційних прав та обов'язків, закріплених законодавством, а ДПСУ ще і у зв'язку із виконанням завдань щодо забезпечення недоторканності державного кордону України у межах визначеної ділянки. Проведене дослідження дозволило сформувати тезу про те, що ДПСУ в контексті інформаційних правовідносин виступає як суб'єкт владних повноважень та є розпорядником інформації у сфері відповідальності.

Сьогодні питання інформаційної правосуб'єктності органів охорони державного кордону, як і загалом органів державної влади, чітко не визначені й несистематизовані. Відносно суб'єктів владних повноважень, у тому числі органів і підрозділів ДПСУ, їх інформаційна правосуб'єктність, передбачена у значній кількості нормативно-правових актів, що, як правило, закріплюють обов'язки щодо оприлюднення офіційної публічної інформації, надання відповідей за зверненнями (запитами) громадян, а також захисту інформації.

Об'єктом інформаційних відносин у діяльності ДПСУ є відомості, пов'язані з функціонуванням органів охорони державного кордону та порядком перетинання державного кордону. Різноманітність та обсяги даних у сфері охорони державного кордону дозволили згрупувати їх за окремими критеріями: за характером, за напрямком діяльності, порядком доступу, сутністю, результатами службової діяльності, очікуваним результатом, способом доведення, формою вираження; формою візуалізації, територіальним спрямуванням, за державно-правовим та суспільним схваленням.

За роки незалежності органи охорони державного кордону України стають усе більш відкритими до людини, це пов'язано з демократизацією суспільних і державно-правових відносин, прагненням Української держави стати повноправним членом у європейській спільноті. Для цього військовий орган – Прикордонні війська України у 2003 році було реформовано в Державну прикордонну службу України, але наскільки готова і спроможна система органів

охорони кордону і її посадові особи до сучасних інформаційних процесів буде розглянуто у наступних розділах і підрозділах дослідження.

1.5 Державна політика у сфері прикордонної інформаційної безпеки

Зважаючи на світову тенденцію становлення державності, лінії державних кордонів у історичному аспекті постійно змінювались, а основні завдання держави залишались сталими – забезпечення недоторканності та надійної охорони державних кордонів. Лише підходи до його охорони й основні правові засади функціонування державного рубежу постійно удосконалюються. За останні майже п’ятнадцять років правове забезпечення сфери охорони державного кордону якісно і кількісно змінилось, що обумовлено загрозами у цій сфері, зміною обстановки на державному кордоні, як на окремих ділянках, так і загалом.

Відсутність військової загрози в кін. XIX – поч. XX століття зумовили перехід Прикордонних військ України до Державної прикордонної служби України (2003 рік), що привело до суттєвих змін у підходах до охорони державного кордону, зокрема перехід до чотирирівневої (у перспективі обговорюється перехід до трирівневої станом на початок 2020 року) системи управління: Адміністрація ДПСУ – регіональне управління – орган охорони державного кордону – відділ прикордонної служби, спрощення порядку перетинання державного кордону тощо, усе це позначилося також на інформаційних відносинах у діяльності ДПСУ. На початку XX століття українська держава обрала курс у напрямку відкритості та прозорості державних кордонів за аналогами охорони європейських кордонів у зв’язку зі зменшенням військової загрози з боку сусідніх держав. Серед таких заходів можна відмітити і декриміналізацію статті 331 Кримінального кодексу України (далі – КК України) «Незаконне перетинання державного кордону» (2004 р.).

2014 рік змінив ситуацію: окупація АРК, збройний конфлікт на сході України змушують повернути військову складову в охороні державного кордону України та запровадити відповідальність за незаконне перетинання державного кордону України (ст. 332-2 КК України, 2018 р.) Установлення лінії розмежування, яка фактично стає новим умовним місцем проходження державного кордону на окремих ділянках, змушує переміщуватись громадян України територією нашої держави (з тимчасово неконтрольованої і в зворотному напрямку) по тимчасових перепустках і через контрольні пункти в'їзду-виїзду. З початком запровадження таких заходів не всі мали можливість отримати інформацію про особливості переміщення через лінію розмежування, що призводило до незручностей і значних проблем для громадян України.

Отже, сьогодні Україна опинилась в умовах «гібридної війни», у якій одним з основних засобів є інформаційне протистояння. В умовах інформаційного суспільства «вже не фізичний, а віртуальний простір став стратегічним полем бою, докорінно змінивши геополітичні та військово-політичні пріоритети» [146, с. 189]. Сучасні інформаційні технології дають змогу досягти реалізації власних інтересів без застосування воєнного інструментарію, послабити або навіть зруйнувати конкуруючу державу, не застосовуючи сили, за умови, якщо ця держава не усвідомить реальних і потенційних загроз негативних інформаційних впливів, і не створить дієвої системи захисту та протидії цим загрозам [147]. У зв'язку з цим у наукових працях усе частіше використовується термін «інформаційна війна» [146, с. 190]. Тому сьогодні реальною загрозою для нашої країни стало використання Російською Федерацією (далі – РФ) найновіших інформаційних технологій, які негативно впливають на свідомість громадян, розпалюють національну і релігійну ворожнечу, пропагують агресивну війну, зміни конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності України [148] та подання владою РФ міжнародній громадськості недостовірної інформації відносно подій в Україні. Але існують і інші загрози, зокрема у прикордонній сфері, які не пов'язані з діяльністю кремлівської влади, роль яких не можна зменшувати, такі як міжнародний

тероризм, нелегальна міграція та інші, які несуть загрозу національній безпеці держави та її інформаційним відносинам [149, с. 247].

Такі обставини вимагають від держави кардинальних кроків із протидії та ліквідації загроз територіальній цілісності, своєчасного інформування про зміни в умовах перетинання державного кордону тощо. Сукупність цих факторів визначають, що сфера охорони державного кордону знаходиться в залежності від політичних, економічних та інших обставин, подій як усередині країни, так і на території інших держав та свідчить про постійну мінливість і динамізм відносин у сфері охорони державного кордону і її інформаційної складової.

Держава є основним регулятором усіх відносин, які виникають, відбуваються та припиняються з її санкціонування, у тому числі і інформаційних. Основний вектор розвитку таких відносин задають компетентні владні органи – апарат держави, таким чином держава і тільки держава реалізує державну інформаційну політику. Події в Україні на початку 2014 року показали, що питання інформаційної безпеки є такими ж важливими, як і всі системоутоврюючі складові національної безпеки, а особливо під час ведення проти України інформаційної війни. Тому ці болючі й актуальні питання для нашої держави не оминули погляди науковців з існуючої проблематики – державної інформаційної політики держави, серед них: В. М. Желіховський, В. А. Ліпкан, Ю. Є. Максименко, В. О. Негодченко, Г. Г. Почепцов та ін. Сучасні проблеми інформаційної безпеки дослідили: О. О. Безвершенко, Б. А. Кормич, Ю. П. Лісовська, В. В. Остроухов, Г. Г. Почепцов, S. Braman, J. Fruhlinger та інші. Питання, присвячені загрозам, забезпеченню національної безпеки на державному кордоні, прикордонній політиці та прикордонній безпеці, вивчали такі науковці, як В. П. Бірюков, В. Л. Зьолка, Д. А. Купрієнко, А. П. Курашкевич, С. О. Каштелян, М. М. Литвин, В. О. Назаренко, В. С. Нікіфоренко, М. В. Плахотний, В. М. Серватюк, О. Є. Цевельов та інші. Проте сьогодні залишається недослідженою державна політика у сфері інформаційної прикордонної безпеки, що зумовлює актуальність та об’єктивну необхідність її розробки.

Інформаційна політика держави

З’ясовувати сутність та зміст державної інформаційної політики у прикордонній сфері будемо за допомогою філософського методу пізнання – індукції. Отже, розпочнемо з осмислення терміна «політика». Словник української мови надає такі визначення терміна «політика»: цілі й завдання, що їх ставлять суспільні класи в боротьбі за свої інтереси; методи і засоби досягнення цих цілей і завдань; загальний напрямок, характер діяльності держави, певного класу або політичної партії; напрямок діяльності держави або політичної партії у тій чи іншій галузі у певний період; події і питання внутрішньодержавного і міжнародного суспільного життя [150].

Філософський словник тлумачить політику як термін, який походить з грецької мови і дослівно перекладається як державна діяльність. У загальному значенні – це діяльність, що має своєю метою регулювання взаємин між людьми для забезпечення певного стану деякої суспільної одиниці (суспільного утворення). Підтримання певного ладу чи порядку (заради загальної безпеки) належить до найперших і найважливіших цілей політики. У нормативному розумінні політика розглядається як вид діяльності, що має мету забезпечення найважливіших передумов добробуту суспільного утворення шляхом узгодження інтересів та ціннісних орієнтацій осіб і суспільних груп [37, с. 494]. При цьому держава є одним із типів політичних установ, а серед підстав появи політичної системи є намагання людей відвернути хаос і збільшити міру своєї безпеки, тобто спільні інтереси [37, с. 494]. Тому визначальною метою політики є підтримання загальної безпеки для ефективного забезпечення і підтримання суспільних відносин.

Автори підручника «Політологія: наука про політику», розкриваючи зміст політики, указують на існування різноманітних її визначень: простих і осмислених, в яких виділяються різні аспекти політики, що свідчать про багатство змісту поняття політики і його інтегрований характер [151, с. 11]. При цьому зазначають, що політика не створює особливу сферу суспільного життя, але й не заперечує наявності власної державно-владної сфери, інтегрує різні сторони явищ,

але й не зводиться до жодного з них [151, с. 12]. Але все ж таки державна політика забезпечує впровадження окремих самостійних напрямків регулювання державно-правового та суспільного життя.

Окремим напрямком державної політики є державна прикордонна політика, розроблення, формування та закріплення якої здійснюється у структурах державного апарату та виконується прикордонниками [152, с. 320]. Основою сучасної системи прикордонної безпеки держави, наголошує М. Пахотний є інформаційна сфера, яка є засадою для вивчення масштабів, характеру, спрямованості реальних і потенційних загроз на державному кордоні, протидія яким покладена на ДПСУ [153, с. 105].

Доктриною інформаційної безпеки сформульовані пріоритети державної політики в інформаційній сфері, зокрема актуальними для прикордонної сфери є: створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них [148, п. 5]. Розвиток системи аналізу ризиків у ДПСУ було розпочато ще в 2006 році [13], сьогодні продовжується удосконалення; удосконалення повноважень ДПСУ з метою досягнення адекватного рівня спроможності відповідати реальним і потенційним загрозам національним інтересам України у прикордонній інформаційній сфері; законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави інформації, яка пропагує війну або порушення територіальної цілісності України, загрожує державному суверенітету; розвиток і захист технологічної інфраструктури забезпечення прикордонної інформаційної безпеки України; забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах, а також тимчасово окупованих територій; посилення протидії спеціальним інформаційним операціям, спрямованим на порушення суверенітету і територіальної цілісності, підрив обороноздатності України, деморалізацію особового складу ДПСУ, загострення суспільно-політичної ситуації, зокрема у прикордонних районах; унеможливлення вільного обігу інформаційної продукції (друкованої та електронної), насамперед походженням з території держави-агресора, що містить пропаганду війни,

національної і релігійної ворожнечі, зміни конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України, провокує масові заворушення. Контроль за ввезенням в Україну такої друкованої продукції (можливості перевіряти електронні носії немає) здійснюється у пунктах пропуску через державний кордон [154] або в контрольних пунктах в'їзду на тимчасово окуповану територію та виїзду з неї відповідними підрозділами ДПСУ [155]; проведення розвідувальними органами України акцій сприяння реалізації та захисту національних інтересів України в інформаційній сфері, протидії зовнішнім загрозам інформаційній безпеці держави за межами України [148, п. 5]. У ДПСУ здійснюється оперативно-розшукову діяльність (далі – ОРД)в інтересах безпеки державного кордону самостійно та у взаємодії з Службою безпеки України (далі – СБ України). Забезпечує реалізацію державної політики у сфері захисту державного кордону, управління, організацію та контроль ОРД Департамент оперативно-розшукової діяльності Адміністрації ДПСУ [156]. Розвідувальні органи України у процесі здійснення розвідувальної діяльності мають сприяти реалізації та захисту національних інтересів України в інформаційній сфері за кордоном, протидіяти зовнішнім загрозам інформаційній безпеці держави [148, п. 6], контррозвідувальне забезпечення в частині поширення негативної інформації про ДПСУ.

Загалом прикордонна політика – це сукупність заходів (механізмів), спрямованих на забезпечення суверенітету, недоторканності й цілісності території, реалізацію та захист національних інтересів і безпеки держави у її прикордонній сфері [157, с. 17], а невід'ємним елементом прикордонної політики є її інформаційна складова. Прикордонна та інформаційна безпека є окремими самостійними компонентами державної політики, але разом з тим зв'язок, що їх пов'язує та об'єднує, дозволяє говорити про них як про взаємопов'язані явища, які співвідносяться як ціле та частина відповідно. Адже у сфері відповідальності ДПСУ (охорона державних кордонів) інформаційна є однією із складових прикордонної безпеки та безпеки державних кордонів.

Прикордонна безпека

Із початком функціонування ДПСУ як правоохоронної структури держави у науковий обіг та в практичну діяльність ДПСУ було введено багато термінів, понять і категорій (прикордонна сфера, прикордонний простір, прикордоннологія тощо), які до сьогодні не знайшли законодавчого закріплення. У межах нашої наукової розробки необхідно зупинитись на з'ясуванні значення та співвідношення таких самостійних правових категорій, як «безпека державного кордону» та «прикордонна безпека», на підставі аналізу нормативно-правових актів, наукових досліджень та лексичного розбору кожного слова.

Отже, для юриспруденції важливе законодавче формулювання дефініції, але аналіз законодавства дозволив констатувати відсутність такої щодо понять «прикордонна безпека» та «безпека державного кордону», хоча самі терміни неодноразово використовуються у нормативно-правових актах України. Так, зокрема Закон України «Про національну безпеку України» визначає, що ДПСУ 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 [158, п. 6 ст. 18]. Варто зазначити, що ця норма не є ідентичною, визначеним у Законі України «Про Державну прикордонну службу України» завданням, які покладаються на Державну прикордонну службу України: «забезпечення недоторканності державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні» [79, ст. 2]. При тому, що завдання із реалізації державної політики у сфері охорони державного кордону, здійснення управління у сфері охорони державного кордону втілює Адміністрація ДПСУ [159, п. 3]. З урахуванням цього, варто зазначити про існування широкого та вузького розуміння реалізації державної політики. У першому випадку державна політика реалізується через державний механізм управління, до складу якого входять механізми державного управління. У другому – реалізація державної політики здійснюється за допомогою комплексного механізму державного управління, який містить набір окремих механізмів, що дозволяє реалізувати конкретний

напрямок державної політики відповідно до сфер суспільної діяльності [160, с. 421]. Але все ж таки необхідно уточнити, що відповідальним органом за реалізацію державної політики у сфері безпеки державного кордону України має бути Адміністрація ДПСУ. Хоча реально у системі управління ДПСУ сьогодні відслідковується певний колапс. Указом Президента України від 24 грудня 2012 р. № 726/2012 «Про деякі заходи з оптимізації системи центральних органів виконавчої влади» [161] було внесено зміни до Указу Президента України «Про оптимізацію системи центральних органів виконавчої влади» від 09 грудня 2010 р. № 1085/2010 [162], чим було перекладено функцію управління та координування діяльності Адміністрації ДПСУ з КМУ на МВС України. Як цілком достатньо обґрунтовано доводить І. Ф. Корж, згаданий акт порушує «ряд конституційних положень в частині делегування здійснення відповідних функцій державно-адміністративного управління сектором безпеки і оборони іншому органу» [163]. Тому сьогодні, на наш погляд, є дискусійним питання щодо того, хто відповідальний за реалізацію державної політики у сфері безпеки державного кордону України та потребує уточнення, як і сам правовий статус ДПСУ, про що зазначив І. Ф. Корж у своєму дослідженні [163].

У Законі України «Про основи національної безпеки України», що втратив чинність 8 липня 2018 року, у зв’язку із прийняттям Закону України «Про національну безпеку України» використовувалась термінологічна конструкція «сфера безпеки державного кордону України» [164, ст. 7]. Зважаючи на те, що новий Закон України «Про національну безпеку України» було прийняти нещодавно, у переважній більшості наукових досліджень, присвячених прикордонній проблематиці, розглянуто безпеку державного кордону з позицій, закріплених у Законі України «Про основи національної безпеки України» (втратив чинність) у контексті її як складової національної безпеки [30, с. 121; 165, с. 12; 166, с. 55]. Це розкриває «безпеку державного кордону» з позиції широкого її розуміння. З цього приводу В. Л. Зьолка зауважує, що це не дає змоги повністю охопити весь спектр правовідносин, пов’язаних із забезпеченням національної безпеки у відповідній сфері. Адже коли сприймати дану категорію у

вузькому сенсі, то необхідно тісно прив’язуватись до поняття «державний кордон» [30, с. 127].

У законах України «Про державний кордон України» (1991 р.) та «Про Державну прикордонну службу України» (2003 р.) словосполучення «безпека державного кордону» взагалі не зустрічається, це можна пояснити стрімким розвитком прикордонних відносин, уведенням нових термінів у цій сфері в обіг, але не включення їх у понятійний апарат фундаментальних законів, що є основою правового регулювання у забезпеченні непорушності державних кордонів. «Сфера безпеки державного кордону» згадується у Законі України «Про прикордонний контроль» [154, п. 11], який був прийнятий значно пізніше від законів згаданих вище, але без додаткових роз’яснень.

Більш гнучкими до реагування на зміни, що відбуваються у відносинах, пов’язаних із державним кордоном, є підзаконні нормативно-правові акти. Так, зокрема, метою Стратегії розвитку Державної прикордонної служби України, яка затверджена розпорядженням КМУ, є забезпечення ефективної реалізації політики у сфері безпеки державного кордону, а також охорони суверенних прав України в її виключній (морській) економічній зоні [59]. Кабінетом Міністрів України також була затверджена Концепція інтегрованого управління кордонами, метою якої було підвищення ефективності реалізації державної політики у сфері безпеки державного кордону, запровадження європейських стандартів інтегрованого управління кордонами [167]. 24 липня 2019 р. була прийнята Стратегія інтегрованого управління кордонами на період до 2025 року, яка визначила основні напрями системного формування державної політики розвитку й ефективного управління державним кордоном на період до 2025 року. Стратегія інтегрованого управління кордонами (далі – Стратегія ІУК) спрямована на запровадження ефективних інструментів співпраці та координації на внутрішньовідомчому, міжвідомчому, міжнародному рівнях, а також з приватним сектором. Визначено, що проблеми управління кордонами не можуть бути розв’язані тільки шляхом проведення дій на кордоні. Стратегія ІУК передбачає скоординований розвиток та реалізацію функцій суб’єктів інтегрованого

управління кордонами, що разом діють і на державному кордоні, і всередині держави, оптимально використовуючи національні ресурси [59].

Ключовою у цих програмних документах є мета – ефективна реалізація політики у сфері безпеки державного кордону. Мета – це те, чого прагнуть досягти через певний час, змінити сучасний стан відносин чи обставин. Отже, узагальнена діяльність ДПСУ протягом тривалого періоду часу цілеспрямована на досягнення максимально високого рівня безпеки державного кордону України відносно існуючого [168, с. 77]. Отже, чинне законодавство не дає повного вичерпного розуміння поняття «безпека державного кордону», тому розглянемо погляди науковців з цього питання.

Дослідивши загрози національній безпеці у сфері безпеки державного кордону, О. Є. Цевельов зазначив, що безпека державного кордону спрямована на ефективну реалізацію політики безпеки у сфері захисту та охорони державного кордону України, а також охорони суверенних прав України у її виключній (морській) економічній зоні [169, с. 36]. Тобто безпека державного кордону у цьому розумінні ототожнюється з реалізацією політичних рішень, які виражені у законах, стратегіях тощо із забезпеченням непорушності та цілісності державного кордону та пов’язаних із цим правових відносин.

Діяльність із забезпечення «безпеки державного кордону» І. Ф. Корж розглядає як невід’ємну складову захисту територіальної цілісності держави зокрема і безпеки держави загалом [170, с. 223]. Проаналізувавши праці українських учених з питань національної безпеки [171, с. 81–82; 172, с. 163; 173, с. 364–367], В. Л. Зьолка зробив висновок, що «безпека державного кордону» розглядається як складова або різновид воєнної безпеки, а застосування законодавцем категорії «безпека державного кордону» здійснюється у прив’язці до «воєнної сфери» [30, с. 126].

Проаналізоване дає можливість визначити, що безпека державного кордону уособлюється з безпекою держави та територіальною цілісністю. **Безпека державного кордону** – це цілеспрямована повсякденна та безперервна діяльність органів і підрозділів ДПСУ з моніторингу за лінією державного кордону України,

виявлення та недопущення небезпек її зміни, забезпечення непорушності та цілісності. Крім виразу «безпека державного кордону», у наукових працях використовують споріднене поняття – «прикордонна безпека».

У розумінні Б. М. Марченко [174, с. 6] та М. М. Литвина [165, с. 12], прикордонна безпека це не тільки прив'язка до безпеки державного кордону як фізичної лінії, що розмежовує суміжні держави, та територіальна безпека й цілісність держави, але й це ще й відповідні законні інтереси різних суб'єктів, пов'язані із проходженням державного кордону.

У сфері прикордонної безпеки, зазначають Д. А. Купрієнко та С. Я. Білявець, перетинаються не тільки загрози, але й інтереси багатьох суб'єктів, які зумовлені об'єктивною потребою людства в соціальній, економічній, політичній, інформаційній та інших видах взаємодії. Прикордонну безпеку забезпечують глобальна, регіональна та національна системи прикордонної безпеки [175, с. 162]. У зв'язку із цим формулюють, що прикордонна безпека – це складова національної і міжнародної безпеки, яка характеризує прийнятний рівень захищеності життєво важливих інтересів соціальних суб'єктів у прикордонному просторі, при якому здійснюються оперативне виявлення та припинення правопорушень, протидія зовнішнім і внутрішнім загрозам, планомірна діяльність щодо усунення причин їх виникнення, а також створюються умови для сталого розвитку прикордонних територій, здійснення законної транснаціональної і транскордонної діяльності, подорожування осіб, дотримання прав і свобод осіб, які шукають притулку та/або захисту» [175, с. 163].

Прикордонну безпеку Ю. Б. Курилюк пропонує розуміти, «як збалансований стан захищеності суспільних відносин у прикордонній сфері від зовнішніх та внутрішніх загроз охоронюваним законодавством про державний кордон інтересам людини, суспільства й держави» [176, с. 50]. Цілком підтримуємо позицію науковця, щодо інтегративного характеру прикордонної безпеки.

Подібні думки відслідковуються у О. Г. Мельникова [177, с.47] О. В. Ананьїна, які розглядають прикордонну безпека як складову національної безпеки, яка досягається через політичні, організаційно-правові, економічні, військові, розвідувальні, оперативно-технічні, екологічні, санітарні, гарантійні та інші заходи, що здійснюються шляхом реалізації державної політики у сфері прикордонної безпеки [178]. М. М. Литвин та В. С. Нікіфоренко зазначають, що прикордонна безпека України забезпечується здійсненням комплексу правових, організаційних, режимних, контррозвідувальних, розвідувальних, оперативно-розшукових, спеціальних і військових заходів, спрямованих на захист об'єктів прикордонної безпеки, у тому числі, державного суверенітету, територіальної цілісності, економічного потенціалу тощо [165, с. 17; 179]. Отже, проаналізовані вище погляди з приводу розуміння прикордонної безпеки, зводяться до такого: це є складова національної безпеки, забезпечується комплексом різноманітних заходів; захищеність інтересів особи, суспільства та держави у прикордонній сфері.

Розглянуті наукові позиції щодо понять «безпека державного кордону» і «прикордонна безпека», на наш погляд, не дають чіткого уявлення про їх характерні відмінності. Отже, ключовим словом, яке однозначно поєднує їх, є термін «безпека». Словник української мови безпеку роз'яснює як стан, коли кому-, чому-небудь ніщо не загрожує [180]. У Словнику політологічних термінів, безпе-ка – це стан, при якому небезпека у будь-якому вигляді не загрожує будь-кому, будь-чому [181]. Відносно безпеки державного кордону неможливо досягти стану коли «ніщо не загрожує», лише можна враховувати в оперативно-службовій діяльності ДПСУ актуальні загрози і планувати та діяти у напрямку їх своєчасного виявлення, попередження та нейтралізації. Тому «безпека» щодо державного кордону, – це своєчасне реагування на випередження, недопущення та усунення загроз.

Відносно поняття «державний кордон», його офіційне тлумачення міститься у Законі України «Про державний кордон України», а саме – це є лінія і

вертикальна поверхня, що проходить по цій лінії, які визначають межі території України – суші, вод, надр, повітряного простору [182, ст. 1].

Роз'яснення терміна «прикордонний» зустрічається у спільнокореневому «прикордоння» як розмовне слово – територія, розташована біля кордону, вздовж кордону [183]. Крім цього, використовується у словосполученнях: прикордонний регіон [184; 185], прикордонний режим, прикордонна смуга, контрольований прикордонний район [186], прикордонна територія [187], прикордонний простір [188, с. 51–52; 189, с. 56]. Загалом, «прикордонний» необхідно розглядати як пов'язаний із державним кордоном, а саме: наближений до державного кордону, розташований недалеко, уздовж лінії державного кордону. Крім цього, варто використовувати «прикордонний» як пов'язаний із державним кордоном не тільки відносно території, але й у будь-якому іншому значенні, наприклад прикордонний інтерес, право чи запит на інформацію у прикордонній сфері, інформація у прикордонній сфері.

Прикордонну безпеку необхідно розуміти як сформований у нормативно-правових актах та забезпечений діяльністю ДПСУ стан безпеки державного кордону та усіх її складових (у тому числі інформаційної), забезпечення реалізації прав і законних інтересів суб'єктів у прикордонній сфері.

Отже, якщо сприймати буквально або обмежено, то «безпека державного кордону» є незмінність лінії державного кордону та надійне збереження територіальної цілісності держави, а «прикордонна безпека» охоплює ширші безпекові заходи не тільки на державному кордоні, але і вздовж нього, спрямовані на недопущення та усунення загроз, наслідком чого є безпека державного кордону та реалізація прав усіх суб'єктів, пов'язаних із проходженням державного кордону [168, с. 79].

Діяльність щодо охорони державного кордону (лінії державного кордону) не здійснюється тільки на державному кордоні, це складні відносини з організації управління, планування та здійснення оперативно-службової діяльності, службово-бойової діяльності, підготовки особового складу, кадрового забезпечення, ресурсного та інших видів забезпечення, які комплексно проходять

не тільки у прикордонних регіонах, але і у всіх структурних підрозділах і навчальних закладах ДПСУ відповідно до державної політики у цій сфері. Безпека державного кордону залежить від існуючих загроз та можливостей компетентних органів та підрозділів ДПСУ своєчасно їх виявляти, усувати та не допускати.

Тому вважаємо, що такі поняття як «безпека державного кордону» та «прикордонна безпека» співвідносяться як частина та ціле відповідно. «Прикордонна безпека» стале поняття, а її стан – динамічне, який залежить від діяльності перш за все прикордонного відомства щодо створення системних заходів забезпечення безпеки державного кордону, невід'ємною частиною яких є інформаційна безпека, що реалізується у межах інформаційної політики держави.

Уведення поняття «інформаційна політика» С. Бремен пов'язує з початком пропаганди з боку держави під час Першої світової війни, яке уособлювало технологічне забезпечення впливу на великі маси населення [190]. С. Бремен зазначає, що інформаційна політика складається із законів, регулювання та доктрин, прийняття рішень і практик на рівні суспільних базових принципів, включаючи створення інформації, її обробку, передачу, доступ до неї та використання [190]. Отже, держава повинна забезпечити чіткі правові межі інформаційних відносин з одночасним створенням відповідної інформації, забезпеченням її обігу та захисту.

В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський під інформаційною політикою держави розуміють діяльність держави в інформаційній сфері, спрямованої на задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору цілісної держави та його інтеграції у світовий інформаційний простір з урахуванням національних особливостей і інтересів при забезпеченні інформаційної безпеки на внутрішньодержавному та міжнародному рівнях [191]. Саме системне врахування інформаційних потреб людини, суспільства й держави має бути ключовим у формуванні інформаційної політики держави у прикордонній сфері.

Військовослужбовці ДПСУ, серед яких проводилось опитування, 53,7 % розуміють інформаційну політику держави як вироблення, реалізацію та контроль за реалізацією й удосконаленням державної стратегії і тактики в інформаційній сфері, 22,1 % як забезпечення доступу до інформації, її охорона й захист, 7,8 % – збереження державної таємниці, 6,1 % – забезпечення функціонування інформації в суспільстві, 5,6 % – політику інформаційної безпеки, 3 % – регулювання інформаційних процесів, 1,7 % – інформаційна ідеологія держави **(додаток В)**. На наш погляд, інформаційна політика держави передбачає розроблення стратегічного планування інформаційної безпеки та реалізацію інформаційних прав усіх суб'єктів інформаційних відносин.

Г. Г. Почепцов, аналізуючи сучасні підходи до інформаційної політики, переважно акцентує свою увагу на сфері інформаційних воєн і захисту від них та виділяє дві проблемні сфери: технічну і політичну. При цьому зауважує, що поганим прикладом є те, коли закономірності однієї сфери беруться як зразок для всієї подібної проблематики [192]. Основною метою політики інформаційної безпеки держави є управління реальними та потенційними загрозами й небезпеками з метою створення необхідних умов для задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів [191]. Сучасні інформаційні відносини у прикордонній сфері будуються на урахуванні аналізу та профілюванні ризиків у сфері охорони державного кордону та захисті суверенних прав України в її виключній (морській) економічній зоні [193].

Спеціалісти з комп'ютерних систем і мереж як представники технічної сфери налаштовані на встановлення все сильніших способів захисту, у той же час для представників політичних (соціальних) наук це виглядає досить дивно. З їхньої точки зору, проблема не так у захисті, як у побудові власних текстів, які б могли вистояти під атакою чужих. Доля Радянського Союзу чітко демонструє, що при знятті цього штучного захисту відбувається повна руйнація ціннісного компонента країни. Інформаційна політика є невід'ємною частиною урядування і поки ми бачимо лише підсилення інформаційної складової, що привертає все

більшої уваги до інформаційної політики в сучасних державах [192]. Інформаційна політика стає у центрі уваги суспільства, оскільки на наших очах принципово змінюється роль інформації. У найширшому розумінні інформаційна політика – це функціонування інформації в суспільстві [192]. Лаконічне визначення державної інформаційної політики бере за основу у своєму дослідженні Ю. М. Іванченко як сукупності основних напрямів і способів діяльності держави з отримання, використання, поширення та зберігання інформації [194].

Кожен центральний орган виконавчої влади силового та правоохоронного спрямування щодо «інформаційного» блоку вже має свої повноваження у сфері інформаційної безпеки, але навіть у такому випадку необхідність координації спільної діяльності й отримання зворотного зв'язку є очевидною. На думку Т. Попової, – експерта зі стратегічних комунікацій громадської організації «Інформаційна безпека», колишнього заступника міністра інформаційної політики України: нам слід піднятися над нашим внутрішнім «перетягуванням ковдри» між державними структурами та спробувати прогнозувати дії противника. У випадку реалізації керівництвом Росії плану масованого інформаційного впливу проти України в поєднанні з іншими заходами «гібридної війни» буде задіяно весь арсенал інформаційного протиборства. Об'єктами атак стануть усі можливі цільові аудиторії в Україні, система державного та військового управління, інформаційна інфраструктура тощо. За найбільш песимістичними сценаріями ми можемо втратити суверенітет у національному інформаційному просторі. З метою недопущення зазначеного з української сторони має бути забезпечена здатність системи державного управління зберегти можливості свого функціонування та впливу на ситуацію в інформаційній сфері [195]. Отже, не можна зупинятись на досягнутому, а необхідно безперервно бути готовими до інформаційних атак, тому в першу чергу необхідно постійно підтримувати на високому рівні забезпечити захист інформаційного простору у сфері охорони та захисту державного кордону України.

Ю. П. Лісовська, досліджуючи основні положення державної політики щодо забезпечення інформаційної безпеки, робить висновок, що впровадження вдалої інформаційної політики може істотно впливати на зниження соціальної напруги та розв'язання внутрішньополітичних і воєнних конфліктів [196, с. 61]. J. Fruhlinger інформаційну безпеку пропонує розглядати з урахуванням подвійності станів: статичному – як захищеність особистості, суспільства та держави від деструктивних та інших негативних впливів в інформаційному просторі; динамічному – як сукупність практичних дій, спрямованих на захист даних від несанкціонованого доступу чи змін як при їх зберіганні, так і при передачі [197]. З приводу цього серед опитаних респондентів (58,9 %) переважає думка, хоча із невеликою відмінністю про те, що інформаційна безпека відображає динамічний стан, а 41,1 % розглядають її у статичному стані **(додаток В).**

Державна інформаційна політика повинна будуватись з урахуванням переваг у конкретний період розвитку. Так, О. В. Соснін визначив головні пріоритети України в інформаційній сфері: захист внутрішньо- та зовнішньо політичних інтересів держави; реформування засобів масової комунікації згідно з демократи-ними принципами Ради Європи; формування інформаційних ресурсів єдиного українського інформаційного простору і концепції інформаційної безпеки; контроль за дотриманням принципів інформаційної політики та національного законодавства; розвиток інформаційної культури і духовного середовища [26, с. 12].

Основними напрямами державної політики в інформаційній сфері в 2005 році науковець визначив: забезпечення інформаційного суверенітету України; удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, упровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до боротьби з корупцією; забезпечення неухильного

дотримання конституційного права громадян на свободу слова, доступ до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність ЗМІ; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії його монополізації [26, с. 14]. Варто підкреслити, що більше десяти років такі напрямки залишаються актуальними, лише варто додати нові, наприклад недопущення інформаційного протистояння інтересам та безпеці України з боку РФ, поширенням пропаганди міжнародного тероризму, нелегальної міграції тощо.

Ґрунтуючись на основних напрямках державної інформаційної політики, закріплених у Законі України «Про інформацію», можна визначити ті, які актуальні для прикордонної сфери [57, ст. 3]: забезпечення доступу кожного до інформації про порядок і правила перетинання державного кордону, про діяльність прикордонного відомства тощо; створення умов для формування в Україні інформаційного суспільства в частині отримання публічної інформації, розпорядником якої є ДПСУ; забезпечення відкритості та прозорості діяльності органів ДПСУ через систематичне й оперативне оприлюднення інформації про особливості перетинання державного кордону, результатів службової діяльності, задоволення запитів (звернень) громадян та ін.; створення інформаційних систем і мереж інформації, розвиток електронного урядування (офіційний веб-сайт в мережі Інтернет – https://dpsu.gov.ua/, функціонування Контактного центру ДПСУ (служба «Довіра»); здійснення заходів з реалізації державної політики у сферах телекомунікації, інформатизації та захисту інформації в ДПСУ [109]; постійне оновлення, збагачення та зберігання інформаційних ресурсів відомства; забезпечення функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем (мереж) ДПСУ, у тому числі міжвідомчих, баз (банків) даних та інших електронних інформаційних ресурсів за компетенцією [109].

Інформаційна безпека

Отже, одним із напрямків державної інформаційної політики держави є забезпечення інформаційної безпеки [57, ч. 1 ст. 3]. Концепція Національної

програми інформатизації визначає, що інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки [197]. У Законі України «Про національну безпеку України» інформаційна безпека згадується в контексті необхідності її забезпечення [158, ч. 4 ст. 3]. У Доктрині інформаційної безпеки України сформульовано національні інтереси України в інформаційній сфері; актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері; напрями і пріоритети державної політики в інформаційній сфері, але зміст терміна «інформаційна безпека» не знайшов належного розкриття [148]. Загалом у згаданих нормативно-правових актах категорія «інформаційна безпека» пов'язується із захистом інформації та захищеністю її від загроз.

У проекті Концепції інформаційної безпеки України, яка розроблена Міністерством інформаційної політики України, запропоновано закріпити поняття інформаційної безпеки як стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій [199]. На жаль, через недоліки нормотворчих процесів в Україні поки дане поняття ми можемо використовувати лише в науковому обігу.

Ще одне нормативне поняття «інформаційна безпека» міститься в Основних засадах розвитку інформаційного суспільства в Україні на 2007–2015 роки. Але термін, на який був розрахований даний закон, вже сплинув, а отже і нормативний акт втратив чинність. Поняття інформаційної безпеки було визначене в Основних засадах як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності,

конфіденційності та доступності інформації [200]. Дане тлумачення переважно збігається з поняттям, закріпленим в Проекті Концепції інформаційної безпеки України.

Інформаційну безпеку суспільства А. Суббот пропонує розглядати у двох напрямах, а саме: вплив інформації на аудиторію через засоби масової інформації (телебачення, Інтернет, пресу тощо); захист і збереження особистої, корпоративної та державної інформації [201, с. 29]. О. О. Безвершенко зазначає, що в повсякденному житті інформаційна безпека реалізується у напрямку боротьби з витоком закритої (таємної) інформації, а також з розповсюдженням хибної та ворожої інформацій. Осмислення нових інформаційних безпек у суспільстві ще тільки починається. Тому необхідно здійснити перехід від принципу забезпечення безпеки інформації до принципу інформаційної безпеки з урахуванням майбутнього розвитку інформатизації, проникнення інформаційних технологій у найважливіші сфери життя суспільства [147].

Одним з основних напрямів забезпечення ефективної охорони державного кордону є своєчасне отримання (добування, обробка, формування) інформації необхідної якості про стан і перспективи розвитку ризиків і загроз національній безпеці держави у прикордонній сфері, а також про можливості відповідних служб і органів щодо зниження, попередження та ліквідації цих ризиків і загроз [202, с. 79]. Дії по роботі з інформацією та її джерелами в ДПСУ повинні наперед, готуватись та управлятись в реальному масштабі часу з метою захисту національних інтересів [202, с. 80].

Різноманітними є погляди науковців щодо інформаційної безпеки:

захищеність державних інтересів, за якої забезпечується запобігання, виявлення і нейтралізація внутрішніх та зовнішніх інформаційних загроз, збереження інформаційного суверенітету держави і безпечний розвиток міжнародного інформаційного співробітництва [203, с. 116];

інформація є чинником, який може призвести до технологічних аварій, військових і політичних конфліктів, дезорганізації державного управління, фінансової системи [204, с. 157];

інформаційна безпека забезпечується з метою створення нормальних умов функціонування конкретного органу державного управління, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки [191];

інформаційна безпека – стан, вільний від таких загроз, як: надання інформації стороннім особам; шпигунство; саботаж та диверсійні заходи. Інформаційна безпека являє собою також будь-яку дію, систему або метод, які спрямовані на захист інформаційних ресурсів, збір, обробку, а також передаються, зберігаються у пам'яті комп'ютерів і телекомунікаційних мереж; складається не тільки із захисту від несанкціонованого доступу, крадіжки даних або їх знищення, але і як компонент фізичної, особисто організаційної та IT-безпеки [205, с. 292];

у механізмі безпекотворення в інформаційній сфері повинні бути враховані національні інтереси в інформаційному середовищі, внутрішні та зовнішні небезпеки, ризики, виклики та загрози цим інтересам і передбачена система засобів із їх виявлення, попередження, нейтралізації і припинення. Забезпечення інформаційної безпеки передбачає захист таких елементів: інформації з обмеженим доступом; систем і засобів передавання та зберігання інформації; інформаційного простору від поширення інформації, зміст якої через неповноту, недостовірність тощо суперечить національним інтересам держави [206, с. 319];

інформаційна безпека – це одна зі сторін розгляду інформаційних відносин у межах інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства, держави й акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [207];

стан захищеності об'єкта (особистості, суспільства, держави, інформаційно-технічної інфраструктури), при якому досягається його нормальне функціонування незалежно від внутрішніх і зовнішніх інформаційних впливів [208, с. 136];

стан захищеності держави, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття

інформації (за допомогою спеціальних технічних засобів) та комп'ютерні злочини не завдають суттєвої шкоди національним інтересам [208, с. 137].

Тобто інформаційна безпека у загальному контексті діяльності механізму держави розкривається як своєрідний бар'єр для деструктивного впливу на інформаційне середовище.

Інформаційна безпека в податкових органах, визначає Т. В. Субіна, – це «система унормованих методів, заходів, засобів, способів дотримання належного рівня охорони і захисту інформації, недопущення негативного інформаційного впливу на діяльність податкової служби з метою реалізації конституційних прав, свобод і законних інтересів людини, громадянина, підприємств, установ, закладів усіх форм власності у сфері оподаткування» [209, с. 12]. Такий підхід до розуміння інформаційної безпеки враховує не тільки загрози інформаційним правам, системам, але і необхідність захисту інформації, яка є об'єктом інформаційних відносин. На відміну від розглянутих вище наукових розумінь інформаційної безпеки, у яких вона пов'язувалась із суб'єктним складом інформаційно-правових відносин (захист інтересів та інформаційних прав суб'єктів цих відносин), то позиція Т. В. Субіної, крім того, ураховує і об'єктний склад – інформацію та необхідність її захисту. Вважаємо, що не можна розглядати інформаційну безпеку поза межами захисту інформації, адже інформація є основним об'єктом з приводу чого і виникають та відбуваються інформаційні правовідносини.

Захищеність усієї інформаційної системи пов'язана не тільки з її збереженням від зовнішніх або внутрішніх впливів, але збереженням усіх елементів інформаційної системи в первинному значенні параметрів, яке дозволяє забезпечити цілісність, рівновагу їхнього існування і стійкість у розвитку. Інформаційна безпека виявляється у такому стані інформаційного суспільства, при якому створюється неможливість нанесення шкоди існуванню, функціонуванню і властивостям об'єктів інформаційної діяльності, а також інтересам її суб'єктів [210].

Структурно «інформаційну безпеку» Т. Ю. Ткачук, пропонує розглядати у поєднанні елементів безпеки інформації, безпека «від інформації» (суб'єктів,

інформаційних систем) та дотримання порядку реалізації прав та інтересів інформаційної сфери [211, с. 102].

Дослідивши адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади, О. В. Логінов у своєму дисертаційному дослідженні робить висновок, що «інформаційну безпеку не може розглядатися лише як окремий стан, вона має враховувати майбутнє, отже є не станом, а процесом. Таким чином, інформаційну безпеку слід розглядати крізь органічну єдність ознак, таких як стан, властивість, а також управління загрозами і небезпеками, за допомогою якого забезпечується обрання оптимального шляху їх усунення і мінімізації впливу негативних наслідків. Одним із механізмів гарантування даного процесу є ефективно функціонуюча система органів виконавчої влади, які є суб'єктом і об'єктом забезпечення інформаційної безпеки одночасно». Інформаційна безпека є характеристикою стабільного, стійкого стану органів виконавчої влади, яка при впливі внутрішніх і зовнішніх загроз та небезпек зберігає суттєво важливі характеристики для власного існування [212, с. 10].

Інформаційна безпека забезпечується проведенням єдиної державної політики національної безпеки в інформаційній сфері, системою заходів економічного, політичного й організаційного характеру, адекватних загрозам і небезпекам національним інтересам особи, суспільства та держави в інформаційній сфері. Окремий орган держави для забезпечення інформаційної безпеки здійснює власну діяльність на базі використання інформаційної інфраструктури суспільства, виробляє і споживає інформаційні ресурси, має певні відносини із громадянами і як власник інформаційних ресурсів і тих, що складають інформаційну інфраструктуру, має вживати певних заходів із забезпечення збереження ресурсів і безпеки функціонування інформаційних і телекомунікаційних систем, мереж зв'язку, систем управління [212, с. 12].

На запитання «Які заходи передбачає інформаційна безпека у діяльності ДПСУ?» 54,2 % респондентів відповіли – «захист і збереження інформації у сфері діяльності ДПСУ», 19,9 % – «боротьба з витоком закритої (таємної) інформації, а

також з розповсюдженням хибної та ворожої інформацій», 12,1 % – «захист інформації та захищеність її від загроз», 6,9 % – «своєчасне реагування на інформаційні загрози у прикордонній сфері», 5,2 % – «створення нормальних умов функціонування ДПСУ» й лише 1,7 % – «недопущення негативного інформаційного впливу на військовослужбовців ДПСУ», що свідчить про зведення інформаційної безпеки у практичній повсякденній діяльності до дій із захисту, збереження службової та таємної інформації. При цьому опитані надали свою оцінку рівню заходів із забезпечення інформаційної безпеки у ДПСУ 49,8 % як «посередній», 43,7 % як «достатній» і лише 6,5 % як «недостатній» **(додаток В)**.

Б. А. Кормич указує, що забезпечення інформаційної безпеки повинно здійснюватися «шляхом проведення виваженої і збалансованої політики держави в інформаційній сфері, яка має три основні вектори: захист інформаційних прав і свобод людини; державної безпеки в інформаційній сфері; національного інформаційного ринку, економічних інтересів держави в інформаційній сфері, національних виробників інформаційної продукції» [213, с. 146].

Ґрунтовно дослідивши правове та організаційне забезпечення інформаційної безпеки у воєнній сфери, К. І. Бєляков сформулював принципи її забезпечення, а саме: «свобода збирання, зберігання, використання та поширення інформації; достовірність, повнота та неупередженість інформації; обмеження доступу до інформації виключно на підставі закону; гармонізація особистих, суспільних і державних інтересів; запобігання правопорушенням в інформаційній сфері; економічна доцільність; гармонізація українського законодавства в інформаційній сфері з міжнародним; пріоритетність національної інформаційної продукції» [214, с. 465].

Отже, поняття *інформаційної безпеки* можна розглядати у декількох ракурсах. По-перше, це *стан захищеності інформаційного середовища* суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави. Під *інформаційним середовищем* розуміють сферу діяльності суб’єктів, пов’язану зі створенням, обробленням і

споживанням інформації. По-друге, *інформаційна безпека* – це стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок – обґрунтованість рішень і дій, що приймаються [207].

Адміністративно-правове забезпечення інформаційної безпеки утворює сукупність правових норм, що регламентують суспільні відносини в інформаційній сфері і спрямовані на організаційне, правове та технічне забезпечення обігу інформації [209, с. 12].

З урахування наукового диспуту щодо формулювання поняття «інформаційна безпека» визначимо її особливості у прикордонній сфері:

по-перше, це синтезуюче поєднання реалізації державної політики національної, інформаційної та прикордонної безпеки;

по-друге, інформаційна безпека багатовимірна категорія, що може розглядатись як окремий стан, процес і властивість;

по-третє, відображає рівень захищеності інформаційного середовища у прикордонній сфері, при якому відповідно до вимог законодавства здійснюється та відбувається: реалізація прав та обов'язків суб'єктів інформаційних правовідносин; інформаційна діяльність ДПСУ; інформаційні процеси з використанням усіх існуючих у ДПСУ інформаційних ресурсів; нормальне функціонування інформаційних систем («Гарт», «Аркан» тощо); збереження та цілісність інформації, розпорядником якої є ДПСУ;

по-четверте, здійснюється у процесі управлінням загрозами за допомогою здійснення аналізу ризиків, шляхом обробки інформації для визначення наявних і потенційно можливих ризиків у сфері безпеки державного кордону, урахування як зовнішніх, так і внутрішніх загрозливих факторів;

по-п'яте, усі заходи адміністративного, технічного та іншого характеру вживаються для перешкоджання втручанню та заподіянню негативного впливу інформаційним ресурсам ДПСУ (наприклад, установлення та дотримання чіткого

порядку отримання доступу до конкретного виду інформації, функціонування спеціальних підрозділів (Головного центру зв'язку, автоматизації та захисту інформації ДПСУ) із забезпечення інформаційної безпеки в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах ДПСУ);

по-шосте, потребує вжиття відповідних заходів у відношенні суб'єкта й об'єкта інформаційних відносин;

по-сьоме, стан інформаційної безпеки у межах діяльності ДПСУ безпосередньо впливає та відображає рівень забезпечення прикордонної безпеки країни.

Інформаційна безпека є наслідком діяльності конкретного органу публічної адміністрації у сфері його повноважень. **Інформаційна безпека у діяльності ДПСУ** полягає у забезпеченні функціонування системи своєчасного реагування на випередження, недопущення та усунення інформаційних загроз, що можуть нанести шкоду суб'єктам у прикордонній сфері, об'єктам інформаційно-правового захисту, прикордонній безпеці, а також забезпеченню збереження, цілісності інформації та встановленого порядку доступу до неї. Отже, захист інформації, інформаційних прав є складовими частинами інформаційної безпеки [215, с. 83].

Поняття «інформаційна безпека» у чинному законодавстві досі нормативно не закріплено, хоча згадується у багатьох нормативно-правових актах, проте «захист інформації» в Законі України «Про інформацію» визначено як сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [57, ст. 1]. Перераховані заходи спрямовані на забезпечення збереження інформації, її цілісності й дотримання порядку доступу до інформації. Захисту підлягає будь-яка документована інформація, дані і програми автоматизованих систем, неправомірна дія з якими може спричинити шкоду власникові, користувачеві або іншому учасникові інформаційної діяльності [216]. Під час опитування військовослужбовців ДПСУ з'ясувалось, що 72,7 % респондентів

визначили зміст понять «інформаційна безпека» ширшим за «захист інформації» (27,3 %) **(додаток В).**

Отже, інформаційна безпека є ширшим поняттям і у його межах забезпечується захист інформації з урахуванням специфіки реалізації функцій ДПСУ. Інформаційна безпека у прикордонній сфері є складним систематизованим поняттям, забезпечення якого є підґрунтям (крім власне інформаційної) національної та прикордонної безпеки. Захист інформації передбачає здійснення конкретних заходів, спрямованих на забезпечення збереження вмісту даних, що містяться на матеріальних носіях, забезпечення права на інформацію та дотримання режимних правил доступу до інформації, розпорядником якої є ДПСУ. Тому можна вважати інформаційну безпеку напрямком діяльності ДПСУ, захист інформації її складовою, а їх співвідношення відображається як частина цілого [215, с. 83].

Таким чином, проаналізовані нами положення у межах даного підрозділу дозволили встановити, що у сучасному розумінні політика уособлюється з діяльністю державних структур при активній участі та контролі громадськості. Діяльність держави має багатоманітні напрямки та спрямування, при цьому умови часу обумовлюють модернізацію існуючих та постійне виникнення і визнання нових загальносуспільних сфер інтересів, які необхідно забезпечувати політичною функцією, до таких нових напрямків політики належить інформаційна сфера, при цьому вона як стрімко ввійшла у суспільне життя, так і стрімко розвивається. Зміст інформаційної політики держави, відображає політичну діяльність в окремій сфері – інформаційно-правовій, але є невідокремленою від інших однорідних правових відносин (адміністративних, цивільних та ін.) [217, с. 83].

Прикордонна інформаційна сфера як складова національної безпеки України передбачає оброблення великого масиву інформації, виділення тієї, яка свідчить про ризики та загрози національній безпеці у прикордонній сфері, прогнозування впливу таких загроз і їх попередження, прийняття на цих підставах управлінських рішень посадовими особами ДПСУ. Прикордонна інформаційна

безпека ґрунтується на урахуванні актуальних загроз національній безпеці України, забезпеченні інформаційних прав та визначенні пріоритетів державної політики в інформаційній сфері, залежить від чіткого нормативного регулювання та злагодженої роботи державних органів влади, особливо ДПСУ у напрямку її забезпечення [218, с. 232].

Прикордонна інформаційна безпека поєднує дві термінологічні конструкції «прикордонна» і «інформаційна» безпека, які досі в наукових колах залишаються дискусійними та є порівняно новими, хоча відображають явища, які мають довготривалу історію. Інформаційна безпека у прикордонній сфері полягає у забезпеченні збереження цілісності інформації, режиму доступу до неї та інформаційних ресурсів, які є у розпорядженні ДПСУ, порушення яких може заподіяти значну шкоду прикордонній безпеці держави й окремим сферам національної безпеки, деструктивно вплинути на діяльність прикордонного відомства у виконанні завдань визначених законодавством.

Отже, **державна політика у сфері прикордонної інформаційної безпеки** являє собою діяльність компетентних органів держави із формування правових засад, напрямків інформаційної безпеки та їх реалізації, що ґрунтується на урахуванні загроз територіальній цілісності держави та прикордонній безпеці в інформаційній сфері, спрямована на забезпечення інформаційних потреб сучасного суспільства з оволодіння даними про особливості перетинання державного кордону України, про стан охорони державного кордону та про діяльність прикордонного відомства тощо.

Висновки до розділу 1

Розглянуті погляди вчених у наукових дослідженнях як з інформаційних (І. В. Арістової, К. І. Бєлякова, В. М. Брижка, Р. А. Калюжного, Б. А. Кормича, О. В. Кохановської, А. І. Марущака, О. М. Селезньової, І. М. Сопілко, О. О. Тихомирова, В. С. Цимбалюка, М. Я. Швеця та інших), так і

прикордонних відносин (В. Л. Зьолки, Р. М. Ляшука, О. Б. Фаріона та інших), дозволили диференціювати ці попередньо отримані знання (у вже існуючих дослідженнях) на якісно нові закономірності розвитку інформаційних відносин у межах реалізації форм оперативно-службової діяльності ДПСУ.

Проаналізовані роботи дали змогу встановити не тільки відсутність комплексного дослідження інформаційних відносин у діяльності ДПСУ, але і однозначного розуміння інформаційних відносин, його змісту, структурних елементів, інформації, інформаційної діяльності, інформаційної безпеки.

Обґрунтовано, що дослідження інформаційних відносин у діяльності ДПСУ здійснюється на підґрунті методологічних засад, обрання яких обумовлено специфікою сфери пізнання та спирається на методологічний плюралізм. Дослідження показало, що методологія інформаційних відносин у діяльності ДПСУ є доволі складним і несформованим на сьогодні у межах науки інформаційного права явищем, яке можливо пізнати через систему методів (загальнофілософських, загальнонаукових, науково-правових, спеціально-наукових), на підставі яких здійснюється розкриття теоретико-правових засад інформаційних відносини у прикордонній сфері. З урахуванням особливостей досліджуваних відносин, сформована система методів через онтологічне, гносеологічне, аксіологічне та праксеологічне сприйняття дійсності, які стали теоретичною основою дослідження інформаційних відносин у діяльності ДПСУ, що логічно спирається на методи, характерні для науки інформаційного права, які не є вичерпними. Методологічне дослідження створює умови для пізнання та відображення об’єктивної дійсності цих відносин, а також теоретичне підґрунтя для вирішення практичних завдань у діяльності ДПСУ.

Методологічний підхід до вивчення теоретичних засад інформаційних відносин у прикордонній сфері зумовлює такі особливості: створює теоретичну основу для формування нових змістовно якісних знань відповідно до сучасних умов розвитку інформаційних відносин у прикордонній сфері; формує логічні засади процесу опрацювання великого обсягу інформації, теоретичного та практичного значення, пов’язаної з інформаційною діяльністю ДПСУ; обумовлює

дослідження чіткими теоретичними та практичними цілями; результат дослідження залежить від оптимально обраного методологічного інструментарію, що залежить від світогляду науковця, специфікою прикордонної сфери та очікуваним результатом дослідження; є фундаментом для вироблення та уніфікації понятійного апарату інформаційних відносин; забезпечує всебічність отримання інформації про інформаційні відносини у прикордонній сфері; вибір методологічного інструментарію залежить від конкретного науковця, а, отже, має суб'єктивний характер, причому існує об'єктивно і не залежить від волі дослідника.

У результаті проведеного дослідження інформаційних відносин автором визначені їх особливості, які характерні в діяльності ДПСУ та обумовлюють правову природу цих відносин: вони є різновидом суспільних відносин, притаманних сфері охорони державного кордону, специфічність яких обумовлюється динамічними процесами, пов'язаними з охороною державного кордону, забезпеченням контролю за його перетинанням, підтриманням прикордонного режиму та утриманням державного кордону; урегульовуються нормами інформаційного, адміністративного, кримінального та інших галузей права, а також нормами прикордонного законодавства; носять публічний характер у зв'язку із тим, що відбуваються за участі та ресурсів органу публічної адміністрації, – ДПСУ; абсолютний характер цих відносин означено конкретизацією одного із суб'єктів – розпорядника інформації у сфері охорони державного кордону, де інший суб'єкт не визначений; характер та мета таких відносин обумовлюється інформаційною потребою з приводу інформації у діяльності ДПСУ та визначає вид інформаційної діяльності; стосуються інтересів суміжних держав, фізичних і юридичних осіб, які перетинають державний кордон або здійснюють різну діяльність уздовж чи безпосередньо на державному кордоні України, а також стосуються інтересів персоналу ДПСУ; є інформаційною складовою прикордонної безпеки, інформаційної безпеки держави, що в загальному впливає на забезпечення державної та національної безпеки; мають подвійну спрямованість: внутрішнє та зовнішнє. До внутрішніх належать

інформаційні відносини, пов’язані зі здійсненням органами та підрозділами ДПСУ завдань щодо реалізації їх інформаційно-правового статусу. До зовнішніх належать відносини, пов’язані з правом на інформацію, інформаційними потребами осіб у зв’язку з функціонуванням ДПСУ.

Інформаційні відносини у діяльності ДПСУ – це різновид суспільних відносин у сфері охорони державного кордону, які урегульовані нормами (інформаційного, адміністративного та інших галузей) законодавства, а також нормами законодавства у прикордонній сфері, які обумовлені реалізацією прав, потреб і процесів щодо інформації, що пов’язана з діяльністю або створюється у процесі виконання завдань ДПСУ.

Складовими елементами змісту інформаційних відносин у діяльності ДПСУ є: суб’єкт (загальний – фізичні та юридичні особи, громадські організації тощо, які мають інтерес чи право, пов’язане з інформацією у сфері діяльності ДПСУ та особливий – ДПСУ та усі її структурні підрозділи), зміст (інформаційні прав та обов’язки) та об’єкт (інформація, пов’язана із функціонуванням органів охорони державного кордону, забезпеченням охорони та порядком перетинання державного кордону).

Особливим суб’єктом досліджуваних відносин є ДПСУ як суб’єкт владних повноважень і розпорядник інформації у сфері відповідальності. У межах структури ДПСУ виділено спеціальні суб’єкти інформаційних відносин: Управління апаратної роботи, Департамент інформаційно-аналітичного та документального забезпечення, Головний центр зв’язку, автоматизації та захисту інформації, Контактний центр (служба «Довіра»), підрозділи документального забезпечення, інформаційно-аналітичні підрозділи). Правовий статус спеціальних суб’єктів обумовлений безпосереднім здійсненням інформаційної діяльності за окремими напрямками: оприлюднення публічної інформації; надання консультування та прийняття заяв, звернень; забезпечення обігу оперативно-службової інформації; документування, робота з управлінськими, внутрішньоорганізаційними й індивідуальними документами; обробка електронної інформації; забезпечення захисту інформації.

Проблемність інформаційної правосуб'єктності органів і підрозділів охорони державного кордону полягає у тому, що вона чітко не визначена й несистематизована. Відносно органів ДПСУ як суб'єктів владних повноважень їх інформаційна правосуб'єктність, передбачена у значній кількості нормативно-правових актів, що, як правило, закріплюють обов'язки щодо оприлюднення офіційної публічної інформації, надання інформації у порядку звернення (запиту) та захисту інформації з обмеженим доступом.

Прикордонна інформаційна безпека ґрунтується на врахуванні актуальних загроз національній безпеці України, забезпеченні інформаційних прав і визначенні пріоритетів державної політики в інформаційній сфері, залежить від чіткого нормативного регулювання та злагодженої роботи усіх структурних елементів ДПСУ у напрямку її забезпечення.

Визначено, що державна політика у сфері прикордонної інформаційної безпеки – це діяльність компетентних органів держави із формування правових засад, напрямків інформаційної безпеки та їх реалізація, що ґрунтується на урахуванні загроз територіальній цілісності держави та прикордонній безпеці в інформаційній сфері, спрямована на забезпечення інформаційних потреб сучасного суспільства з оволодіння даними про особливості перетинання державного кордону України, про стан охорони державного кордону та про діяльність прикордонного відомства тощо.

РОЗДІЛ 2
НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ВНУТРІШНЬОВІДОМЧИХ ІНФОРМАЦІЙНИХ ВІДНОСИН У ДІЯЛЬНОСТІ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

2.1 Нормативно-правове регулювання інформаційних відносин у діяльності Державної прикордонної служби України

Серед усієї складної системи забезпечення охорони державного кордону України (оперативної, технічної, фізичної тощо) своє особливе місце посідає її інформаційна складова. Сьогодні виконання поставлених перед ДПСУ завдань щодо забезпечення недоторканності державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні перебуває у нерозривному взаємозв'язку з прогресуючим розвитком інформаційних відносин та їх нормативно-правовим регулюванням, що обумовлено встановленням і поступовим збільшенням правових меж регулювання у зв'язку з обігом інформації, здебільшого в публічних органах влади.

Складне та динамічне безпекове середовище довкола України, а також узяті Україною в рамках виконання Плану дій щодо лібералізації ЄС візового режиму для України та імплементація Порядку денного асоціації між Україною та ЄС, запровадження у зв'язку із цим європейських стандартів інтегрованого управління кордонами обумовлюють необхідність модернізації інформаційної складової системи охорони державного кордону [59]. Важливість та актуальність нормативно-правового регулювання інформаційної складової у діяльності ДПСУ зростає з розвитком інформації, інформаційних ресурсів та інформаційних технологій у сфері охорони державного кордону.

Роль ДПСУ як суб'єкта владних повноважень і розпорядника інформації у межах компетенції у цих відносинах виявляється через цілеспрямований вплив на інформаційну сферу, пов'язану з охороною державного кордону. Характеризуючи

«вплив» ДПСУ на інформаційні відносини та внутрішньовідомчі інформаційні зв'язки цих відносин доцільно аналізувати їх у площині інформаційної діяльності ДПСУ, яка відображає внутрішньовідомчий аспект інформаційних відносин.

Загальні питання нормативно-правового регулювання інформаційної діяльності розглядались науковцями переважно у межах джерел інформаційного права, інформаційних відносин чи інформаційного законодавства, зокрема у працях: В. М. Брижка С. О. Дорогих, Р. А. Калюжного, Л. П. Коваленка, Б. А. Кормича, О. В. Кохановської, А. Л. Петрицького, В. Г. Пилипчуа, О. М. Селезньової, І. М. Сопілко, М. Я. Швеця та інших. Однак питання нормативно-правового регулювання інформаційної складової системи забезпечення охорони державного кордону України окремо не досліджувались.

Через нормативно-правове регулювання відбувається упорядкування інформаційних відносин у сфері охорони державного кордону, утвердження інформаційно-правового статусу, меж функціонування ДПСУ та різноманітні можливі зв'язки з іншими суб'єктами у цих правовідносинах. Загалом нормативно-правове регулювання інформаційної складової в діяльності ДПСУ відображає дію норм права на відносини, об'єктом яких є інформація у сфері охорони державного кордону, та упорядкування інформаційної діяльності органів і підрозділів ДПСУ.

Опитування показало, що 58,9 % респондентів достатньою мірою інформовані про нормативно-правове регулювання відносин пов'язаних зі створенням, збиранням, одержанням, зберіганням, використанням, поширенням, охороною та захистом інформації в діяльності ДПСУ, 13,4 % – ні і 27,7 % не змогли відповісти. Зокрема, 69,3 % вказали, що джерелом знань про правове регулювання цих відносин є нормативно-правові акти, 59,7 % навчання у НАДПСУ, 49,8 % особистий досвід, з досвіду колег (підрозділу) (34,2 %) та 13,4 % навчання у інших вищих навчальних закладах **(додаток В)**. Вважаємо, що якісна основа системних знань інформаційного законодавства повинна закладатись та формуватись під час навчання майбутніх офіцерів-прикордонників.

Інформаційна сфера є середовищем обігу інформації (виробництво – поширення – споживання), при якому суб'єкти реалізують свої потреби і можливості відносно інформації [219, с. 133]. При цьому до об'єктів інформаційної сфери належить: інформація, у тому числі інформаційні ресурси, зафіксована на відповідних носіях інформація; інформаційна інфраструктура, що містить сукупність інформаційних систем: організаційні структури, інформаційно-телекомунікаційні структури, інформаційні, комп'ютерні та телекомунікаційні технології, системи засобів масової інформації [219, с. 137–139]. Системне нормативно-правове регулювання інформаційної сфери безпосередньо впливає на забезпечення інформаційної безпеки, яка у прикордонній сфері полягає в забезпеченні збереження цілісності інформації та інформаційних ресурсів, які є у розпорядженні ДПСУ, порушення яких може заподіяти значну шкоду прикордонній безпеці держави, деструктивно вплинути на діяльність прикордонного відомства у виконанні завдань, визначених законодавством.

Інформаційні відносини, змінюються і припиняються в інформаційній сфері та регулюються інформаційно-правовими нормами [48, с. 166]. Тому інформаційна діяльність ДПСУ здійснюється відповідно до визначених меж повноважень, закріплених Конституцією і законами України, що обумовлено ст. 6 Конституції України. Саме тому Б. Кормич підкреслює, що «Конституція України, безумовно, є одним з найважливіших джерел інформаційного права, формуючи основи правового регулювання в цій галузі» [220, с. 48].

Закон України «Про інформацію» визначає, що основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації [57, с. 9]. С. О. Дорогих, спираючись на цю норму, визначив, що інформаційна діяльність пов'язана зі «збиранням, зберіганням, поширенням та захистом інформації (інформаційних ресурсів) в інтересах відповідного правоохоронного органу», а особливості обумовлені компетенцією конкретного органу [221, с. 186]. Тут варто доповнити, що інформаційна діяльність ДПСУ здійснюється не тільки у власних інтересах,

але й інтересах інших суб’єктів інформаційних відносин, зокрема задоволення інформаційних потреб через запит на інформацію, інформування громадськості про результати діяльності тощо, тобто враховує внутрішні та зовнішні інформаційні інтереси.

Інформаційна складова передбачає «діяльність, спрямовану на задоволення інформаційних потреб громадян, юридичних осіб і держави, що реалізується через інформаційні процеси, які охоплюють виробництво, поширення, пошук, одержання, споживання, зберігання інформації та утворюють інформаційні продукти і впорядковані інформаційні ресурси, а також через формування інформаційно-телекомунікаційної інфраструктури, засобів зв’язку та засобів інформаційної безпеки» [30, с. 77]. Опитані респонденти висловили своє розуміння змісту поняття «інформаційна складова» у сфері охорони державного кордону, як: порядок обігу інформації у діяльності ДПСУ (31,8 %), елемент у системі забезпечення охорони державного кордону (26,4 %), система інформаційних відносин у ДПСУ (18,2 %), функціонування інформаційних систем ДПСУ (17,3 %) **(додаток В).** У нормативно-правових актах [59] інформаційна складова зазначається як елемент у системі забезпечення охорони державного кордону, але з урахуванням її змісту можна розглядати її як вияв інформаційних відносин у діяльності ДПСУ.

Інформаційну діяльність ДПСУ можна розглядати як реалізацію (втілення) її основних видів (створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації), пов’язаних із процесами, які здійснюються з інформацією в інтересах охорони державного кордону та реалізацією прав людини, пов’язаних з вільним перетинанням державного кордону та дотриманням у зв’язку із цим інформаційних прав усіх суб’єктів прикордонних відносин. У такому випадку, досліджувана інформаційна складова забезпечує керованість підпорядкованими органами та підрозділами у здійсненні такої діяльності.

Інформаційна діяльність безпосередньо спрямована на виконання завдань, що стоять перед інформаційним суспільством [219, с. 13], а також забезпеченням

інформаційної складової ДПСУ. Основні засади інформаційної діяльності всіх суб'єктів відповідних відносин з урахуванням розвитку інформаційного суспільства закріплені в нормах Основного закону, через аналіз яких можна визначити такі принципові положення відносно внутрішньої інформаційної діяльності ДПСУ: інформаційна безпека України пронизує всю діяльність ДПСУ [126, ст. 17]; дотримання режимів обігу інформації – відкритої та обмеженої в обігу (конфіденційна, таємна та службова) [126, ч. 3 ст. 32]; дотримання усіх інформаційних прав інших суб'єктів інформаційних правовідносин [126, ч. 1 ст. 32, ст. 31, ч. 3 ст. 32, ст. 34]. Інформаційну діяльність ДПСУ пронизує вся видова різноманітність процесів (створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації) такого функціонування, закріпленого у ст. 9 Закон України «Про інформацію» [57, ст. 9].

Під час проведення опитування військовослужбовців ДПСУ їм було запропоновано відповісти на питання «Який із видів інформаційної діяльності Вам частіше доводиться реалізовувати у своїй службовій діяльності?» із можливістю обрати декілька варіантів запропонованих відповідей. Результати були отримані такі: одержання інформації (57,6 %), збирання інформації (55,8 %), використання інформації (52,8 %), зберігання інформації (37,7 %), створення інформації (25,1 %), інформаційно-аналітична діяльність (23,4 %), складно відповісти (19 %), охорона та захист інформації (15,6 %), робота із запитами і зверненнями громадян (9,5 %), забезпечення безпеки та функціонування інформаційних систем (9,1 %), і лише 7,4 % оприлюднення відкритої публічної інформації **(додаток В)**. Отже, переважно у внутрішній службовій діяльності ДПСУ відбувається одержання, збирання та використання інформації.

В. Г. Пилипчук та В. М. Брижко констатують, що види інформаційної діяльності знаходяться в жорстких рамках того, що прописане в Конституції України (збирання, зберігання, використання, поширення), хоча сучасний електронний простір (е-простір) визначає свої види діяльності (обробка, введення, виведення, передача, компіляція, відображення даних та ін.). При цьому види

інформаційної діяльності, які подано у ст. 9 Закону України «Про інформацію» не повною мірою відповідають видам, визначеним ст. 32 Конституції України [222, с. 12]. Отже, Конституцією України урегульована класична модель інформаційних компетенцій у вигляді меж дозволеного та забороненого, визначенні прав та обов'язків, а також їх співвідношення, коли інформаційне право одного суб'єкта (наприклад, отримання інформації про наявність або відсутність стосовно фізичної особи тимчасового обмеження у праві виїзду з України або в'їзду в Україну) відповідає обов'язку іншого (наприклад, органу публічної влади надати таку інформацію за запитом особи у встановленому законодавством порядку).

Конституція України визначає основні інформаційні права, а також установлює інші норми, які прямо чи опосередковано детермінують внутрішньовідомчі інформаційні правовідносини. Зазначені норми Конституції України формують ті положення, що знаходять свій подальший розвиток у законах і підзаконних нормативно-правових актах нашої держави [14, с. 113].

Загальні правила здійснення інформаційної діяльності урегульовані нормативно-правовими актами, які визначають правосуб'єктність ДПСУ як суб'єкта інформаційних відносин. До них належать: закони України «Про інформацію», «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про Національну програму інформатизації», «Про науково-технічну інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про доступ до публічної інформації», «Про звернення громадян», «Про захист персональних даних» тощо; укази Президента України «Питання забезпечення органами виконавчої влади доступу до публічної інформації», «Про першочергові заходи щодо забезпечення реалізації та гарантування конституційного права на звернення громадян до органів державної влади та органів місцевого самоврядування»; постанови та розпорядження КМУ «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що

містять службову інформацію», «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах»; «Про затвердження Плану заходів з реалізації Концепції розвитку електронного урядування в Україні», «Деякі питання документування управлінської діяльності» тощо. О. М. Селезньова називає цю групу правових актів базовими, які визначають основні положення інформаційного права [14, с. 114].

Окремо варто виділити нормативні акти, які регулюють порядок, підстави та організацію здійснення інформаційної діяльності як інформаційної складової у функціонуванні ДПСУ. До них належать: закони України «Про Державну прикордонну службу України», «Про державний кордон України», «Про прикордонний контроль», «Про оперативно-розшукову діяльність», накази МВС України «Про затвердження Порядку дій посадових осіб Державної прикордонної служби України та органів Національної поліції України у разі виявлення в пунктах пропуску через державний кордон України осіб, автомобільних транспортних засобів і паспортних документів, які перебувають у банках даних інформаційної системи Міжнародної організації кримінальної поліції – Інтерполу», «Про затвердження Інструкції з організації обліку особового складу ДПСУ», «Про затвердження Інструкції з проведення аналізу ризиків у ДПСУ», відомчі накази Адміністрації ДПСУ «Положення про базу даних «Відомості про осіб, які перетнули державний кордон України», «Положення про інформаційно-телекомунікаційну систему прикордонного контролю «Гарт-1» ДПСУ», «Про організацію обміну інформаційними повідомленнями», «Про обмін відкритою знеособленою інформацією про виявлені підроблені документи та ознаки правопорушення», «Про затвердження Інструкції з діловодства в ДПСУ», «Про затвердження Положення про Головний аналітичний центр ДПСУ», «Про затвердження Переліку відомостей, що становлять службову інформацію у ДПСУ», «Про затвердження Інструкції із захисту публічної інформації у Державній прикордонній службі України», міжвідомчі накази «Про затвердження Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну

систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон» тощо.

І. М. Сопілко підкреслює, що такі нормативні акти врегульовують можливості органів державної влади України щодо дій з інформацією та інформаційними ресурсами, зокрема стосовно їх отримання від інших учасників інформаційних відносин, а також правовий статус того чи іншого органу державної влади, або встановлюють процедуру реалізації важливих державних функцій [20, с. 23]. О. М. Селезньова виділяє закони в галузі інформаційного права, що регулюють конкретну сферу інформаційних відносин в окрему групу, предметних законів [14, с. 114].

На нашу думку, їх можна назвати спеціальними нормативно-правовими актами, що врегульовують інформаційну діяльність ДПСУ і сферу охорони кордонів, за яку відповідальне прикордонне відомство. Ці нормативні акти спрямовані на врегулювання інформаційних відносин у межах функціонування всіх структурних підрозділів ДПСУ та її посадових осіб.

Окреме місце у врегулюванні інформаційної діяльності, на нашу думку, належить програмним документам, затвердженим КМУ, таким як Стратегія ІУК, Стратегія розвитку ДПСУ (далі – Стратегія), схваленим рішенням Колегії ДПСУ, у яких визначають основі напрямки розвитку відомства на близьку та середню перспективи з урахуванням реально існуючих загроз і потреб розвитку прикордонної сфери. Також формулюються конкретні завдання за окремими напрямками діяльності, які є найбільш вразливими [223, с. 168].

Проаналізовані положення Стратегії дозволили нам узагальнити, що вона визначає та конкретизує напрямки інформаційної діяльності ДПСУ у межах, визначених законодавством, з урахуванням загроз у сфері охорони державного кордону, інтеграційних процесів та удосконалення її інформаційної складової. Стратегія передбачає здійснення таких процесів з інформацією, як обмін інформацією, накопичення, оброблення, оцінка й аналіз інформації, які розширюють і доповнюють видову різноманітність інформаційної діяльності, на відміну від тієї, що закріплена в Законі України «Про інформацію».

Разом із наявністю великого обсягу норм, що врегульовують досліджувані відносини, у результаті їх аналізу було виявлено низку проблемних чинників: по-перше, правові акти були видані у різний час різними уповноваженими на те органами і за різних підстав. У результаті цього в законодавстві поступово виникають норми, які часто є неузгодженими, суперечливими і застарілими, що значно ускладнює їх реалізацію та потребує систематизації інформаційного законодавства [48, с. 166]. Наприклад, у нормах законів України, які були прийняті з невеликим проміжком у часі «Про захист персональних даних» та «Про доступ до публічної інформації» використані поняття «персональні дані» і «конфіденційна інформація», що стосуються фізичних осіб не є тотожними і містять різні вимоги щодо оформлення запитів на інформацію [224]; по-друге, при установленні, як правило, нових інформаційних прав законодавець не завжди вчасно визначає механізм його реалізації, наприклад, право використання електронного цифрового підпису при подачі громадянами електронного запиту до сьогодні неможливо забезпечити в ДПСУ у зв'язку із зазначеними умовами; по-третє, неузгодженість термінології в інформаційному законодавстві, зокрема «персональні дані», «конфіденційна інформація», «службова інформація» у різних законах, що регулюють право на отримання та обробку інформації.

Отже, **нормативно-правове регулювання інформаційної складової у діяльності ДПСУ** передбачає упорядкування інформаційних відносин на підставі сукупності чинних нормативно-правових актів, що визначають основні засади, принципи, механізми забезпечення обігу інформації, зокрема й з використанням інформаційно-телекомунікаційних систем у сфері охорони державного кордону, та здійснюється в процесі виконання завдань ДПСУ.

Інформаційна складова в діяльності ДПСУ урегульована системою нормативно-правових актів різного рівня ієрархії, а саме: Конституцією України (визначає основні інформаційно-правові засади такої діяльності); загальними або базовими нормативно-правовими актами, які визначають основні положення інформаційного права; спеціальними нормативно-правовими актами, що врегульовують інформаційну діяльність у межах повноважень ДПСУ;

програмними документами, що формулюють основі напрямки розвитку відомства на близьку та середню перспективи з урахуванням актуальних загроз і потреб розвитку сфери охорони державного кордону.

У зазначених нормативно-правових актах згадується ширше коло видів інформаційно-правової діяльності, пов'язаних зі сферою охорони державного кордону, за ті, які визначені у статті 9 Закону України «Про інформацію», а саме: обмін інформацією, накопичення, оброблення, оцінка та аналіз інформації. Переважно вони стосуються внутрішньоорганізаціних завдань, спрямованих на забезпечення актуальних питань виявлення загроз, їх аналіз у сфері охорони державного кордону та є обмеженими у доступі, що буде окремо проаналізовано нами у наступному підрозділі.

2.2 Правовий режим інформації з обмеженим доступом

Уся інформація, яка перебуває в межах правового регулювання відповідно до Закону України «Про інформацію», поділяється за порядком доступу на відкриту інформацію та інформацію з обмеженим доступом. Умовно вся інформація є відкритою, за виключенням тієї, яка цим Законом віднесена до інформації з обмеженим доступом [57, ст. 20]. Категорія щодо інформації «з обмеженим доступом», порівняно із «відкритою», передбачає застосування додаткових заходів щодо її обігу, використання, розповсюдження й захисту, що загалом відображає правовий режим інформації.

Установлення певного режиму зумовлено досягненням конкретної мети, це може бути дотримання законності, забезпечення виконання завдань органом публічної адміністрації, захист прав, свобод, інтересів і цінностей тощо. Діяльність ДПСУ спрямована на забезпечення недоторканності державного кордону та охорону суверенних прав України в її прилеглій зоні та виключній (морській) економічній зоні [79, ст. 1]. Беззаперечно й цілком справедливо окреслює В. Л. Зьолка взаємопов'язаність реалізації національних інтересів у

прикордонній сфері, метою якої є гарантування суверенітету, незалежності і територіальної цілісності, з системою забезпечення охорони національних інтересів як її складовий елемент [225, с. 1]. Отже, діяльність ДПСУ спрямована на охорону національних інтересів України в межах відомчої компетенції, що знаходиться у нерозривному зв'язку із забезпеченням обігу інформації, значна частина якої обмежена у доступі.

Серед основних завдань Стратегії розвитку ДПСУ передбачено удосконалення механізму обміну інформацією, розширення формату обміну інформацією, проведення спільного аналізу ризиків ДПСУ із суб'єктами інтегрованого управління кордонами та прикордонними органами держав – членів ЄС – Республіки Польща, Словацької Республіки, Румунії та Угорщини, а також Республіки Молдова та Республіки Білорусь, Європейською агенцією з питань управління оперативним співробітництвом на зовнішніх кордонах держав – членів ЄС, а також міжнародними організаціями й установами у межах забезпечення ефективної реалізації політики у сфері безпеки державного кордону, а також охорони суверенних прав України в її виключній (морській) економічній зоні [59]. Така діяльність вимагає чіткої диференціації видів інформації за порядком доступу. Теоретичне опрацювання правового режиму інформації з обмеженим доступом також зумовлено практичним значенням питань захисту інформації у діяльності ДПСУ, а також інформаційних прав суб'єктів у прикордонній сфері. Тому розгляд правового режиму інформації з обмеженим доступом набуває неабиякої важливості, зокрема в умовах сьогодення, триваючої загрози територіальній цілісності й національній безпеці (на сході країни), що визначає актуальність тематики дослідження цього підрозділу.

Правовому режиму інформації присвячено чимало наукових праць, як монографічних (Є. Ф. Збінський, В. А. Ліпкан, О. А. Мандзюк, О. В. Шепета), так і наукових статей (В. Ю. Баскаков, І. Л. Бачило, О. О. Крестьянінов, В. А. Ліпкан, О. А. Мандзюк та інші). Але такі розробки переважно стосуються загальної теоретичної характеристики правового режиму або окремого виду інформації, що обмежена в доступі. Окремо варто зазначити праці, присвячені цим питання щодо

обігу податкової інформації («Правовий режим податкової інформації в Україні», В. А. Ліпкан, О. В. Шепета, О. А. Мандзюк; «Правовий режим податкової таємниці в Україні», В. А. Ліпкан, Є. Ф. Збінський). Окремо варто згадати дослідження А. І. Коротушака «Місце та значення правового механізму в структурі механізму державного управління публічною інформацією з обмеженим доступом у ДПСУ» [226] та «Мотиваційний механізм в структурі державного управління публічною інформацією у Державній прикордонній службі України» [227], але у зазначених роботах акцентовано увагу на механізмі управління публічною інформацією та інформацією з обмеженим доступом.

Категорія «правовий режим інформації» використовується у чинних нормативно-правових актах, зокрема у законах України «Про інформацію», «Про науково-технічну інформацію» та інших, але досі не отримала законодавчого визначення. Загалом термін «режим» досить широко застосовується як в юридичних, так і в інших галузях науки. Проаналізоване тлумачення цього терміна у словнику Сучасної української мови дозволило виділити такі його характеристики щодо теми нашого дослідження, а саме: систему заходів, правил, запроваджуваних для досягнення певної мети; певні умови, необхідні для забезпечення роботи, функціонування, існування чого-небудь [43, с. 1206].

Правовий режим інформації розглядається як «передбачений чинним законодавством особливий порядок правового регулювання суспільних відносин, що здійснюється за допомогою системи спеціальних юридичних засобів у сфері суспільно значимих відомостей та/або даних, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, що створені чи одержані в межах повноважень, передбачених законодавством, з метою забезпечення ефективного функціонування відповідної системи інформації» [228, с. 4].

У межах діяльності ДПСУ правовий режим інформації з обмеженим доступом набуває додаткових ціннісних характеристик, обумовлених прикордонною сферою, де прикордонна сфера являє собою комплексну систему складних відносин, елементів, від чіткого й ефективного забезпечення яких

залежить безпека державного кордону, територіальна цілісність, безпека держави та її громадян. Одним з ключових елементів цієї системи є інформаційна сфера («складова», термін, що використовується у Стратегії розвитку) та інформаційна безпека.

Правовий режим інформації є одним із головних визначальних чинників прикордонної безпеки, а саме: важливим засобом захисту та збереження цілісності інформації, розпорядником якої є ДПСУ. Мета його встановлення полягає у визначенні та дотриманні додаткових обмежувальних заходів для доступу до інформації та захисті тієї частини інформації, розголошення якої може завдати значної шкоди національним інтересам у прикордонній сфері [229, с. 182].

Для забезпечення обробки та захисту інформації правовими нормами встановлюється система правил, умов і заходів, які спрямовані на організацію обігу, обмеження в доступі й охорону інформації. Така система заходів є правовим режимом інформації, що спрямований на досягнення конкретної мети. У юридичній літературі зазначається, що єдиною метою адміністративно-правових режимів є забезпечення загальної безпеки в державі [230, с. 4]. Разом з тим установлення режиму інформації з обмеженим доступом здійснюється з метою упорядкування суспільних відносин, що виникають у сфері інформації з обмеженим доступом, та має подвійну мотивацію: необхідність реалізації права на інформацію та захист національних інтересів між різними запитувачами інформації та розпорядниками інформації [231, с. 130–131].

Правовий режим інформації, зазначають Н. І. Логінова та Р. Р. Дробожур, містить: право використання інформації; право володіння інформацією; право доступу до інформації; право власності та інші майнові права на різні носії, що містять документовану інформацію; право поширення та надання інформації [232, с. 55]. Правовий режим передбачає не тільки визначення інформаційних прав, які є частиною інформаційного статусу суб’єктів відповідних відносин, а й порядок отримання, користування, розповсюдження та захисту інформації, тобто умови обігу інформації. Найбільш повно визначає елементи правового режиму

інформації Т. В. Чернишова, а саме: порядок створення (або збирання) відповідної інформації; право власності на інформацію; порядок збереження, розповсюдження та використання інформації; порядок доступу до інформації; порядок правового захисту інформації [233, с. 100]. На нашу думку, варто додати такий елемент, як порядок віднесення інформації до інформації з обмеженим доступом **(додаток Г).**

С. Г. Гордієнко зазначає, що стосовно кожного різновиду інформації з обмеженим доступом (науковець застосував узагальнену категорію «таємниця») характерне визначення: ознак таємності, кола суб'єктів, що мають право на кожну з таємниць, прав та обов'язків осіб, які стосуються певних видів таємниць, відповідальності за розголошення інформації, що повідомляється, та особливостей захисту для кожного виду таємниць [234, с. 233]. Отже, можна констатувати, що для кожного різновиду інформації, що обмежена в доступі, характерне встановлення конкретних меж правового режиму.

Закон України «Про інформацію» встановлює, що інформація з обмеженим доступом є конфіденційна, таємна та службова [57, ч. 1, ст. 21] та визначає, що відносини, пов'язані з правовим режимом конфіденційної інформації [57, ч. 2, ст. 21], порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами [57, ч. 3, ст. 21]. Хоча варто зазначити, що з переліку видів інформації найбільше урегульована й захищена таємна інформація. Щодо службової інформації, її правовий режим урегульований на рівні урядових (постанов КМУ «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію», «Про затвердження Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях»), відомчих нормативно-правових актів, а також наказів, розпоряджень командирів (начальників) відповідних структурних підрозділів ДПСУ. За таких умов можливе як посилення режимних заходів, які спрямовані на забезпечення режиму службової інформації, з урахуванням

усвідомлення відповідальності конкретного начальника за збереження такої інформації, так і необґрунтоване (суб'єктивне) обмеження в доступі «потрібної» інформації від широкого загалу. Тому з метою забезпечення балансу та вжиття адекватних заходів для підтримання режиму службової інформації, який би обґрунтовував її призначення та суть, необхідне чітке законодавче регулювання та розмежування.

У ході проведеного опитування 82,7 % респондентів відповіли, що до інформації з обмеженим доступом належить «службова інформація», 80,1 % – «таємна», 71,4 % – «конфіденційна», 23,4 % – «будь-яка інформація у сфері діяльності ДПСУ», 13,9 % – «корпоративна інформація» **(додаток В)**. Переважна більша частина опитаних надали свої варіанти відповідно до норм чинного законодавства, але відсутність чітких знань інформаційного законодавства іншою частиною опитуваних може свідчити про можливі порушення та недодержання режиму відповідного виду інформації з обмеженим доступом у службовій діяльності.

Загальним обмеженням відносно інформації з обмеженим доступом є те, що до неї не можна віднести такі відомості, з урахуванням прикордонної сфери це: про стан довкілля; про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей; про медичне обслуговування та соціальне забезпечення (стосується тільки військовослужбовців ДПСУ), а також про стан правопорядку у сфері охорони державного кордону; про факти порушення прав і свобод людини; про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових і службових осіб (у межах забезпечення інтегрованого управління кордонами); інші відомості, доступ до яких не може бути обмежено відповідно до законів і міжнародних договорів України, згода на обов'язковість яких надана ВРУ [57, ч. 4 ст. 21].

Отже, проведений аналіз змісту поняття «правовий режим інформації з обмеженим доступом у діяльності ДПСУ» можемо охарактеризувати як:

систему закріплених законодавством заходів і правил, що супроводжують процеси отримання, зберігання та надання тощо інформації з обмеженим доступом у сфері охорони державного кордону України;

чітке розмежування видів інформації з обмеженим доступом для визначення обсягу та меж правового режиму й обрання конкретних заходів (інструментів) правового впливу;

мета його встановлення обумовлена обмеженням загального доступу до інформації, зміст якої визначає захищеність національних інтересів, державної безпеки, з урахуванням нашого дослідження, – прикордонної безпеки;

утворює умови для обігу та збереження цілісності та змісту інформації у функціонуванні ДПСУ, необхідної для виконання поставлених перед нею завдань.

Основними елементами правового режиму інформації з обмеженим доступом у діяльності ДПСУ є:

прядок і підстави здійснення інформаційної діяльності з відповідним видом інформації, що обмежена в доступі (створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації, а також порядок віднесення та скасування інформації, обмеженої у доступі);

права посадових осіб ДПСУ щодо здійснення окремих процедур із такою інформацією;

процедура отримання допуску до цієї інформації;

відповідальність за порушення встановленого режиму інформації.

Отже, **правовий режим інформації з обмеженим доступом** у діяльності ДПСУ пропонуємо розглядати як установлені законодавством процедури та порядок надання дозволу, доступу, охорони, захисту, а також здійснення діяльності з інформацією, яка становить значну цінність для прикордонної безпеки держави. Загальною проблематикою щодо упорядкування інформаційних відносин, пов’язаних з інформацією, яка законодавством обмежена в доступі, є багатозначність і розбіжність окремих правових норм, що врегульовують ці відносини.

Згідно зі ст. 21 Закону України «Про інформацію» конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень [57, ч. 2 ст. 21]. При цьому Закон України «Про інформацію», а не особа визначає, яка саме інформація про фізичну особу, обмежена в доступі, є конфіденційною: дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження [57, ч. 2 ст. 11]. Опитані респонденти відповіли, що, на їхню думку, конфіденційною інформацією є: 74 % інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, 13,4 % службова інформація, 7,8 % інформація про фізичну особу, 4,8 % інформація про посадову особу. На питання «Чи потрібне бажання (згода) особи на поширення її конфіденційної інформації?» майже однозначно 96,5 % відповіли «так» **(додаток В).** Отже, така інформація без згоди особи на збирання, зберігання, використання та поширення не допускається. Тобто обмеження встановлені Законом України «Про інформацію» «за замовчуванням». Разом з тим інформація про фізичну особу може бути і іншою – будь-які відомості чи сукупність відомостей, які можуть ідентифікувати особу. У той же час частина інформації про особу, що є представником публічної сфери, підлягає публічному розголошенню (наприклад, Декларації про доходи). Тому частина конфіденційної інформації про особу може бути обмежена самою особою, як це зазначено у ч. 2 ст. 21 Закону України «Про інформацію», так і законом, що апріорі не передбачено у законодавчому визначенні такої інформації.

Відповідно до ст. 9 Закону України «Про доступ до публічної інформації» до службової може належати така інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади,

процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці [97, ст. 9].

Важливим індикатором правового регулювання службової інформації є означення двох її субстанцій. По-перше, це сталий стан, що відображає зміст відомостей про прийняті у процесі управління посадовими особами розпорядження, плани організації та діяльності охорони державного кордону, а також інша інформація про обстановку на кордоні, про особливості організації охорони кордону тощо, а також динамічний стан – розголошення цих відомостей може мати негативні наслідки у сфері державної безпеки [135].

Ключову роль у цьому відіграє слово «може». Важко наперед спрогнозувати напевно, що відомості або дії з інформацією призведуть до зазначених наслідків. У сучасному інформаційному суспільстві, в умовах загострення інформаційної війни будь-яку інформацію можна «перекрутити» в інтересах супротивника. Тому такий критерій є відносний і сумнівний щодо класифікації службової інформації, який має як свої позитивні, так і негативні тенденції. З одного боку, ДПСУ забезпечує збереження інформації, шляхом обмеження її у доступі, з іншого – втрачається можливість контролю, чи дійсно конкретна інформація підлягає обмеженню або її приховують від громадського контролю. Тому службова інформація має відносний характер.

При цьому ч. 2 ст. 6 Закону України «Про доступ до публічної інформації» встановлює основні питання, які необхідно вирішити, а спільна єдність яких дозволяє посадовим особам ДПСУ відносити інформацію до службової:

1) яких саме стосується інтересі національної безпеки, територіальної цілісності або громадського порядку, чи сприятиме: запобіганню заворушень, кримінальним правопорушенням; охороні здоров’я населення; захисту репутації або прав інших людей; запобіганню розголошенню інформації, одержаної конфіденційно; підтриманняю авторитету і неупередженості правосуддя?

2) чи можливо завдати істотної шкоди цим інтересам через розголошення такої інформації?

3) що переважає: шкода від оприлюднення такої інформації чи суспільний інтерес в її отриманні, що полягає в інтересах національної безпеки, економічного добробуту та прав людини? [97, ч. 2 ст. 6] Хоча сьогодні, як в законодавстві, так і в судовій практиці немає єдиних підходів до визначення «суспільного інтересу».

Загалом, В. А. Ліпкан та В. Ю. Баскаков ставлять під сумнів необхідність розмежування інформації з обмеженим доступом на три види, при цьому пропонують розглядати лише конфіденційну та таємну. Пояснюючи це тим, що зміст конфіденційної інформації може становити професійна, таємниця слідства тощо, яка не містить державної таємниці. Науковці пропонують визнавати конфіденційною «будь-яку інформацію з обмеженим доступом, що не має ознак державної таємниці, а таємною – будь-яку інформацію з обмеженим доступом, що має ознаки державної таємниці» [231, с. 96]. Такий підхід має своє раціональне зерно, оскільки як конфіденційна, так і службова інформація підлягає обмеженню в доступі самими суб'єктам, які нею володіють чи вона їх ідентифікує.

Варто зазначити про існування іншого підходу до розуміння конфіденційної та таємної інформації. А. І. Марущак до таємної інформації відносить різні види таємниць, у тому числі: державну, службову, професійну тощо. При цьому науковець зазначає, що визначення «конфіденційна інформація» у Законі України «Про інформацію» має недоліки: «до переліку суб'єктів права власності конфіденційної інформації не включено державу, яка також володіє відомостями конфіденційного характеру, а після слова «відомості» слід доповнити конструкцією «що не становлять передбаченої законом таємниці» [12, с. 24–25].

Загалом, «таємниця» тлумачиться як: те, що приховується від інших, відоме не всім; те, що не підлягає розголошенню; відомості, знання про щось, способи досягнення чого-небудь, невідомі іншим; прихована внутрішня сутність предмета, явища [43, с. 1426]. Але ж і конфіденційна інформація наділена аналогічними ознаками, що пов'язується з етимологією поняття «конфіденційний», який не підлягає розголосу; довірчий, таємний [235].

Розмежування інформації з обмеженим доступом повинно відбуватись із врахуванням того, чиї інтереси «потребують захисту у зв'язку із такою інформацією» [231, с. 100]: приватні (фізичної особи), колективні (службові, корпоративні, у зв'язку із забезпеченням виконання завдань органом влади) чи державні.

До переліку службової інформації у ДПСУ, крім іншої, належать відомості, які є персональними даними, або інформація про особу, зокрема:

відомості (дані, інформація), що містяться в автобіографіях, актах, анкетах, базах даних, особових справах, паспортах, посвідченнях, що створюються (обробляються) посадовими та службовими особами ДПСУ, розголошення яких може мати негативні наслідки у сфері державної безпеки [135, п. 58];

відомості про персональні дані учасників антитерористичної операції на сході України з числа військовослужбовців та/або працівників ДПСУ та/або відомості про персональні дані членів їхніх сімей [135, п. 65];

відомості, які містяться в послужному списку військовослужбовців ДПСУ (по заповненню за встановленою формою), розголошення яких може завдати шкоди законним інтересам і правам таких військовослужбовців ДПСУ [135, п. 66];

відомості про персональні дані: назва посади, прізвище, ім'я, по батькові, дата народження, адреса реєстрації та проживання співробітника оперативного підрозділу ДПСУ (за сукупністю усіх показників) [135, п. 78].

Такі дані ідентифікують особу й належать швидше до персональних даних, якими володіють відповідні посадові особи ДПСУ через їх повноваження (керівники та начальники підрозділів, представники кадрових підрозділів). Така інформація пов'язана у першу чергу із захистом персональних даних, а лише в другу чергу із діяльністю ДПСУ. Наприклад, інші дані, такі як характеристики, що створюються (обробляються) посадовими та службовими особами ДПСУ, є службовою документацією, але все рівно містять інформацією про фізичну особу із персональними даними про неї, за якою можна її ідентифікувати.

Відсутність чіткого правового закріплення службової інформації негативно відображається на практичній складовій. Так, опитування показало, що переважна більшість (70,6 %) респондентів ознайомлені з переліком службової інформації у сфері діяльності ДПСУ, але 29,4 % – «ні» **(додаток В)**.

Досить незрозумілими є терміни, що містяться в «Інструкції із захисту публічної інформації у Державній прикордонній службі України» затверджена наказом Адміністрації ДПСУ від 07.07.2011 р. № 501, зокрема «конфіденційна публічна інформація» (Розділ 2) і «службова публічна інформація» (Розділ 3). Таких термінологічних конструкцій не має у чинному законодавстві, тому ці поняття потребують узгодження та приведення у відповідність із чинним законодавством [236].

Отже, основні проблеми правового регулювання інформації з обмеженим доступом перебувають у нормативно-правовій площині, по-перше, це відсутність законодавчої дефініції «службова інформація»; по-друге, відсутність принципових вимог розмежування окремих її видів відповідно до суті (було наведено вище щодо конфіденційної інформації та службової, яка є по суті персональними даними); по-третє, наявність суб'єктивного фактору, при віднесенні інформації до службової. Можливо, варто поділяти інформацію з обмеженим доступом на конфіденційну (приватно-публічного характеру) та державну таємницю. При цьому створити законодавче підґрунтя та забезпечити належні гарантії захисту інформації, яка обмежена в доступі (конфіденційна) її володільцями, розпорядниками.

Правове регулювання державної таємниці є найбільш детально унормоване та контрольоване у порівняння з іншими видами інформації з обмеженим доступом, зокрема Законом України «Про державну таємницю» [237], постановою КМУ «Про затвердження порядку організації та за без-печення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях» [238], наказом СБУ «Про затвердження Зводу відомостей, що становлять державну таємницю» [239] тощо. Достатньо досліджена державна таємниця в наукових працях таких науковців як,

А. М. Благодарного [240], Ю. П. Мірошника [241], В. Ю. Баскакова [242], О. М. Сибіги [243] та інших. Сфера правового обігу інформації, що становить державну таємницю, у загальному урегульована та чітко визначена у законодавстві (поняття державної таємниці, перелік відомостей, що становлять державну таємницю, порядок та підстави надання допуску до державної таємниці тощо), а специфіка та проблемні питання стосовно цієї інформації (порядок обліку, обробки, збереження тощо) у діяльності ДПСУ не можуть бути розкриті у межах даного дослідження у зв'язку з обмеженим доступом такої інформації.

Говорячи про інформацію з обмеженим доступом, ми розуміємо, що така інформація підлягає захисту та врегулюванню набагато більше, ніж відкрита інформація, тому на законодавчий і компетентний нормотворчий орган покладається відповідальність щодо упорядкування, розмежування та встановлення чітких механізмів обігу та захисту такої інформації, які б забезпечували збереження та захист національних інтересів у сфері прикордонної інформаційної безпеки.

2.3 Організаційні засади інформаційних відносин в управлінні оперативно-службовою діяльністю Державної прикордонної служби України

Сьогодні інформація стала основним ціннісним орієнтиром у процесі управлінської діяльності органів державної влади. У сфері управління охороною державного кордону України вона має свої відмінності й особливості. Це пов'язано із характером завдань, що виконують структурні підрозділи ДПСУ усіх рівнів, у тому числі і тих, що безпосередньо охороняють державний кордон, – прикордонних загонів. Розвиток правоохоронної складової у напрямку забезпечення розвитку інтегрованого управління кордонами з урахуванням досвіду держав – членів ЄС обумовлює необхідність з'ясування та дослідження інформаційної складової процесу прийняття управлінських рішень в органах

охорони державного кордону (далі – ООДК) з урахуванням існуючих загроз прикордонній безпеці України.

Успішне управління у сфері охорони державного кордону спрямоване на досягнення високого рівня безпеки державних кордонів, невід'ємною складовою якої є застосування активних форм ведення бойових дій (службово-бойової діяльності) у межах ДПСУ. Найважливішою передумовою цього є своєчасне одержання достовірної інформації, її швидкий аналіз і чітке подання результатів. Це пов'язане із тим, що сучасне суспільство все більше набуває рис інформаційного суспільства, необхідною умовою життя в якому є розвиток інформаційно-аналітичної діяльності [244, с. 65]. Цілком справедливо підкреслює значення інформації в процесі управління В. Л. Грохольский, «однією з умов прийняття оптимальних управлінських рішень є забезпеченість суб'єктів управління необхідною інформацією. Інакше можна прийняти дефектне (хибне) рішення. До того ж поставлені завдання будуть вирішуватися іншим шляхом, з надмірною витратою сил і засобів, більшою витратою часу і ресурсів» [245, с. 12].

Новітні процеси розвитку інформаційної діяльності як невід'ємна складова управлінської діяльності привернули увагу багатьох науковців із різних сфер наукових знань. Варто відзначити дослідження, проведені у напрямку інформаційно-правових аспектів управлінської діяльності, а саме: В. Б. Авер'яновим, І. В. Арістовою, О. М. Бандурком, Р. А. Калюжним, О. В. Копаном, А. І. Марущаком, О. Г. Марценюком, О. М. Селезньовою, І. М. Сопілко, О. О. Тихомировим, М. Я. Швецом та багатьма іншими. Питання інформаційної складової прийняття рішень у різних сферах державного управління розглянуті у працях: О. В. Ананьєва, О. М. Белейя, В. Л. Грохольського, В. В. Єжунінова, О. Г. Комісаровим, О. М. Олійниченко тощо. Окремі напрямки забезпечення інформаційної складової у сфері охорони державного кордону розглянуті: В. Л. Зьолкою, І. С. Катеринчуком, В. А. Кириленком, М. О. Корольом, Р. М. Ляшуком та іншими науковцями. Проаналізовані праці дозволили окреслити не вирішені раніше наукові завдання з приводу дослідження інформаційної складової у процесі управлінської діяльності

начальників прикордонних загонів щодо формування рішень з питань охорони державного кордону України, що відіграють вагоме значення в організації ОСД.

Основним об'єктом інформаційної складової підготовки та прийняття управлінських рішень у сфері охорони державного кордону є інформація як правова категорія, що має широке значення у всіх сферах життєдіяльності та функціонування органів публічної влади. Л. Ю. Вдовиченко підкреслює, що саме в публічній сфері формується відповідна система інформаційних врегульованих національними правовими нормами відносин, коли будь-який суб'єкт має право отримувати інформацію відповідного характеру, а другий суб'єкт зобов'язаний передати певний вид інформації [246, с. 10]. Отже, варто зазначити, що в контексті нашого дослідження інформація, окрім власно інформативної функції, виконує ще одну важливу функцію – інструментальну – участь в організації та управлінні охороною державного кордону [247].

Опрацювання та сприйняття великого обсягу інформації обумовлено нормативно закріпленими обов'язками начальника ООДК: завжди мати точні відомості про особовий склад, озброєння, боєприпаси, бойову та іншу техніку, пальне, матеріальні засоби (кошти), що є у військовій частині, на кораблі (у підрозділі) за штатом, списком і в наявності [248, ст. 59]; знати потреби і запити особового складу, приймати рішення за його заявами, скаргами та іншими зверненнями [248, ст. 59]; знати правову базу діяльності ДПСУ [100, п. 5.1. Р. 3]; своєчасно приймати рішення, ставити завдання підлеглим та вимагати їх неухильного виконання [100, п. 5.3. Р. 3]; знати можливості та забезпеченість підрозділів, спрямовуючи їх зусилля на виконання поставлених завдань [100, п. 5.4. Р. 3], тощо. У попередній редакції Положення про ООДК ДПСУ [44] у п. 9.1 було визначено що начальник ООДК повинен знати «обстановку, стан охорони державного кордону на ділянці відповідальності» [249]. Ми вважаємо, що володіння обстановкою є важливою інформацією, що впливає на прийняття рішень та управління ООДК. Тому таку норму необхідно внести до редакції згаданого вище чинного Положення від 30.11.2018 р. № 971 [100].

Інформаційна складова управлінської діяльності начальника прикордонного загону втілюється та набуває практичних форм через його інформаційну діяльність, основними видами якої згідно із Законом України «Про інформацію» є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації [57, ст. 9].

О. М. Шинакрук, Л. М. Артюшин, В. А. Кириленко та І. І. Стоянов пов'язують початок процесу прийняття рішення на охорону державного кордону із виявлення суперечностей (проблеми), вибору мети рішення, визначення завдань щодо усунення попередження даної проблеми [250, с. 333]. Авторський колектив науковців пропонує розглядати процес вирішення основних інформаційних завдань у процесі формування рішень у вигляді окремих послідовних елементів, а саме: збір інформації щодо можливих загроз; виявлення (прогноз) і визначення причин виникнення загроз у конкретній ситуації; формування мети рішення, спрямованого на протидію загрозі; обґрунтовування рішення, спрямованого на протидію загрозі; визначення вимог до рішення; розробка кращого варіанта; корегування та узгодження рішення; реалізація рішення [250, с. 334–335]. У разі виникнення реальної загрози рішення готується завчасно, варіанти дій згідно з таким рішенням доводяться до оперативно-чергової служби ДПСУ [250, с. 334].

Одним із принципів діяльності ДПСУ, що визначено в Законі України «Про Державну прикордонну службу України», є «єдиноначальність та колегіальність при розробці важливих рішень» [79, ст. 3]. На підставі аналізу положень постанови КМУ «Про Адміністрацію ДПСУ» та наказу ДПСУ «Про ООДК ДПСУ» можна визначити, що принцип колегіальності реалізується у межах діяльності Адміністрації ДПСУ. Це відображено у п. 12 Положення про Адміністрацію ДПСУ «для погодженого вирішення питань, що належать до компетенції Адміністрації ДПСУ, обговорення найважливіших напрямів її діяльності в Адміністрації ДПСУ може утворюватися колегія» [159]. Щодо ООДК, то нормативно закріплено, що їх начальники зобов'язані своєчасно приймати рішення, визначати завдання підлеглим і вимагати їх неухильного виконання (зокрема у частині прийнятого рішення, його правильного

застосування підпорядкованими підрозділами (підлеглими) та успішне виконання ними поставлених завдань) [100, п. 5.3. P. 3]. Отже, нормативне закріплення принципу колегіальності стосується тільки Адміністрації ДПСУ шляхом утворення колегії, і лише як право, а не як обов'язок.

Тому, вважаємо слушною думку Р. М. Ляшука, який пропонує використовувати принцип щодо прийняття управлінського рішення у такому формулюванні «єдиноначальність, централізація управління з делегуванням повноважень щодо самостійного вибору способів виконання поставлених завдань» [31, с. 41]. У зв'язку із цим на посадових осіб ДПСУ, уповноважених приймати управлінські рішення, покладається відповідальність за прийняті рішення у сфері охорони державного кордону та під час вирішення поточних організаційних питань на ділянці відповідальності. Відповідальність за прийняті рішення є необхідним елементом функціонування державно-владного апарату. Такий підхід характерний для всіх цивілізованих країн, що зокрема, зазначає Bohumil Pikna: «держави-члени ЄС перш за все відповідальні за управління своїми ділянками на зовнішніх кордонах» [251, с. 76].

Незалежно від закріпленого принципу єдиноначальності у прийнятті управлінського рішення начальником прикордонного загону, його особистої відповідальності за них переважну більшість необхідної інформації він отримує від підлеглих. Таку інформацію начальник ООДК отримує під час доповідей від підлеглих керівників структурних підрозділів про обстановку, результати оперативно-службової діяльності, у зведених даних за добу, у разі ускладнення обстановки, з інформаційних та звітних документів тощо. У зв'язку із цим якість прийнятого рішення та ефективність його реалізації залежить від актуальності (оперативності), вірогідності, об'єктивності, повнити й адекватності інформації, отриманої начальником ООДК [252, с. 101]. Тому підлеглі, які забезпечують начальника інформацією для подальшого прийняття управлінського рішення також повинні відповідати в разі порушення її властивостей. Така відповідальність можлива в межах загальної дисциплінарної практики. Крім того, у випадках, передбачених Кримінальним кодексом України (далі – КК України)

настає кримінальна відповідальність у разі: складання, видачі службовою особою завідомо неправдивих офіційних документів, внесення до офіційних документів завідомо неправдивих відомостей, інше підроблення офіційних документів [253, с. 366]; несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї [253, с. 362]; невиконання або неналежне виконання службовою особою своїх службових обов'язків через несумлінне ставлення до них, що завдало істотної шкоди охоронюваним законом правам, свободам та інтересам окремих громадян, державним чи громадським інтересам або інтересам окремих юридичних осіб [253, с. 367].

Окремих статей у КК України з інформаційних злочинів не передбачено, відповідальність за порушення правил інформаційної діяльності містяться у складах інших злочинів. Загалом кримінальна відповідальність настає за вчинення суспільно небезпечних діянь, а в повсякденній діяльності виникає багато інформаційних завдань, які не пов'язані зі злочинами. Разом з тим розвиток інформаційного суспільства обумовлює конкретизацію інформаційних правопорушень. Так, зокрема у Митному кодексі України передбачена відповідальність за порушення порядку надання інформації, «посадові особи органів доходів і зборів несуть відповідальність, передбачену законом за надання недостовірної інформації, а також за неправомірну відмову у наданні відповідної інформації, несвоєчасне надання інформації та інші правопорушення у сфері інформаційних відносин» [254, ст. 22]. Вважаємо за доцільне включити аналогічні норми до Закону України «Про Державну прикордонну службу України».

У ході проведеного анкетування на запитання «Хто несе персональну відповідальність за організацію створення, збирання, одержання, зберігання, використання, поширення, охорону та захист інформації в діяльності ДПСУ?» відповіли «персонально кожен військовослужбовець ДПСУ» 54,6 % респондентів, «компетентні посадові особи» 22,1 %, «командири органів та підрозділів ДПСУ»

20,3 % і 3 % МВС України. На запитання «Хто, на Вашу думку, несе персональну відповідальність за ненадання чи розповсюдження персональних даних, службової інформації?» кожен військовослужбовець 65,8 %, 18,6 % компетентні посадові особи і 15,6 % командири підрозділів **(додаток В)**. Отже, важливо розрізняти, що відповідальність за організацію діяльності несе командир підрозділу, а за розповсюдження персональних даних, службової інформації, яка стала відома у зв'язку із виконанням службового обов'язку – персонально кожний військовослужбовець.

У процесі прийняття управлінського рішення у сфері охорони державного кордону інформація здійснює кругообіг, тільки змінюється її зміст, кількість та якість. Сукупність відомостей надходять до начальника прикордонного загону про обстановку чи окремі факти, події. Начальник може запросити уточнюючу інформацію. Так, для постановки конкретних завдань збирається більш детальна інформація, ніж на ранніх етапах: про правову сторону питання; оперативні підрозділи; відомий досвід, склад своїх сил і засобів; сили, засоби і можливу тактику дій противника тощо [250, с. 336]. У подальшому сукупність інформації узагальнюється та обробляється, на підставі цього приймається рішення, що доводиться до відповідальних посадових осіб, у вигляді керівництва до подальших дій. У конкретній ситуації проблема прийняття рішень полягає у виборі тільки одного рішення з множини можливих за визначеним критерієм [255, с. 43].

Для означення «сукупності циркулюючих відомостей, необхідних для підготовки, прийняття та контролю реалізації управлінського рішення», О. М. Олійниченко використовує поняття «інформаційні потоки». У зв'язку із цим зазначає, що такі відомості можуть існувати у вигляді усних повідомлень і паперових або електронних документів, які на практиці формуються у систему усного інформування (у формі доповідей, засідань, нарад, бесід з підлеглими, консультантами тощо), систему паперового документообігу та комп'ютеризовану (автоматизовану) інформаційну систему відповідно [256]. Інформаційні потоки здійснюються за допомогою основних видів інформаційних технологій: усної,

письмової та комп'ютеризованої (тобто комп'ютерної та телекомунікаційної технологій). Як правило, комп'ютерні інформаційні системи частково замінюють або дублюють усну та паперову систему інформування [256].

О. Г. Комісаров для початкового етапу інформаційного супроводження службово-бойової діяльності керівником підрозділу використовує поняття «моніторинг інформаційного простору» [257, с. 73], а сама службова діяльність має здійснюватись на підставах «інформаційної насиченості» [257, с. 71].

Первинними мотивуючими відомостями процесу прийняття рішення начальником ООДК є завдання, яке необхідно вирішити. Як стверджують А. Ф. Мельник, О. Ю. Оболенський та А. Ю. Васіна, «управління завжди здійснюється з метою досягнення певних цілей, а реалізація цілей будь-якого організаційного формування забезпечується шляхом прийняття і виконання численних рішень» [258, с. 157]. Мета прийняття управлінського рішення обумовлює інформаційні потреби, які зумовлюють появу інформаційних бажань (тобто прагнення отримати потрібну інформацію) та визначають інформаційні ресурси, що необхідні для досягнення мети прийнятого управлінського рішення. Інформаційні бажання реалізуються в інформаційні запити, які формують вимоги до інформаційних потоків, що, певною мірою, сприяють задоволенню інформаційних потреб начальника ООДК [256].

Інформаційна складова щодо реалізації завдань в ООДК формується на підставі конкретних повідомлень, які отримує начальник із таких джерел, які містяться: в законах України, підзаконних нормативно-правових актах, які врегульовують загальну діяльність ДПСУ і окремих її підрозділів, а також у керівних документах ДПСУ (інформаційно-нормативна складова); загальних або конкретних вказівок, уточнень обстановки, дій, які надходять від керівництва ДПСУ (інформаційно-управлінська складова); надходить по лінії оперативно-чергової служби від підрозділів прикордонного загону, взаємодіючих правоохоронних органів або місцевих органів публічної влади (оперативно-інформаційна складова); дані, опрацьовані в результаті діяльності інформаційно-аналітичних підрозділів (інформаційно-аналітична складова); обстановки

(ситуації), яка склалась у підрозділах прикордонного загону (інформаційно-практична складова); за результатами проведення оперативно-розшукової діяльності відповідними підрозділами ДПСУ (оперативно-розшукова інформаційна складова); у результаті роботи зі зверненнями громадян (інформаційно-консультативного характеру).

Отримавши інформацію щодо конкретної ситуації на державному кордоні чи у підпорядкованому підрозділі з одного або декількох джерел, начальнику ООДК необхідно її проаналізувати та відфільтрувати для формування управлінського рішення. В. Л. Грохольський пропонує в управлінській діяльності використовувати різні джерела інформації: гласні і негласні; інформацію інших служб, підпорядкованих підрозділів, інших правоохоронних і контролюючих органів [245, с. 12], що є цілком виправдане. На цьому етапі начальник буде керуватись як зовнішніми, так і внутрішніми інформаційними факторами. Зовнішні – це ті уявлення, які склались на підставі отриманих даних із різних джерел. Внутрішні – це інтелектуальна складова, яка притаманна начальнику як конкретній особистості. Зміст такої внутрішньої інформаційної складової особистості наповнює інформація із загального розвитку; здобутої вищої освіти; практичного досвіду; знання та уміння керуватись нормативно-правовими актами, керівними документами; уміння вирішувати поставлені завдання вищим начальником; обстановка у підрозділах; знання про підлеглих; постійне володіння оперативною обстановкою; усвідомлення інформації у результаті інформаційно-аналітичної діяльності підлеглих; кримінальний аналіз тощо.

У практиці управління досить часто виникає проблема недостатності інформації у зв’язку з тим, що не всі відомості, які входять до системи, корисні, подані в потрібному вигляді та відповідають поставленим цілям. У зв’язку з цим постає проблема високої вірогідності інформації, без якої неможливо організувати ефективну роботу суб’єкта управління [252, с. 103].

Важливим елементом системи управління є своєчасність надходження інформації. Від цього значною мірою залежить якість управлінських рішень. Часто затримка інформації призводить до втрати її актуальності, а згодом – і до

прийняття на основі застарілої інформації управлінських рішень, що призведуть до небажаних наслідків [244, с. 65].

Сучасна управлінська діяльність підтримується інформацією, яка відображається на матеріальних носіях та передається по каналах зв'язку. Для підвищення достовірності ведеться обробка лише оформленої інформації. Постійне удосконалення управління та збільшення обсягу процесів у прикордонній сфері супроводжується збільшенням супутніх інформаційних потоків. Інформаційні бази даних повинні містити весь комплекс показників, які характеризують діяльність у сфері охорони державного кордону загалом і її окремих складових, а також матеріал про всі фактори, які впливають на стан і тенденції в даній сфері. При формуванні бази даних вирішуються питання про систему збереження і обновлення даних, а також обґрунтовується пов'язаність даних, їх взаємна узгодженість, можливість проведення порівняння і співставлення оцінок даних, що зберігаються в банку даних. Бази даних безперервно обновлюються з урахуванням вимог основних користувачів банку даних і є основою для прийняття певних рішень [259, с. 83].

Особливої актуальності сьогодення є забезпечення управління інформацією у сфері охорони державного кордону в умовах кризових ситуаціях воєнного характеру. О. Г. Комісаров і О. Л. Хитра зазначають, що визначення ситуації кризовою перебуває у залежності повноважень відповідного суб'єкта у забезпеченні «національних інтересів» та умов його діяльності відносно впливу «небезпечних чинників» [260, с. 108]. Отже, умови управління інформацією у таких кризових ситуації детермінує співвідношення цих чинників: повноваження ДПСУ, забезпечення національних інтересів у сфері відповідальності, умови обстановки та характер загрозливих факторів на державному кордоні (чи поблизу нього).

Інформаційна складова процесу прийняття управлінських рішень визначається множиною управлінських дій, множиною станів середовища (зареєстрованих ситуацій) і значеннями показників ефективності, що включаються у визначення оціночного функціоналу при проведенні розрахунків

зі знаходження оптимального рішення за вибраним критерієм прийняття рішень [255, с. 43].

Отже, достовірна й актуальна інформація є основою правильного та своєчасного рішення у сфері охорони державного кордону України та впливає на прикордонну безпеку держави. Сьогодні це досить актуально для української держави. Інформаційна складова підготовки та прийняття управлінського рішення в охороні державного кордону містить багато компонентів (інформаційну діяльність, інформаційно-аналітичну діяльність, інформаційні завдання, інформаційні потреб людини й держави у прикордонній сфері, актуальні бази даних, зовнішні та внутрішні інформаційні фактори начальника прикордонного підрозділу тощо), які необхідно вміло враховувати та поєднувати начальникам прикордонних підрозділів. Розвиток інформаційних відносин обумовлює застосування в управлінській діяльності нових інформаційних технологій, інформаційно-аналітичного забезпечення як одних із найважливіших засобів удосконалення управління у сфері охорони державних кордонів. Такі заходи дозволяють втілювати положення Стратегії розвитку ДПСУ в частині здійснення модернізації системи управління шляхом упровадження сучасних інформаційних технологій у систему управління.

2.4 Інформаційна взаємодія в діяльності Державної прикордонної служби України

Надійна охорона державного кордону як невід'ємний елемент національної безпеки неможлива без взаємодії ДПСУ з іншими правоохоронними органами України та суміжних держав. Безперечно кожний із цих органів відповідає за виконання завдань у визначеній конкретній сфері, але разом з тим їх діяльність неможлива без злагодженої співпраці у міжвідомчих питаннях, крім того, без надання взаємодопомоги й взаємопідтримки. Саме ці зв'язки дозволяють гармонійно та належним чином функціонувати державно-правовому механізму й

утворюють цілісність не тільки держави, але й усього українського суспільства, забезпечують підтримання законності та правопорядку, збереження територіальної цілісності й недоторканності державних кордонів. Така взаємодія стає можливою за умови, перш за все, обміну інформацією між компетентними органами, у тому числі у сфері охорони державного кордону. Інформаційна взаємодія закладає основи для спільної діяльності та покращання ефективності в охороні державного кордону України. Разом з тим Закон України «Про інформацію» такий вид інформаційної діяльності, як обмін інформацією безпосередньо не визначає [57, ст. 9], але фактично він здійснюється у межах охорони державного кордону. Обмін інформацією як сутнісне відображення інформаційної взаємодії є все ж таки окремим напрямком інформаційної діяльності, яка у сучасних умовах функціонування інформаційного суспільства та розвитку системи прикордонної безпеки потребує окремого наукового аналізу та визначає актуальність тематики цього підрозділу.

Інформаційна взаємодія у загальнотеоретичному ракурсі сьогодні не набула широкого наукового розгляду й обґрунтування. Разом з тим, теоретичний аналіз та висновки стали можливими завдяки напрацюванням В. М. Дубняка, І. М. Забари, Р. А. Калюжного, О. П. Клементьєва, І. Л. Олійника та інших. Варто зазначити, що особливості інформаційної взаємодії у діяльності ДПСУ до сьогодні комплексно не були проаналізовані. Тому метою даного підрозділу є визначення правової природи, сучасного стану та напрямків інформаційної взаємодії у діяльності ДПСУ.

Звертаючись до етимології категорії «інформаційна взаємодія» можна визначити, що інформаційний – це пов’язаний з інформацією у різних її виявах та процесах відповідно до Закону України «Про інформацію», як об’єкт інформаційних відносин. Інформація у контексті дослідження є базовим виміром, який закладає підґрунтя (інформаційну основу) для спільних дій, процесів, явищ, подій, фактів у напрямку безпеки державних кордонів з іншими міжнародними (у межах міжнародного співробітництва) та національними (у межах інтегрованого управління кордонами) компетентними інституціями у прикордонній сфері.

Взаємодія передбачає взаємозв'язок, спільність, погодженість і взаємовплив суб'єктів, що перебувають у рівноправних партнерських відносинах та пов'язані окремою сферою правових відносин – прикордонною безпекою [261, с. 96].

У законодавстві термін «інформаційна взаємодія» нормативно закріплено лише у рішенні Національної комісії з цінних паперів та фондового ринку від 22 листопада 2012 р. № 1688, яким затверджено «Положення про функціонування фондових бірж», де інформаційна взаємодія – це обмін інформацією між фондовими біржами, яка ними узгоджена за складом, формою та структурою даних, періодичністю формування та передач [262, п. 2. Р. 1]. Отже, інформаційна взаємодія ототожнюється з обміном інформацією, який нормативно закріплений як «автоматизований процес прийому і передачі інформації, якою компетентні органи … обмінюються для» досягнення конкретної мети [263, ст. 1].

У постанові «Про затвердження Вимог до організації роботи з оформлення віз для в'їзду в Україну і транзитного проїзду через її територію», яка затверджена наказом Міністерства закордонних справ України (далі – МЗС України), МВС України та СБ України від 30 жовтня 2017 р. № 469/897/605 закріплено, що «інформаційна взаємодія» передбачає:

отримання уповноваженим органом від компетентних органів інформації про осіб, яким заборонено в'їзд в Україну;

погодження з компетентними органами оформлення віз іноземцям, які є громадянами держав згідно з переліком держав, оформлення віз громадянам та ОБГ, які постійно проживають у зазначених державах, здійснюється закордонною дипломатичною установою України в державі тимчасового або постійного проживання заявників після проведення особистої співбесіди з іноземцем або ОБГ;

надання уповноваженим органом інформації про оформлені візи компетентним органам та Службі зовнішньої розвідки України (далі – СЗР України) шляхом направлення повідомлення щодо відомостей про іноземців та осіб без громадянства, яким оформлено візи для в'їзду в Україну [264]. Отже, проаналізовані положення здійснення інформаційної взаємодії дають нам

можливість узагальнити, що її утворюють такі елементи, як отримання та надання інформації, а також узгодження окремих питань.

О. П. Клементьєв розглядає інформаційну взаємодію як відносини суб'єктів інформаційних правовідносин, оскільки вони беруть безпосередню участь у формуванні інформаційного суспільства у межах своїх повноважень, які стосуються інформації, оскільки вона є єдиним об'єктом даного виду відносин [265, с. 156].

Інформаційна взаємодія являє собою інформаційну діяльність усіх взаємодіючих суб'єктів, результатом якої є інформація (інформаційні продукти, документи, дані тощо), що здатна задовольнити інформаційні потреби будь-якого суб'єкта, який є учасником процесу прийняття рішень [266, с. 174]. Інформаційна взаємодія має цілеспрямований характер, орієнтована на обмін інформацією щодо своєчасного виявлення, попередження та недопущення порушення прикордонного законодавства та забезпечення недоторканності державного кордону. Обмін інформацією здійснюється з урахуванням інформаційних потреб і інформаційних інтересів, що є окремим напрямком спільної діяльності правоохоронних органів в забезпеченні прикордонної безпеки.

І. Л. Олійник зазначає, що взаємодія, застосована на нормативних актах, являє собою взаємозалежну, погоджену за місцем і часом діяльність декількох її суб'єктів, спрямовану на виконання загального завдання зміцнення законності та правопорядку у боротьбі зі злочинністю; обмін результатами діяльності, у процесі якої важливо не тільки здійснити обмін інформацією, а й організувати обмін діями, спланувати загальну діяльність [267, с. 10]. Отже, інформаційна взаємодія – це не лише фактична передача відповідних даних, але й організація та здійснення інформаційного процесу. Проте ключова роль відводиться саме обміну інформацією, який може відбуватись усно (в телефонному режимі), письмово, електронно. За змістом це може бути: передача інформації в інтересах відомства, узгодження спільних дій, обмін результатами діяльності, внесення інформації у банки даних тощо [268, с. 186].

Юридичною підставою інформаційної взаємодії у сфері охорони державного кордону є передбаченість її правовими нормами. Так, у Законі України «Про Державну прикордонну службу України» серед повноважень ДПСУ визначено здійснювати: автоматизований обмін інформацією про транспортні засоби, що перетнули державний кордон України, з територіальними органами МВС України [79, п. 19 ст. 20]; одержувати навігаційну, метеорологічну, гідрографічну та іншу інформацію, необхідну для забезпечення польотів і кораблеводіння [79, п. 20 ст. 20] тощо.

Стратегією розвитку ДПСУ встановлено, що у напрямку розвитку інформаційної складової системи охорони державного кордону планується здійснити удосконалення системи аналізу й оцінки інформації, а також модернізацію системи зв'язку, інформатизації та захисту інформації за такими напрямками:

під час організації спільної оперативної охорони державного кордону з державами – членами ЄС, що мають спільний кордон з Україною, а також з Республікою Молдова передбачається: впровадити механізм обміну інформацією та проведення спільного аналізу ризиків;

для поглиблення співробітництва з прикордонною службою Республіки Білорусь передбачається розширити формат обміну інформацією та співробітництва оперативних органів;

забезпечити удосконалення існуючих механізмів обміну відкритою статистичною і аналітичною інформацією між суб'єктами інтегрованого управління кордонами та прикордонними органами держав – членів ЄС, а також міжнародними організаціями та установами;

модернізувати інтегровану міжвідомчу інформаційно-телекомунікаційну систему «Аркан» щодо контролю осіб, транспортних засобів і вантажів, які перетинають державний кордон;

забезпечити створення дієвого механізму оперативного співробітництва з правоохоронними органами на національному та міжнародному рівні, зокрема у сфері обміну інформацією, проведення спільних оперативних заходів [59].

Передбачені у Стратегії заходи підкреслюють важливість і необхідність функціонування сучасної прикордонної охорони у безперервному та невід'ємному зв'язку з інформаційною взаємодією як на міжнародному, так і на внутрішньодержавному рівнях. Втілення визначених конкретних кроків щодо інформаційної взаємодії сприятиме ефективній діяльності ДПСУ, розвитку та посиленню прикордонної безпеки України [261, с. 98].

Стратегія ІУК передбачає сучасну модель ефективного управління кордонами – інтегроване управління кордонами, яка є скоординованою діяльністю компетентних державних органів України та військових формувань, спрямована на створення та підтримання балансу між забезпеченням належного рівня прикордонної безпеки і збереженням відкритості державного кордону для законного транскордонного співробітництва, а також для осіб, які подорожують [58].

Стратегія ІУК орієнтована на підвищення ефективності реалізації державної політики у сфері безпеки державного кордону, належної його захищеності, запровадження європейських стандартів інтегрованого управління кордонами, невід'ємним елементом якої є обмін інформацією між суб'єктами інтегрованого управління кордонами (МВС України, МЗС України, Мінінфраструктури, МФ України, ДПСУ, Державна міграційна служба України (далі – ДМС України), Державна митна служба України (далі – ДМСУ), СБ України, Національна поліція, Національна гвардія, Державна служба України з питань безпечності харчових продуктів та захисту споживачів, Збройні Сили України (далі – ЗС України).

У Стратегії ІУК конкретизовано основні вектори розвитку інформаційної взаємодії за такими спрямуваннями, як [58]:

опрацювання регламентів взаємодії між інформаційними ресурсами суб'єктів інтегрованого управління кордонами;

проведення нормативного врегулювання відповідних процедур і механізму взаємного доступу до інформаційних систем;

проведення нормативного врегулювання питань інформаційного обміну, порядку отримання та обробки персональних даних та їх захисту;

забезпечення розвитку механізмів обміну інформацією про товари з митними службами суміжних держав;

забезпечення розвитку центрів збору й обробки інформації;

розроблення та своєчасне уточнення планів взаємодії;

забезпечення оперативного обміну інформацією;

поширення співпраці з Європейським агентством прикордонної та берегової охорони – FRONTEX (далі – FRONTEX) під час проведення операцій та обміну інформацією;

забезпечення інформаційно-аналітичної підтримки прийняття управлінських рішень щодо визначення наявних (потенційно можливих) ризиків і превентивного реагування на вияви транскордонної протиправної діяльності на державному кордоні, зокрема шляхом профілювання ризиків в умовах обмежених ресурсів і можливостей проведення заходів із забезпечення діяльності міжвідомчих аналітичних центрів та удосконалення механізму обміну інформацією та її використання з метою припинення протиправної діяльності;

розроблення інтегрованої системи автоматизованого управління кордонами та міграційними процесами й інтегрованої системи біометричної інформації про особу, її ідентифікації та верифікації як функціональних підсистем єдиної інформаційної системи МВС України;

організація обміну даними з правоохоронними органами;

запровадження інформаційного обміну між суб’єктами інтегрованого управління кордонами щодо ідентифікації незаконних мігрантів;

розширення мережі та вдосконалення роботи спільних контактних пунктів;

забезпечення роботи програмно-аналітичних модулів обробки інформації, запровадження системи попередньої інформації про пасажирів (APIS та PNR);

надання відповідного доступу до відомчих баз даних;

забезпечення спільного використання спроможностей, розвиток електронної інформаційної взаємодії;

модернізація інтегрованої міжвідомчої інформаційно-телекомунікаційної системи «Аркан» та відомчих ІТ-систем;

запровадження сучасних програмно-апаратних комплексів захисту інформації;

забезпечення інтероперабельності систем та опрацювання регламентів взаємодії з метою надання доступу до ресурсів в межах повноважень суб'єктів інтегрованого управління кордонами [58].

На міжвідомчому рівні обмін даними здійснюється контактними підрозділами через Віртуальний контактний аналітичний центр [270]. Основними формами діяльності аналітичного центру є: робочі засідання представників Сторін з питань, що належать до компетенції аналітичного центру; проведення спільних аналітичних досліджень у сфері безпеки державного кордону; підготовка робочих документів, проектів спільних планів, актів тощо за результатами виконання основних завдань [270, п. 4]. За результатами діяльності координатор аналітичного центру щороку забезпечує видання інформаційного бюлетеня [270, п. 6]. Передбачено, що електронна версія інформаційного бюлетеня розміщується на офіційному веб-порталі МВС України [269, п. 6].

На засіданнях Віртуального контактного аналітичного центру суб'єкти інтегрованого управління кордонами вирішують глобальні та загальні питання, наприклад Адміністрацією ДПСУ за участю експертів Консультативної Місії ЄС в Україні (EUAM) розглядаються питання організації розробки Стратегії ІУК та діяльності міжвідомчої робочої групи з питань координації інтегрованого управління кордонами, обговорюється стан виконання Плану заходів щодо реалізації інтегрованого управління кордонами у поточному році та розглядаються пропозицій щодо подальшої міжвідомчої співпраці у наступному році [270].

Інформаційна взаємодія може відбуватись з урахуванням окремої предметної сфери, зокрема – протидії нелегальній міграції. Так, з метою забезпечення нормативно-правового врегулювання процедури обміну статистичною та аналітичною інформацією, організації інформаційно-

аналітичного забезпечення з питань протидії нелегальній міграції МВС України, МЗС України, Міністерством соціальної політики України (далі – Мінсоцполітики), Міністерство освіти і науки України (далі – МОН України), СЗР України, СБ України була розроблена та прийнята Методика аналізу ризиків з метою протидії нелегальній міграції [271] **(додаток Д).**

Існує низка протоколів, підписаних Адміністрацією ДПСУ з прикордонними службами суміжних держав, спрямованих на розвиток міжнародної інформаційної взаємодії, зокрема:

протокол між Адміністрацією ДПСУ і Департаментом Прикордонної поліції Міністерства внутрішніх справ Республіки Молдова про обмін статистичною та аналітичною інформацією від 20 листопада 2014 р. (забезпечує координацію заходів, що вживаються ДПСУ та Департаментом Прикордонної поліції Міністерства внутрішніх справ Республіки Молдова на українсько-молдовському державному кордоні щодо запобігання незаконному переміщенню через державний кордон осіб, транспортних засобів, вантажів та іншого майна, а також вирішення інших питань, що належать до їх компетенції. Для досягнення цього домовилися про здійснення обміну статистичною та аналітичною інформацією про ситуацію на державному кордоні та прогнози її розвитку, а також про основні результати службової діяльності ДПСУ і Департаменту Прикордонної поліції Міністерства внутрішніх справ Республіки Молдова згідно з Переліком відомостей, за якими здійснюється взаємний обіг інформацією) [272];

протокол між Адміністрацією ДПСУ і Державним прикордонним комітетом Республіки Білорусь про порядок обміну інформацією про обстановку на державних кордонах України і Республіки Білорусь, підписаний 18 червня 2013 р. (спрямований на координацію зусиль органів охорони державного кордону ДПСУ та органів прикордонної служби Республіки Білорусь з протидії незаконному переміщенню через українсько-білоруський державний кордон осіб, транспортних засобів, вантажів та іншого майна, а також вирішення інших питань, що належать до їх компетенції, домовилися про здійснення обміну інформацією про обстановку на державному кордоні та прогнози її розвитку, а також основні

підсумки ОСД ООДК ДПСУ та органів прикордонної служби Республіки Білорусь відповідно до Переліку відомостей, за якими здійснюється взаємний обіг інформацією) [273];

протокол між Адміністрацією ДПСУ та Державним прикордонним комітетом Республіки Білорусь про пілотний контактний пункт «Житомир – Пінськ» від 14 грудня 2016 р. (спрямований на розвиток співробітництва та взаємного сприяння забезпеченню безпеки українсько-білоруського державного кордону; співробітництва у сфері інтегрованого управління кордонами; вдосконалення процесу обміну інформацією і протидії проявам транскордонної організованої злочинності, підтримки громадської безпеки та порядку у прикордонній зоні) [274].

Для організації та підтримання взаємодії і співробітництва з прикордонних питань, а також обміну інформацією під час узгоджених спільних заходів в інтересах протидії протиправній діяльності на державному кордоні України із суміжними державами створені структурні підрозділи органів охорони державного кордону ДПСУ, – Консультаційні пункти ДПСУ (далі – КП ДПСУ) [275].

Консультаційні пункти забезпечують обмін інформацією з конкретних питань:

про зміни в законодавстві з прикордонних питань;

виникнення надзвичайних ситуацій у пунктах пропуску через державний кордон та на під'їзних шляхах до нього;

обстановку, що може вплинути на проведення прикордонного, митного та інших видів контролю в пунктах пропуску через державний кордон;

осіб, яким відмовлено у в'їзді, та причини відмови;

порушення або спроби порушення законодавства під час перетинання державного кордону;

протидію злочинам, пов'язаним з торгівлею людьми та незаконною міграцією;

припинення злочинів, пов’язаних з контрабандою, у тому числі незаконним переміщенням через державний кордон зброї та її складових частин, вибухових пристроїв, боєприпасів, вибухових і радіоактивних речовин, наркотичних засобів, психотропних речовин і прекурсорів;

зразки документів, що використовуються для здійснення протиправної діяльності на державному кордоні;

протидію незаконному переміщенню викраденого автотранспорту через державний кордон;

транспортні засоби, що перетинають державний кордон, та вантажі, які переміщуються через нього;

законність в’їзду громадянина третьої країни або особи без громадянства на територію України чи суміжної держави;

запити та пропозиції з охорони державного кордону, які виникають за підсумками спільного патрулювання [275, п. 2].

Повний перелік відкритої, публічної і конфіденційної інформації, обмін якою здійснюється через КП ДПСУ, визначається міжнародними договорами. Відповідно до покладених завдань КП ДПСУздійснює обмін інформацією у письмовий формі, а в екстрених випадках усно з подальшим письмовим її підтвердженням протягом 24 годин після отримання запиту [275, п. 2].

Запити на інформацію і відповіді на них в обов’язковому порядку реєструються в журналі обліку запитів та інформації КП ДПСУ. У наданні інформації може бути відмовлено повністю або частково, якщо це може завдати шкоди інтересам України. Відмова повинна бути обґрунтованою та надісланою в письмовій формі. Обмін секретною інформацією та інформацією, яка в установленому порядку віднесена до службової, – забороняється [275, п. 2].

Питання інформаційної взаємодії у сфері прикордонної безпеки урегульовані й на рівні національного законодавства та стосуються взаємодіючих органів публічної адміністрації, повноваження яких стосуються прикордонної сфери. Обмін інформацією може здійснюватися на рівні окремих органів і підрозділів ДПСУ з територіальними органами публічної адміністрації з питань,

які визначаються у процесі підготовки планів взаємодії зазначених органів або уточнення цих планів [276, с. 108]. Такий порядок установлений постановою КМУ «Про затвердження порядку здійснення координації діяльності органів виконавчої влади та органів місцевого самоврядування з питань додержання режимів на державному кордоні». Дана постанова визначає основні напрями координації Адміністрації ДПСУ діяльності органів виконавчої влади та органів місцевого самоврядування, що здійснюють різні види контролю у пунктах пропуску через державний кордон або беруть участь у забезпеченні режиму державного кордону, прикордонного режиму і режиму в пунктах пропуску через державний кордон відповідно до Закону України «Про державний кордон України» [277].

У постанові окреслено коло питань, за якими взаємодіючими органами здійснюється обмін інформацією: про будь-які наміри і спроби порушити державний кордон та про затримання його порушників; ознаки підготовки до порушення державного кордону; місця зосередження та маршрути пересування нелегальних мігрантів; виявлення осіб, стосовно яких є відповідні доручення правоохоронних органів; спроби переміщення через державний кордон злочинців, що перебувають у розшуку, у тому числі з міжнародних злочинних угруповань; диверсії, терористичні акти, провокаційні дії та конфліктні ситуації в пунктах пропуску через державний кордон, у прикордонній смузі та контрольованому прикордонному районі; факти і канали незаконного переміщення через державний кордон товарів та інших предметів, валюти, сировини, небезпечних речовин і відходів, культурних та історичних цінностей, викрадених транспортних засобів; будь-які спроби незаконного ввезення та вивезення наркотичних засобів; надзвичайні ситуації, що виникли внаслідок порушення техногенної та екологічної безпеки у прикордонній смузі та контрольованому прикордонному районі і заходи щодо їх ліквідації; неможливість пропуску через державний кордон транспортних засобів, зумовлену обставинами організаційного або технічного характеру; факти і причини затримання транспортних засобів у пунктах пропуску через державний кордон, порушення розкладу руху

транспортних засобів міжнародного сполучення; осіб, у яких виявлено ознаки небезпечних інфекційних захворювань під час переміщення через державний кордон; ускладнення санітарно-епідемічної обстановки у прикордонній смузі та контрольованому прикордонному районі [277, п. 9].

Обмін інформацією може здійснюватися на рівні окремих органів і підрозділів ДПСУ з територіальними органами публічної адміністрації з інших питань, які визначаються у процесі підготовки планів взаємодії зазначених органів або уточнення цих планів. Порядок обміну інформацією визначається органами місцевого самоврядування відповідно до їх повноважень разом з Адміністрацією ДПСУ, її структурними підрозділами [276, с. 108].

Позитивною тенденцією є те, що взаємодіючі органи приймають міжвідомчі нормативні документи з питань обміну інформацією в інтересах виконання завдань як окремого органу, так і інтегративного спільного характеру. Наприклад, наказом МФ України, МВС України від 7 вересня 2017 р. № 746/759 затверджено Порядок взаємодії інформаційних систем ДФС України та ДПСУ щодо обміну інформацією, необхідною для забезпечення контролю при переміщенні осіб та транспортних засобів через державний (митний) кордон України та адміністративний кордон вільної економічної зони «Крим». Цей Порядок зорієнтовано на посилення контролю за переміщенням осіб і транспортних засобів через державний (митний) кордон України та удосконалення взаємодії інформаційних систем ДФС України та ДПСУ щодо обміну інформацією, необхідною для здійснення митного та прикордонного контролю за переміщенням осіб і транспортних засобів у пунктах пропуску через державний (митний) кордон України та адміністративний кордон вільної економічної зони «Крим» у контрольних пунктах в’їзду-виїзду [278, п. 1 р. 1].

Засобами забезпечення інформаційної взаємодії є інформаційні системи:

ДПСУ – інформаційно-телекомунікаційна система прикордонного контролю «Гарт-1»;

ДФС України – Єдина автоматизована інформаційна система ДФС України;

інтегрована міжвідомча інформаційно-телекомунікаційна система щодо контролю осіб, транспортних засобів і вантажів, які перетинають державний кордон (система «Аркан») [278, п. 3 Р. 1]. Взаємодія інформаційних систем суб'єктів інформаційного обміну здійснюється в електронному вигляді на центральному та територіальному рівнях шляхом: обміну інформацією у режимі реального часу; подання суб'єктами інформаційного обміну запитів на отримання інформації (у разі відсутності можливості обміну інформацією у режимі реального часу) **(додаток Е.1).**

Наказ МВС України, СБ України, Державної податкової адміністрації України (далі – ДПА України), Адміністрації ДПСУ, ДМСУ від 23 березня 2009 р. № 124/936/ 139/199/250 «Про затвердження Інструкції про порядок організації обміну інформацією між структурними підрозділами МВС України, СБ України, ДПА України, ДПСУ, ДМСУ в діяльності з виявлення та припинення корупційних діянь в правоохоронних органах» установлює порядок, рівні та шляхи організації обміну інформацією з виявлення та припинення корупційних діянь у правоохоронних органах [279] **(додаток Е.2).**

Важливою вимогою інформаційної взаємодії є дотримання та збереження властивостей інформації, а саме: достовірність, актуальність, своєчасність, оперативність, захищеність, повнота, корисність, зрозумілість. За таких умов у результаті інформаційної взаємодії отримана інформація дозволить приймати своєчасні управлінські рішення при зміні обстановки на державному кордоні та за інших умов, що дозволить забезпечити ефективну охорону державного кордону, підтримання правопорядку та законності у прикордонній смузі та контрольованому прикордонному районі, у пунктах пропуску через державний кордон.

Отже, інформаційна взаємодія відбувається на трьох рівнях:

на міжнародному (ДПСУ й прикордонні служби суміжних держав);

на рівні міністерств та інших органів виконавчої влади (між центральними апаратами (адміністраціями) уповноважених органів та підрозділів);

на регіональному (місцевому) рівні. Інформаційна взаємодія передбачає: порядок, підстави, форми обміну інформацією, які конкретні дані та у який час підлягають передачі, які суб'єкти залучені до інформаційної взаємодії. Інформаційна взаємодія здійснюється через інформаційні системи суб'єктів інформаційного обміну та під час проведення спільних заходів.

Адміністрація ДПСУ, впроваджуючи у повсякденну діяльність кращі практики держав ЄС постійно організовує та підтримує роботу Віртуального контактного аналітичного центру суб'єктів інтегрованого управління кордонами на міжвідомчому рівні. Безпосередньо на державному кордоні функціонують структурні підрозділи органів охорони державного кордону України – КП ДПСУ. Такі заходи значно посилюють і розвивають інформаційну взаємодію у сфері державного кордону, наслідком чого є підвищення ефективності охорони державного кордону України. Інформаційна взаємодія у сфері охорони державного кордону активно розвивається за такими основними спрямуваннями: функціонує Віртуальний контактний аналітичний центр; розширюються мережі та функції контактних пунктів; удосконалюється механізм обміну інформацією; проводяться спільні аналітичні дослідження з оцінки загроз і ризиків у сфері безпеки державного кордону й ефективності інтегрованого управління кордонами, надання взаємного доступу до інформаційних систем компетентних державних органів тощо.

Висновки до розділу 2

У процесі дослідження нормативно-правового регулювання внутрішньовідомчих інформаційних відносин ДПСУ запропоновані авторські визначення понять:

нормативно-правове регулювання інформаційної складової в діяльності Державної прикордонної служби України відображає дію норм права на

відносини, об’єктом яких є інформація у сфері охорони державного кордону й упорядкування інформаційної діяльності органів і підрозділів ДПСУ;

інформаційна діяльність ДПСУ є реалізація (втілення) її основних видів (створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації), пов’язаних із процесами, які здійснюються з інформацією в інтересах охорони державного кордону та реалізацією прав людини, пов’язаних з вільним перетинанням державного кордону та дотриманням у зв’язку із цим інформаційних прав усіх суб’єктів прикордонних відносин;

правовий режим інформації з обмеженим доступом у діяльності ДПСУ – це установлені законодавством процедури та порядок надання дозволу, доступу, охорони, захисту, а також здійснення діяльності з інформацією, яка становить велику цінність для прикордонної безпеки держави.

Установлено, що нормативно-правове регулювання інформаційної складової в діяльності Державної прикордонної служби України передбачає упорядкування інформаційних відносин на підставі сукупності чинних нормативно-правових актів, що визначають основні засади, принципи, механізми забезпечення обігу інформації, зокрема і з використанням інформаційно-телекомунікаційних систем, у сфері охорони державного кордону, що здійснюється в процесі виконання завдань ДПСУ.

Інформаційна складова в діяльності ДПСУ урегульована системою нормативно-правових актів різного рівня ієрархії, а саме: Конституцією України (визначає основні інформаційно-правові засади такої діяльності); загальними або базовими нормативно-правовими актами, які визначають основні положення інформаційного права; спеціальними нормативно-правовими актами, що врегульовують інформаційну діяльність у межах повноважень ДПСУ; програмними документами, що формулюють основні напрямки розвитку відомства на близьку та середню перспективи з урахуванням актуальних загроз і потреб розвитку сфери охорони державного кордону.

Особливістю правового режиму інформації з обмеженим доступом є те, що у межах діяльності ДПСУ він набуває додаткових ціннісних характеристик,

обумовлених прикордонною сферою, що являє собою комплексну систему складних відносин, елементів, від чіткого й ефективного забезпечення яких залежить безпека державного кордону, територіальна цілісність, безпека держави та її громадян. Одним з ключових елементів цієї системи є інформаційна складова та інформаційна безпека.

Інформаційній складовій підготовки та прийняття управлінського рішення в охороні державного кордону притаманно багато компонентів (інформаційна діяльність, інформаційно-аналітична діяльність, інформаційні завдання, інформаційні потреби людини й держави у прикордонній сфері, актуальні бази даних, зовнішні та внутрішні інформаційні фактори начальника тощо), які повинні враховувати та поєднувати начальники прикордонних підрозділів.

Інформативна складова щодо реалізації завдань в органах охорони державного кордону формується на підставі конкретних повідомлень, які отримує начальник із таких джерел, які містяться: в законах України, підзаконних нормативно-правових актах, які врегульовують загальну діяльність ДПСУ і окремих її підрозділів, а також у керівних документах ДПСУ (інформаційно-нормативна складова); загальних або конкретних вказівках, уточненнях обстановки, діях, які надходять від керівництва ДПСУ (інформаційно-управлінська складова), по лінії оперативно-чергової служби від підрозділів прикордонного загону, взаємодіючих правоохоронних органів або місцевих органів публічної влади (оперативно-інформаційна складова); даних опрацьованих в результаті діяльності інформаційно-аналітичних підрозділів (інформаційно-аналітична складова); обстановці (ситуації), яка склалась в підрозділах прикордонного загону (інформаційно-практична складова); результатах проведення оперативно-розшукової діяльності відповідними підрозділами ДПСУ (оперативно-розшукова інформаційна складова); результатах роботи зі зверненнями громадян (інформаційно-консультативного характеру).

Інформаційна взаємодія закладає основи для спільної діяльності та покращання ефективності в охороні державного кордону України, має цілеспрямований характер, орієнтована на обмін інформацією щодо своєчасного

виявлення, попередження та недопущення порушення прикордонного законодавства та забезпечення недоторканності державного кордону.

Інформаційна взаємодія являє собою не лише фактичну передачу відповідних даних, але й організацію та здійснення інформаційного процесу. Проте, ключова роль відводиться саме обміну інформацією, який може відбуватись усно (в телефонному режимі), письмово, електронно. За змістом це може бути: передача інформації в інтересах відомства, узгодження спільних дій, обмін результатами діяльності, внесення інформації у банки даних тощо. Обмін інформацією здійснюється з урахуванням інформаційних потреб і інформаційних інтересів та є окремим напрямком спільної діяльності правоохоронних органів в забезпеченні прикордонної безпеки.

Інформаційна взаємодія в діяльності ДПСУ активно розвивається за такими основними спрямуваннями: функціонування Віртуального контактного аналітичного центру; розширення мереж і функцій контактних пунктів; удосконалення механізму обміну інформацією; проведення спільних аналітичних досліджень з оцінки загроз і ризиків у сфері безпеки державного кордону й ефективності інтегрованого управління кордонами, надання взаємного доступу до інформаційних систем компетентних державних органів тощо.

РОЗДІЛ 3
НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ВІДНОСИН ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ З ІНФОРМАЦІЙНОЮ СФЕРОЮ СУСПІЛЬСТВА

3.1 Інформаційна відкритість як основа комунікації Державної прикордонної служби України з інформаційною сферою суспільства

Стратегією розвитку ДПСУ передбачено створення ефективного механізму комунікації з громадськістю та використання її потенціалу для реалізації державної політики у сфері охорони державного кордону, а також залучення громадськості до формування, реалізації та проведення моніторингу антикорупційної політики в ДПСУ. У Стратегії було заплановано збільшити рівень довіри громадян до ДПСУ на близьку перспективу (2017 рік) до 63 %, на середню перспективу (2020 рік) до 70 % [59].

За даними загальнонаціонального дослідження соціологічної служби Центру Разумкова, яке проводилося у період з 7 по 14 лютого 2019 року в усіх регіонах України за винятком Криму та окупованих територій Донецької та Луганської областей, ДПСУ висловили довіру – 52 % опитаних респондентів [280]. За результатами дослідження, проведеного з 6 по 11 вересня 2019 року виявилось, що, у порівнянні з лютим 2019 року, довіра до ДПСУ з боку громадян зросла на 10 % та складає 63 % [281]. Отже, темпи зростання довіри громадян до ДПСУ не повною мірою відповідають очікуваним показникам, зазначеним у Стратегії **(додаток Ж.1)**, а тому потребують вжиття рішучих кроків, щодо оптимізації роботи структурних підрозділів ДПСУ у напрямку наближення до інформаційної сфери суспільства. З цією метою у ДПСУ вперше в Україні розпочато впровадження унікального проекту стратегічних комунікацій. Цей проект здійснюється у прикордонному відомстві разом з Центром стратегічних

комунікацій «StratCom Ukraine» за підтримки Посольства Сполучених Штатів Америки та Міжнародної організації з міграції в Україні. На думку директора Центру стратегічних комунікацій «СтратКом Україна» О. Горбач**,** «впровадження стратегічних комунікацій вже має позитивні результати». З цього приводу, С. Дейнеко наголосив, що «важко бути першими, але ми розуміємо необхідність доносити до суспільства правду» [282].

У законодавстві поняття «інформаційна сфера» детерміновано лише в міжнародній угоді «Про вільний доступ і порядок обміну відкритою науково-технічною інформацією держав – учасниць СНД» як сфера (середовище) – сфера діяльності суб'єктів, пов'язана зі створенням, переробкою та використанням інформації [283]. Загалом термін «сфера» має багатовекторне застосування: район дії, межа поширення чого-небудь; область фізичного або духовного життя, діяльності людини чи суспільства; галузь знання, виробництва і т. ін.; сукупність умов, середовище, в яких що-небудь відбувається; обстановка; область дії, границі поширення чого-небудь [284]. Отже, сфера визначає межі чогось, окреслює певний простір використання чи застосування конкретного предметного явища, у нашому випадку інформації, усе, що пов'язано, підтримує та забезпечує правове упорядкування обігу інформації.

У проекті Концепції інформаційної безпеки «інформаційну сферу» пропонується розуміти як: сукупність інформаційних технологій, ресурсів, продукції і послуг, інформаційної інфраструктури, суб'єктів інформаційної діяльності та системи регулювання суспільних інформаційних відносин [285].

Ще один проект Указу Президента України, який так і не було прийнято, Стратегія розвитку інформаційного простору України на період до 2020 року пов'язує інформаційне середовище з інформаційним простором України у безпосередньому зв'язку з інформаційними процесами та інформаційними відносинами (з приводу створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації), інформаційних продуктів та інформаційних ресурсів, а також інформаційна взаємодія організацій та громадян і задоволення їхніх інформаційних потреб відповідно до чинного

національного законодавства [286]. Отже, із норми законодавства (міжнародна угода «Про вільний доступ і порядок обміну відкритою науково-технічною інформацією держав – учасниць СНД»), а також задумів законотворців (згаданих вище проектів нормативно-правових актів) можна підсумувати, що інформаційна сфера розглядається у широкому сенсі як сукупність інформаційних відносин, а також засобів (ресурсів) їх втілення та забезпечення у межах норм національного законодавства.

У своєму дослідженні Ю. П. Бурило інформаційну сферу уособлює зі сферою інформаційної діяльності та пояснює що, «такий підхід відображає динамічний взаємозв'язок таких категорій, як суб'єкт інформаційної діяльності, його дії та об'єкти, на які спрямовані ці дії». Науковець поділяє інформаційну сферу на інформаційні відносини, об'єктом яких є інформація та інформаційно-інфраструктурні відносини, об'єктом яких виступають засоби зв'язку, інформатизації та інформаційної безпеки [22, с. 5]. Інформаційна сфера, пише А. В. Пазюк, – це сфера суспільних інформаційних відносин, які здійснюються суб'єктами права за допомогою використання існуючої на національному та глобальному рівнях інформаційної інфраструктури [287].

К. І. Бєляков, інформаційну сферу розглядає через сукупність інформаційних ресурсів, активізація та активне використання яких стає можливим завдяки поєднанню із засобами, методами й умовами [288, с. 98].

Інформаційну сферу, зазначає О. А. Баранов, утворює сукупність інформації та інформаційних процесів, інформаційна інфраструктура, суб'єкти, що здійснюють та забезпечують оборот інформації, усі суспільні відносини, які при цьому виникають, система їх правового регулювання та саморегулювання, а також інституційна сфера публічної влади у цій сфері [289, с. 17].

О. А. Заярний підкріплює існуючі наукові погляди, наявні у науковій літературі, твердженням, що змістоутворюючим елементом інформаційної сфери виступає інформація, динамічною (предметно-функціональною) основою цього поняття є інформаційна діяльність та середовище її здійснення (територіальний і віртуальний простір) [290, с. 23]. Науковець обґрунтовує, що функціональне

призначення інформаційної сфери виявляється у забезпеченні виникнення та підтримання у встановлених законодавством України параметрах правових зв'язків між суб'єктами інформаційної діяльності, її об'єктами, змістом, а також законними інтересами та потребами, для досягнення яких фізичні, юридичні особи, суб'єкти владних повноважень вступають в інформаційні відносини. О. А. Заярний підсумовує, що інформаційна сфера з позицій правового регулювання постає як предметно-територіальний, системно-структурний юрисдикційний простір вчинення дій щодо збирання, зберігання, обробки, передачі, перетворення та захисту інформації, виробництва інформаційної продукції, надання інформаційних послуг, формування інформаційної інфраструктури, а також забезпечення прав, законних інтересів учасників інформаційних відносин, інформаційної безпеки держави, межі якого визначаються властивостями самої інформації, її правовими режимами, а також видами інформаційної діяльності [290, с. 24].

Значний науковий інтерес до категорії «інформаційна сфера», на нашу думку, зумовлений всезагальністю, універсальністю та важливістю категорії «інформація», не тільки для юриспруденції та правових відносин, але і інших сфер наукових знань і людської діяльності. У нашому розумінні «інформаційна сфера» охоплює відносини у суспільстві, що акцентовані на інформаційній компоненті (інформація, знання, дані, відомості, факти), з урахуванням сфери людських інтересів (зв'язків), що врегульовані нормативно-правовими актами, тобто її юридичний аспект.

Отже, з урахуванням предмета нашого дослідження варто підсумувати, що «інформаційна сфера суспільства» поняття відносне, яке включає здійснення комунікації держави з громадянським суспільством у певних (просторових, територіальних, державних, предметних) межах, а саме – це урегульовані національним законодавством інформаційні відносини, інформаційні повноваження, сукупність інформаційних ресурсів ДПСУ, які дозволяють реалізувати інформаційні права, інтереси та потреби громадян, суспільства, органів і підрозділів ДПСУ у сфері охорони державного кордону.

На наш погляд, головними складовими інформаційної сфери суспільства у діяльності ДПСУ є суб'єктна та предметна складова. Суб'єктну складову утворюють компетентні структурні підрозділи й посадові особи, уповноважені здійснювати комунікацію з суспільством, громадськістю та громадянами, а також суб'єкти приватного права (фізичні особи), інші особи, що реалізують свої інтереси у сфері охорони державного кордону (перетинають або мають намір перетнути державний кордон України, висловлюють відповідно до законодавства потребу у сприянні, задоволенні чи захисті інформаційних прав). Предметність обумовлена відомчими повноваженнями ДПСУ – сфера охорони державного кордону України.

О. Сосін наголошує на тому, що всі питання розвитку засад громадянського й інформаційного суспільства слід розглядати в комплексі правових проблем такого широкого поняття, як «комунікація» [291, с. 20]. Таке твердження має своє раціональне зерно, адже «комунікація» (від лат. communico – спілкуюсь з кимось, повідомлення) передбачає спілкування, передачу інформації. Також це шляхи сполучення, лінії зв'язку, обмін інформацією, зв'язок [43, с. 562]. У контексті масової комунікації – це суспільний інститут, що виконує завдання формування світогляду і громадської думки широких мас засобами масової інформації і пропаганди [292]; відображає процес інформування широких мас із використанням технічних засобів [43, с. 562]. У широкому сенсі комунікація окреслює людську взаємодію у світі. Вона є ознакою конструктивної взаємодії між особистостями, соціальними групами, основою якої має бути толерантність та порозуміння [37, с. 291]. Крім того, комунікація з урахуванням процесів глобалізації та інформатизації розглядається як процес активного та пришвидшеного обміну інформації [293, с. 154]. О. В. Радченко і О. Є. Бухтатий називають інформаційно-комунікативну функцію цементуючою ланкою, що об'єднує суспільство в державу, й уособлюють її з інформаційною політикою держави [294, с. 34].

Формування засад і умов входження України до світового інформаційно-комунікаційного простору вимагає відкритого й чіткого викладення питань щодо

розв’язання проблем свободи слова, доступу до інформації, гарантій прав людей в інформаційній сфері взагалі (скажімо, захист персональних даних тощо) [291, с. 20]. Інформаційна відкритість органів державної влади пов’язана з дотриманням принципів публічності і гласності, забезпеченням доступу до публічної інформації, висвітленням діяльності органів державної влади, гарантуванням кожному права знати свої права і обов’язки, демократизацією суспільства, здійсненням демократичного цивільного контролю тощо. Усі ці складові відображають стан реалізації норм Конституції України, що «єдиним джерелом влади в Україні є народ» [126, ч. 1 ст. 5] та «кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір» [126, ч. 2 ст. 34]. Такі загальні ключові засади повинні пронизувати всю систему публічної влади з урахуванням предмета відання кожного суб’єкта та меж відповідальності.

Право на доступ до інформації закріплене в різних міжнародно-правових документах, зокрема, Конвенція Ради Європи про доступ до офіційних документів, Хартія основних прав ЄС, Конвенція Європейської економічної комісії ООН про доступ до інформації тощо). На національному рівні право доступу до інформації вважається одним з основних прав, яке в широкому розумінні гарантується конституційними положеннями (ч. 2 та ч. 3 ст. 34, ч. 2 ст. 50) [295, с. 84].

Відкритість держави перед громадянами є пріоритетом державної політики в інформаційній сфері, що закріплено Доктриною інформаційної безпеки України [148]. Зокрема, ця Доктрина уточнює напрямки розвитку відкритості, а саме:

розвиток механізмів електронного урядування;

сприяння розвитку можливостей доступу та використання публічної інформації у формі відкритих даних;

інформування громадян України про діяльність органів державної влади, налагодження ефективної співпраці зазначених органів із засобами масової інформації та журналістами;

проведення реформи урядових комунікацій;

розвиток сервісів, спрямованих на більш масштабне та ефективне залучення громадськості до прийняття рішень органами державної влади та органами місцевого самоврядування;

сприяння формуванню культури суспільної дискусії [148, п. 5]. Такі задекларовані напрямки відповідають вимогам розвитку інформаційного суспільства, тенденціям інформаційних потреб сучасної європейської людини та потребують конкретних механізмів і кроків їх втілення.

На запитання «Як Ви думаєте, що означає принцип «відкритості перед громадянами»?» 77,1 % обрали варіант можливість громадян звернутись (особисто, письмово) до посадових осіб ДПСУ за інформацією у межах компетенції прикордонного відомства, 73,6 % – поінформованість громадян про діяльність ДПСУ, 35,9 % можливість громадян прийти на прийом до посадових осіб ДПСУ, 32,9 % можливість громадян звернутись до посадових осіб ДПСУ за будь-якою інформацією і 12,6 % можливість громадян відвідувати приміщення органів і підрозділів ДПСУ **(додаток В)**. Для ДПСУ межі інформаційної відкритості обумовлені її завданнями (забезпечення недоторканності державного кордону та охорони суверенних прав України в її прилеглій зоні та виключній (морській) економічній зоні) [79, ст. 1] – з одного боку, та потребами громадян в інформації, пов’язаний зі сферою діяльності ДПСУ, – з іншого. Особлива активізація в необхідності отримання такої інформації громадянами спостерігається за останні роки, у зв’язку із розширенням переліку безвізових країн для українців, запровадженням біометричних закордонних паспортів в Україні, установленням контрольних пунктів в’їзду-виїзду до тимчасово окупованої території і з неї тощо. Крім того, сучасне інформаційне суспільство потребує відкритого діалогу та громадського контролю за діяльністю ДПСУ [296, с. 31]. Усе це зумовлює необхідність забезпечення інформаційної відкритості у сфері діяльності ДПСУ.

Варто підкреслити, що питання інформаційної відкритості у діяльності прикордонного відомства є актуальними не тільки для українського суспільства, але й для країн ЄС. Зокрема, за результатами контролю діяльності FRONTEX та у

напрямку подальшого зміцнення європейської кордону рекомендовано посилити прозорість у діяльності FRONTEX [297].

Вирішенню проблеми забезпечення необхідного рівня відкритості органів державного управління присвячені дисертаційні роботи Н. В. Гудими (Принципи відкритості і прозорості в діяльності органів державного управління України) [298], Н. В. Крук (Інформаційна відкритість влади як принцип діяльності органів державної влади) [299] та інших. Однак аналіз цих та інших праць дозволив визначити недосліджене досі коло питань, пов'язаних з інформаційною відкритістю у діяльності ДПСУ.

Інформаційна відкритість у теорії та нормативних джерелах ототожнюється із відкритістю діяльності органів публічної адміністрації. Поняття відкритості визначено в Академічному словнику української мови, де «відкритий» розкривається як такий, що: можна бачити без перешкоди; доступний зорові; доступний для всіх бажаючих; нічим не прикритий; неприхований, нетаємний; явний [300]. Відкритість влади у Енциклопедичному словнику з державного управління розглядається як прозорість (transparency), тобто перебування під публічним контролем; доступність (accessibility) кожному в будь-який час, усюди; чутливість до нових ідей та вимог, готовність оперативно реагувати (responsiveness) [301, с. 91].

У європейському законодавстві для означення відкритості та доступності отримання громадянами інформації, створеної та отриманої під час діяльності органів влади [302], застосовується термін «транспарентність» (transparency) [303], який сьогодні активно розробляється українськими науковцями. Поняття «transparency» дослівно перекладається як «прозорість».

Тлумачення поняття «транспарентність» знаходимо у Словнику бюджетної термінології як доведення до загального відома широкої громадськості інформації про рішення та дії органів влади, взагалі про діяльність будь-яких установ, організацій, суб'єктів господарювання посадових осіб [304]. У Банківській енциклопедії «транспарентність» – це розкриття банком для всіх зацікавлених осіб (кредиторам, інвесторам, громадськості) цілей діяльності, правових,

інституційних і економічних основ, принципових рішень і їх обґрунтування, даних та інформації, прямо або опосередковано пов’язаних з діяльністю банку, а також умов підзвітності в повному обсязі, у доступній формі та на своєчасній основі [305, с. 436].

Українські науковці по різному підходять до змісту категорії «транспарентність». Л. Наливайко та М. Романов вміщують та поєднують у змісті транспарентності такі поняття, як прозорість, відкритість, гласність, публічність, підзвітність, доступ до публічної інформації та участь в управлінні державними справами. При цьому зазначають суттєву відмінність цих окремих складових (ознак) транспарентності, де:

прозорість – це рівень обізнаності діями влади;

відкритість – це функціональна характеристика влади до демонстрації своєї діяльності, обізнаності в діях влади не наступить, допоки влада не буде діяти відкрито;

гласність – це характеристика влади, що робить її доступною до громадського обговорення;

публічність – це здатність влади виконувати свої функції перед «публікою» (тобто особами, що її обрали);

підзвітність є обмежувальною характеристикою влади, що відображає громадський контроль за її діяльністю, саме така «публічна» діяльність влади спричиняє громадське обговорення, а після – контроль (приводить до підзвітності) [306, с. 162].

Е. Афонін та О. Суший розглядають «транспарентність» як збірну категорію таких понять, як: прозорість (англ. – «transparency»), відкритість (англ. – «openness»), гласність (англ. – «publicity») [307].

Є. Б. Тихомірова транспарентність розглядає у тісному взаємозв’язку із відкритістю влади, яка (прозорість) стає можливою завдяки:

прозорості дій посадовців і владних підрозділів у взаємодії з представниками бізнесу та комерційними структурами;

відкритості засідань органів влади й управління, їх комісій, різноманітних консультативних структур для журналістів і представників різних груп громадськості;

відкритості документів органів влади й управління для журналістів і представників різних груп громадськості;

звітуванню державних органів про прийняті рішення, програми діяльності та виконання відповідних бюджетів і програм;

висвітленню діяльності органів державної влади та місцевого самоврядування засобами масової інформації;

розвитку на всіх рівнях державної влади електронного врядування [308, с. 41].

М. В. Пашковська аналізує такі наукові підходи у розумінні транспарентності:

ототожнюється із можливістю громадськості безперешкодного доступу до публічної інформації. Але такий підхід є дещо обмеженим, оскільки зачіпає лише один з аспектів транспарентності, а саме: забезпечення належного рівня відкритості органів державної влади та органів місцевого самоврядування;

розглядається як основа для налагодження ефективної комунікації між громадськістю і органами державної влади, проте таке трактування транспарентності теж не розкриває всіх сторін цього явища;

як засадниче поняття, яке поєднує декілька категорій, таких як: прозорість, відкритість, гласність, громадську участь тощо, які визначають форми та способи функціонування органів державної влади та місцевого самоврядування у демократичній державі. Такий підхід науковець називає – комплексний, який підсумовує, є повним відображенням змісту транспарентності [309, с. 140].

При цьому М. В. Пашковська зауважує, що забезпечення транспарентності в діяльності органів державної влади є складним системним процесом, що потребує постійного удосконалення, з огляду на виклики, які постають перед органами державної влади та громадськістю [309, с. 141].

О. А. Кудіна акцентує, що реалізація принципу транспарентності відбувається в рамках комунікації владних структур та громадськості і передбачає налагодження взаємодії між учасниками політичного процесу на умовах паритетності та інформаційної відкритості [310, с. 35].

Т. Ю. Ткачук зауважує на необхідності розгляду транспарентності, як багатогранного показника ефективної діяльності органів влади у інтегральному поєднанні таких категорій як: відкритість, прозорість, доступність [211, с. 291].

Отже, транспарентність характеризує якість взаємозв'язку влади і суспільства, визначає межі інформації у сфері діяльності органу публічної адміністрації, яка може бути доступною для громадян за їх активної позиції в отриманні конкретної інформації.

У практиці FRONTEX публічний доступ до її документів розглядається з позиції транспарентності. Це означає, що будь-який громадянин ЄС, а також будь-яка інша фізична чи юридична особа, яка проживає або має зареєстрований офіс в ЄС, має право на доступ до документів, що зберігаються у FRONTEX. Таку взаємодію забезпечує Transparency Office FRONTEX (Управління прозорості), що знаходиться у Варшаві (Польща), створено рішенням Правління FRONTEX № 25/2016 від 21 вересня 2016 р. [311]. Як можна побачити, структура FRONTEX також постійно оновлюється та вдосконалюється з реаліями часу та викликами суспільства.

У документах ЄС зустрічається означення відкритості поняттями «transparency» і «openness», тобто все ж таки ці поняття дуже подібні за змістом і означають доступність громадськості до відомостей, пов'язаних із діяльністю прикордонних структур.

Отже, «транспаретнність», «відкритість», «прозорість» є дуже близькими поняттями. Для громадян вони означають прозору діяльність ДПСУ, поінформованість про виконання завдань, обізнаність про рівень безпеки державних кордонів, ступінь дотримання прав громадян у сфері охорони державних кордонів, взаємозв'язок із органами охорони державного кордону та прикордонним відомством.

Інформаційна відкритість є результатом складного історичного процесу. Проблема відкритості як один із ключових аспектів функціонування державної влади була об’єктом наукової дискусії протягом багатьох століть. У міжнародній правовій практиці розуміння поняття «інформаційна відкритість державної влади» передбачає насамперед: свободу доступу (за усним чи письмовим запитом) до інформаційних ресурсів держави та наявність ефективних процедур її забезпечення; наявність у системі органів державної влади механізмів обов’язкового й активного інформування громадян про свою діяльність, незважаючи на наявність запитів [312].

У багатьох працях українських науковців інформаційна відкритість ототожнюється з демократизацією суспільства в таких контекстах:

рівень відкритості є головним критерієм демократичності державної влади [313, с. 264];

демократичність системи пропорційна її інформаційній відкритості [299, с. 6];

відкритість є невід’ємною характеристикою демократичної, відповідальної перед громадянами держави [312];

інформаційна відкритість органів державної влади є індикатором рівня демократії [314];

відкритість і прозорість діяльності органів державного управління виступають важливими чинниками демократичного устрою держави [298, с. 12]. Такі тези підкреслюють нерозривність зв’язку демократичних засад суспільства й інформаційної відкритості в діяльності ДПСУ.

Відкритість і доведення своєчасної інформації громадськості про свою діяльність, за винятком випадків прийняття рішень, що містять службову чи таємну інформацію, відповідає прозорості та гласності як основним принципам діяльності державного апарату [64, с. 168].

Гласність один з принципів: 1) здійснення демократії, гарантії ефективного функціонування усіх її інститутів; 2) діяльності державних органів, органів місцевого самоврядування та об’єднань громадян; 3) реалізації права на

інформацію. Забезпечується насамперед розповсюдженням інформації у всіх сферах суспільного і державного життя через спеціальні інформаційні служби, ЗМІ та інші засоби інформування, відкритим (публічним) характером державних органів, органів місцевого самоврядування, окрім випадків, передбачених законами України [315].

Гласний, тотожний поняттям доступний для широкої громадськості; відкритий, публічний [316]. Гласність Короткий словник політологічних термінів розкриває як один з найважливіших принципів демократизму, який полягає у невід'ємному праві кожного громадянина на отримання повної і вірогідної інформації з будь-якого питання громадського життя, що не становить державної чи військової таємниці [317]. Відкритість і прозорість полягає у забезпеченні громадянам доступу до інформації про управлінські процеси й інститути, достатньої для розуміння та спостереження [258, с. 57].

Ф. Шоер називає прозорість властивістю, що полегшує отримання інформації, яку можна визначити як заборону органам влади приховувати певну інформацію або ж як вимогу формулювати цю інформацію максимально доступно. Разом з тим необхідно осмислювати прозорість як властивість, рівень якої може змінюватися, відповідно до двох характеристик: прозорості самої інформації та доступу до неї [318].

Л. Мосора зауважує, що проблема часто полягає у тому, що відкритість розглядається з точки зору прозорості, відповідно до якої громадяни мають право отримувати інформацію про діяльність органів державної влади та місцевого самоврядування. З цієї точки зору громадяни, по суті, займають пасивну позицію, адже навіть отримавши певну потрібну для них інформацію, не завжди у змозі нею правильно скористатись. А відкритість, стверджує науковець, усе ж повинна відображати активну позицію громадян, яка полягає в можливості впливати на прийняття управлінських рішень шляхом участі в їх обговоренні чи ухваленні [313].

Відкритість перебуває у логічному зв'язку з такими елементами: розповсюдження інформації про особливості перетинання державного кордону

України; взаємовідносин громадян із ДПСУ; довірою суспільства до ДПСУ та її посадових осіб; поінформованістю про події та факти на державному кордоні; можливістю обговорення проектів нормативно-правових і регуляторних актів тощо.

Закон України «Про Державну прикордонну службу України» у ст. 3 закріплює основні принципи діяльності ДПСУ, серед яких: поєднання гласних, негласних та конспіративних форм і методів діяльності; відкритість для демократичного цивільного контролю [79, ст. 3].

Поєднання гласних, негласних та конспіративних форм і методів діяльності є спеціальними принципами діяльності [319, с. 50] та ґрунтується на вимогах Закону України «Про оперативно-розшукову діяльність України» від 18 лютого 1992 р. [320, ст. 2], тобто стосується окремого виду оперативно-службової діяльності ДПСУ – ведення ОРД в інтересах забезпечення захисту державного кордону України, а не всіх напрямків діяльності ДПСУ. Але якщо провести логічний ланцюг, що у формах діяльності державних органів здійснюються їх функції, а їх реалізація відбувається на підставі імперативних засад, у відправних нормах-принципах організації та діяльності, то маємо таку взаємозалежну послідовність: принципи – функції – форми. Тоді можемо допустити, що в Законі України «Про Державну прикордонну службу України» у принципі «поєднання гласних, негласних та конспіративних форм і методів діяльності» йдеться про усі структурні елементи ДПСУ [296, с. 32].

Загалом принцип прозорості зобов’язує публічну адміністрацію таким чином організувати своє функціонування, щоб процеси та належне інформаційне забезпечення були доступними приватним особам для ознайомлення. Інформування населення суб’єктами публічної адміністрації здійснюється про поточні справи, заплановані заходи та прийняті рішення. Таке інформування є додатковим механізмом підвищення довіри до діяльності суб’єктів публічної адміністрації та їх рішень [295, с. 84]. Принцип прозорості може мати вияв як в інформаційній (доступ до інформації), так і фізичній формі (відвідування органу публічної влади для ознайомлення з його роботою та результатами) [295, с. 84].

Відкритість передбачає: право на одержання публічної інформації; обов'язок ДПСУ інформувати населення про свою роботу; оприлюднення нормативно-правових актів та інших владних рішень [319, с. 48]. М. Лациба зауважує, що інформаційна відкритість державних органів визначається трьома простими питаннями:

1. Яку інформацію державні службовці зобов'язані оприлюднювати (публікувати) безвідносно до запиту особи?

2. Яку інформацію державні службовці не мають права надавати на запит особи?

3. Які основні процедури державні службовці мають виконувати з метою оприлюднення чи надання інформації? Причому, це питання потребує найдетальніших уточнень у законах, зокрема в тих моментах, коли йдеться про певні терміни, носіїв інформації, коло суб'єктів, а також про відшкодування витрат за оприлюднення (опублікування) або надання інформації на запит особи [321, с. 13].

Відкритість влади, характеризується трьома основними чинниками: якість чинного нормативно-правового забезпечення, згідно з яким функціонує державний апарат; існування дієвих і конкретних механізмів і процедур реалізації прав доступу громадян до інформації про діяльність державної влади; існуючий у суспільстві, і зокрема в державному апараті, рівень політичної культури [301, с. 91].

Отже, інформаційну відкритість у діяльності ДПСУ характеризують такі елементи: нормативно врегульований механізм забезпечення отримання всіма інформації про діяльність прикордонного відомства та його структурних підрозділів і посадових осіб; стан забезпечення реалізації прав громадян на інформацію у прикордонній сфері; визначення способів оприлюднення інформації у прикордонній сфері через доступні процедури; простота та доступність електронного урядування у ДПСУ; визначення змісту інформації, яка підлягає оприлюдненню, а отже і її чітке розмежування на інформацію, що може бути доведена до всіх (публічна відкрита); стосується окремої особи (конфіденційна)

чи групи осіб або безпеки держави (службова чи таємна), які результати діяльності та дії посадових осіб ДПСУ підлягають оприлюдненню; рівень інформаційної культури персоналу ДПСУ [296, с. 33–34].

Забезпечення прозорості та відкритості суб'єктів владних повноважень і створення механізмів реалізації права кожного на доступ до публічної інформації врегульовано Законом України «Про доступ до публічної інформації». Доступ до публічної інформації відповідно до цього Закону здійснюється на принципах: прозорості та відкритості діяльності суб'єктів владних повноважень; вільного отримання, поширення та будь-якого іншого використання інформації, що була надана або оприлюднена відповідно до цього Закону, крім обмежень, установлених законом; рівноправності, незалежно від ознак раси, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, мовних або інших ознак [97, ст. 4]. Доступ до інформації забезпечується шляхом: систематичного й оперативного оприлюднення інформації: в офіційних друкованих виданнях; на офіційних веб-сайтах у мережі Інтернет; на єдиному державному веб-порталі відкритих даних; на інформаційних стендах; будь-яким іншим способом; надання інформації за запитами на інформацію [97, ст. 5].

З метою підвищення рівня довіри до ДПСУ та поширення її позитивного іміджу в суспільстві прикордонне відомство приділяє посилену увагу інформуванню громадськості про основні події, які відбуваються в ООДК, висвітленню результатів оперативно-службової діяльності через засоби масової інформації, розміщенню інформацій на офіційному сайті ДПСУ та у відомчих виданнях. Такий напрямок діяльності відбувається завдяки функціонуванню прес-служби ДПСУ. Як зазначають, В. І. Захарчук та І. О. Свідерська, головною метою та філософією існування прес-служби органів охорони державного кордону є подолання «закритості» своєї структури, руйнування бар'єра непоінформованості та нерозуміння, які можуть виникати між ООДК та громадськістю (населенням) [322, с. 41]. При цьому зазначають про існування проблеми у наданні інформації при забезпеченні балансування між «точкою зору та позиції керівництва ООДК»

та вимогами представників ЗМІ, які вимагають ту інформацію, з точки зору журналістів «якої потребують читачі, слухачі й глядачі». Тому представники прес-служб ООДК повинні знаходити «золоту середину» між цими напрямками, у чому саме і полягає глибинна філософія їхньої щоденної роботи [322, с. 42]. Така позиція відображає складність роботи прес-служб ООДК в умовах вивільнення від радянських традицій, але ніяким чином не сучасного європейського інформаційного суспільства, де інформація повинна надаватись достовірна й об'єктивна, а не та, яка «зручна». Хоча сьогодні керівництво ДПСУ відстоює позицію дотримання європейських цінностей і необхідності «бути чесним із громадянами» [282]. Усебічне й об'єктивне надання інформації прес-службами з урахуванням своєчасності найбільше відображає інформаційну відкритість у діалозі з інформаційною сферою суспільства.

Оприлюднення інформації про діяльність відомства регулярно здійснюється на офіційному веб-сайті відомства; у власних відомчих виданнях, таких як: телепрограми «Кордон держави», «Периметр», «КордонUA», сторінки ДПСУ у соціальних мережах: основна сторінка ДПСУ у мережі Facebook, Twitter; сторінки регіональних управлінь ДПСУ; інші: Окремий контрольно-пропускний пункт «Київ», 10-й Мобільний прикордонний загін, Навчальний центр, НАДПСУ, у мережі YouTube [323, P. 3]; ЗМІ, оприлюднення інтерв'ю посадових осіб ДПСУ; на інформаційних стендах, зокрема в пунктах пропуску через державний кордон тощо.

Актуальними останнім часом стали повідомлення, новини та інформаційні ролики на сторінці «Державна прикордонна служба України» у мережі Facebook [324], зокрема транслювання ефіру «РадіоКордон» [325], де надаються консультації експертів, юридичні консультації, обговорюються нові умови перетинання державного кордону. Анонсування обговорення таких питань відбувається завчасно, що надає можливості громадянам задати свої запитання, на які у подальшому ефірі отримають конкретні відповіді. У таких ефірах надається актуальна інформація різними експертами у своїй сфері діяльності ДПСУ (начальник відділу паспортної роботи управління організації прикордонного

контролю Адміністрації ДПСУ консультує з питань набрання чинності змін до правил в'їзду на територію тимчасово окуповану територію Автономної Республіки Крим та виїзду з неї громадян України віком до 16 років; роз'яснення особливостей заповнення декларацій посадовими особами ДПСУ, начальником відділу запобігання корупційним ризикам управління забезпечення доброчесності Адміністрації ДПСУ).

Діяльність Головного центру зв'язку, автоматизації та захисту інформації ДПСУ, посадових осіб відділу з питань взаємодії із ЗМІ та зв'язків з громадськістю Адміністрації ДПСУ, прес-служб регіональних управлінь та прес-секретарів органів ДПСУ зосереджена на таких напрямках: створення інформаційного контенту єдиного формату відповідно до розроблених контент-планів для кожної сторінки (акаунта); зменшення навантаження на аудиторію з основної сторінки шляхом систематизації та розмежування новинної складової; максимальне охоплення усієї інформації та висвітлення її через сторінки (акаунти) в рамках нової структури; формування аудиторії за регіональним принципом і забезпечення ідентифікації публікацій, матеріалів та медіапродукції користувачами; визначення ефективних інструментів для покращання інформування громадськості і збільшення аудиторії та читачів; оперативність та ефективність висвітлення інформації та мінімізація можливості маніпуляції контентом у проведенні негативно направлених акцій; забезпечення якісного контенту та усунення неактуального і застарілого; виокремлення цільової аудиторії; зміцнення довіри населення до ДПСУ [323, P. 2].

Отже, інформаційна відкритість полягає в дієвості механізмів оприлюднення та надання інформації, пов'язаної з функціонуванням ДПСУ, а її результатом має бути доступність й отримання безперешкодно громадянами інформації у сфері компетенції прикордонного відомства, за їх потребами й інтересами. Інформаційна відкритість відображає рівень демократичності системи органів публічної адміністрації, може закріплюватись у законодавстві як принципи діяльності окремого органу влади – гласність, відкритість, прозорість. Тому вважаємо, що в Законі України «Про Державну прикордонну службу України»

необхідно доповнити норму стосовно закріплення принципу відкритості (транспарентності) діяльності ДПСУ перед інформаційною сферою суспільства, про що більш детально нами буде сформульовано у розділі 5. Загалом у діяльності прикордонного відомства належним чином організована робота із забезпечення висвітлення публічної інформації, що свідчить про відповідний стан інформаційної відкритості у діяльності ДПСУ, але вона потребує постійного розвитку.

3.2 Організаційні засади забезпечення приватності в регулюванні інформаційних відносин

Приватне життя кожної особи, захищеність її особистих даних становить пріоритет у сучасному цивілізованому суспільстві. Глобальна інформатизація та відсутність чіткого правового механізму регулювання отримання, використання та захисту інформації про особу можуть стати причиною її розповсюдження та порушити баланс предметності приватного та публічного буття. Збереження приватного життя для кожної особи є природною потребою, а розголошення подробиць визначається особисто його власником. Крім того, упровадження принципів захисту приватності в Україні має не лише етичне, але й нормативне підґрунтя. У контексті реалізації договору про асоціацію між Україною та ЄС нові приписи правил ЄС підлягають обов'язковому опрацюванню і впровадженню в національне законодавство [326, с. 5], серед яких затверджені у травні 2016 року Європейським Парламентом і Радою ЄС нові правила і порядок захисту персональних даних – так званий «Пакет захисту даних» [327], який установив більш жорсткі правові та організаційні засади їх захисту, а також передбачає впровадження єдиної правової політики у цій сфері не тільки для держав-членів ЄС, але й для інших країн світу, що мають політичні, економічні та соціальні зв'язки з ЄС [328, с. 46]. Саме тому першочерговим завданням для України на шляху стрімкого розвитку інформаційного суспільства є впровадження та

своєчасне удосконалення на основі кращих європейських практик дієвих механізмів гарантування обігу та захисту інформації, яка ідентифікує особу.

«Приватність» походить від «приватний» (який належить окремій особі (особам); не державний, не суспільний; пов'язаний з індивідуальним господарюванням; стосується окремої особи (осіб); особистий; не пов'язаний з службовою або суспільною діяльністю; який обслуговує окрему особу (осіб) або виконується поза державною службою [329]). А. В. Кардаш пропонує термін «privacy», що походить з англійської мови, використовувати як український відповідник «право на приватність» [330, с. 12]. Отже, приватність це все те, що пов'язане з окремою особою, стосується цієї особи та визначає межі її особистого інформаційного простору. Приватність також уособлюється із недоторканністю приватного життя кожної особи.

Право на приватність визнано й гарантовано нормами Конституції України. Зокрема, ст. 30 захищає територіальну приватність (недоторканність житла), ст. 31 комунікаційну приватність (таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції), ст. 32 інформаційну приватність («ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України», «не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди»), а стаття 28 – деякі аспекти фізичної приватності (жодна людина без її вільної згоди не може бути піддана медичним, науковим чи іншим дослідам») [331].

Приватність у контексті права на недоторканність особистого і сімейного життя розуміється виключно в інформаційному сенсі [330, с. 43]. З урахуванням змісту ст. 32 Конституції України, право на особисте життя означає надану людині й гарантовану державою можливість контролювати інформацію про саму себе, не допускаючи розголошення відомостей особистого, інтимного характеру [332, с. 234]. Актуальність та важливість інформаційної приватності зумовлено теоретичними та практичними передумовами історичного розвитку цього права. В. Г. Пилипчук ґрунтовно дослідивши проблеми захисту приватності, робить цілком логічний висновок, про необхідність і правомірність формування

«інституту права приватної власності людини на свої персональні дані» [333, с. 116–117].

Нас, насамперед, цікавить інформаційна приватність в аспекті ідентифікації осіб, що вступають у відносини з органами та підрозділами ДПСУ, зокрема й під час проходження прикордонного контролю у пунктах пропуску через державний кордон України, доступу до інформації та забезпечення захисту такої інформації.

Важливою складовою у питанні дотримання приватності є установлення кола даних, що її (приватність) визначають, установлення межі між загальнодоступною та особистою інформацією, визначення законних підстав зміни їх полярності. У діяльності ДПСУ актуальною є ідентифікація за допомогою персональних даних, яка (ідентифікація) по суті є засобом встановлення відповідності, ототожнення, розпізнання ідентичних ознак, належність даних між різними об’єктами, відомого з невідомим, у тому числі особи саму із собою (наприклад, пред’явника паспортного або іншого документа із зображенням особи у ньому). Опитані респонденти висловили свої погляди з приводу розуміння відомостей, які можуть бути віднесені до персональних даних, зокрема: інформація, зафіксована у паспортному чи іншому документі (77,1 %), прізвище, ім’я, дата народження (74,9 %), номер телефону, місце роботи (69,7 %), відомості чи сукупність відомостей про фізичну особу, яка ідентифікована (66,2 %), сімейний стан (59,3 %), електронна адреса (55 %), фотографія (49,4 %), обіймана посада (44,6 %) **(додаток В)**, що переважно, але безсистемно відображає розуміння змісту таких даних. При цьому респонденти 80,1 % відповіли «так» на питання: «Чи достатньо Ви поінформовані про перелік персональних даних підлеглих, які Ви не маєте право розголошувати?», у свою чергу 19,9 % відповіли «ні». Такий відсоток останнього показника не сприяє дотриманню персональних даних, тому необхідно посилювати проведення якісних роз’яснень для персоналу з цього питання та загалом підвищувати інформаційну культуру.

Сьогодні українське законодавство перебуває на шляху вироблення оптимальної моделі рівноваги визнання, закріплення, організації та захищеності обігу інформації, що становить персональні дані. У діяльності ДПСУ

використання та обіг персональних даних має багатоаспектну вагомість: відбувається фіксація факту перетинання державного кордону України окремою особою (громадянином України, іноземним громадянином та особою без громадянства); здійснюється виключення особи із переліку осіб, яким установлена заборона у перетинанні державного кордону (в'їзд/виїзд), з метою надання дозволу на реалізацію права на вільне пересування; виявлення осіб, які можуть становити загрозу чи створювати ризики у сфері безпеки державного кордону; установлення особи запитувача інформації, що містить персональні дані про неї.

Під час перетинання державного кордону особа надає необхідні персональні дані для отримання дозволу в'їзд/виїзд з території України, а коли особі потрібно дізнатись (підтвердити) у ДПСУ інформацію про себе (наприклад, щодо існування чи відсутності заборони їй у перетинання державного кордону, чи офіційне підтвердження факту перетинання нею кордону), необхідно пройти низку процедур, зокрема й ідентифікацію з метою забезпечення законодавства у сфері захисту персональних даних.

Реалізація завдань ДПСУ щодо забезпечення недоторканності державного кордону та охорони суверенних прав України в її прилеглій зоні та виключній (морській) економічній зоні будується на основних принципах, серед яких «повага і дотримання прав і свобод людини та громадянина» [79, ст. 3], зокрема й інформаційних прав, гарантованих Конституцією України [126, ст. 31, 32]. Необхідність дотримання зазначеного принципу, крім того, детерміновано вимогою щодо підвищення рівня довіри населення до ДПСУ та її особового складу.

Первинні персональні данні, які переважно (окрім тих осіб, які можуть становити загрозу національній безпеці), є достатніми для встановлення законних підстав для перетинання державного кордону України та формують базу даних «Відомості про осіб, які перетнули державний кордон України», що збираються під час здійснення процедури прикордонного контролю. Джерелом отримання інформації є паспортні та інші документи осіб, які перетинають державний

кордон, а також інформація, отримана у ході опитування осіб, що прямують через державний кордон [154, ст. 7].

Поняття «прикордонна процедура» в українському законодавстві згадується у контексті здійснення контролю першої лінії, другої лінії і лише відносно іноземців та осіб без громадянства під час в'їзду в Україну, де процедура здійснення контролю першої лінії передбачає проведення перевірки:

1) паспортного документа з метою встановлення його дійсності, наявності відповідно до вимог законодавства посвідки на постійне проживання чи візи;

2) наявності чи відсутності у базах даних ДПСУ інформації про заборону в'їзду в Україну та про доручення правоохоронних органів щодо осіб, які перетинають державний кордон;

3) відміток про перетинання державного кордону в паспортному документі іноземця або особи без громадянства [154, ст. 9].

Процедура здійснення контролю другої лінії проводиться за результатами аналізу й оцінки ризиків під час виконання процедури контролю першої лінії, якщо в уповноваженої службової особи ДПСУ виникли сумніви щодо виконання іноземцем або особою без громадянства умов в'їзду в Україну, та передбачає:

1) встановлення місць відправлення та призначення, мети й умов запланованого перебування з проведенням у разі необхідності перевірки відповідних підтверджуючих документів і співбесіди;

2) з'ясування наявності достатнього фінансового забезпечення на період запланованого перебування і для повернення до держави походження або транзиту до третьої держави або наявності можливості отримати достатнє фінансове забезпечення в законний спосіб на території України [154].

У ДПСУ щоденно відбувається робота з обігом інформації, що становить персональні дані осіб, варто згадати хоча б про формування бази даних «Відомості про осіб, які перетнули державний кордон України» [92]. Тому особливої актуальності набуває визначення обсягу персональних даних осіб, що перетинають державний кордон та їх захист у діяльності ДПСУ відповідно до вимог Закону України «Про захист персональних даних», формування пропозицій

удосконалення обігу такої інформації на основі практики прикордонних органів ЄС.

Однією з вагомих умов обробки персональних даних посадовою особою ДПСУ є надання згоди суб'єкта персональних даних, що є вимогою ст. 2 Закону України «Про захист персональних даних» та п. 2.7. наказу Уповноваженого ВРУ з прав людини «Типовий порядок обробки персональних даних» [334].

Обробка персональних даних, зокрема її початкова процедура (збирання) під час прикордонного контролю повинна здійснюватись лише за згодою суб'єкта персональних даних (особи, що прямує через державний кордон), за винятком тих випадків, коли така згода не вимагається Законом [334, п. 2.7]. Зокрема, 97,4 % опитаних респондентів вірно відповіли «так» на питання «Чи потрібна згода суб'єкта персональних даних на обробку її персональних даних?», і лише 2,6 % – «ні». Та зазначили, що згода на обробку персональних даних надається у письмовій формі (61,9 %), у формі, що дає змогу зробити висновок про надання згоди (34,6 %) й 3,5 % усно **(додаток В)**.

Отже, така згода суб'єкта персональних даних можлива в одній із таких форм: висловлене у письмовій формі добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки; висловлене у формі, що дає змогу зробити висновок про надання згоди; у сфері електронної комерції згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції шляхом поставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки за умови, що така система не створює можливостей для обробки персональних даних до моменту поставлення відмітки [335, ст. 2].

Аналіз норм прикордонного законодавства дозволив установити відсутність формулювання мети та форми згоди на обробку персональних даних осіб, що перетинають державний кордон України.

Персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися [335, ч. 8 ст. 6]. У Положенні про базу даних «Відомості про осіб, які перетнули державний кордон України» установлено, що інформація Бази даних осіб зберігається щодо відомостей про громадян України, іноземців та осіб без громадянства протягом 5 років, після закінчення цих строків знищується комісійно [92, п. 29].

Закон України «Про інформацію» визначає, що інформація про фізичну особу (персональні дані) передбачає відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [57, ст. 11]. Ч. 2 ст. 11 цього Закону обмежено встановлює перелік даних, що визначають інформацію про особу, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження [57, ч. 2 ст. 11], при цьому зазначена норма упускає сукупність основних елементів, що ідентифікують особу, – прізвище, ім'я та по батькові, також це можуть бути і інші дані (наприклад, реєстраційний номер облікової картки платника податків, банківська картка тощо).

Закон України «Про захист персональних даних» закріплює, що персональні дані є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [92, ст. 2], що ідентично змісту згаданій вище нормі Закону України «Про інформацію», й аналогічно не надає уточненого переліку видів такої інформації. У ч. 4 ст. 6 цього Закону застосовано категорію «первинне джерело відомостей про фізичну особу», а саме: видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе [65]. Із цієї норми можна виокремити, що первинними відомостями, завдяки яким можна встановити конкретну особу, є: ім'я, дата та місце народження, місце проживання, підпис, інші відомості про особу, які містяться в документах.

Відповідно до Регламенту (ЄС) 2016/679 Європейського парламенту та Ради від 4 травня 2016 року «General Data Protection Regulation» термін «персональні дані» означає будь-яку інформацію, що стосується ідентифікованої фізичної

особи («суб'єкт даних»), та уточнює, що ідентифікувати фізичну особу можна прямо чи опосередковано, зокрема, посилаючись на такий ідентифікатор, як ім'я, ідентифікаційний номер, дані про місце знаходження, ідентифікатор в Інтернеті за одним або декількома факторами, що характеризують фізичні, фізіологічні, генетичні, розумові, духовні, економічні, культурні чи соціальні ідентичності цієї фізичної особи. На практиці вони також включають усі дані, які є або можуть належати людині будь-яким способом. Наприклад, номер телефону, кредитна картка, дані рахунку, номерний знак, зовнішній вигляд, номер клієнта або адреса – це всі особисті дані, крім того це може бути IP-адреса, думки, судження чи оцінки [327]. Отже, персональні дані – це будь-які дані, що можуть конкретизувати та визначити фізичну особу, а ключовою у цьому зв'язку є «будь-яка інформація», яка дозволяє «ідентифікувати особу».

Відносно осіб, щодо яких прийнято рішення про повернення, до їх персональних даних належать: ім'я та прізвище, місце призначення, виїзду та місце прибуття, дата народження, національність, стать, країна походження, тип та термін дії проїзного документа, здоровий чи ні, чи є добровільним чи примусовим повернення та оцінка ризику для безпеки [336].

У Регламенті ЄС використовуються такі категорії відносно інформації про особу «спеціальні категорії персональних даних» (special categories of personal data) (Art. 9 GDPR), до яких належать персональні дані, що виявляють расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання чи членство в профспілках, генетичні дані, біометричні дані, дані про стан здоров'я або дані щодо статевого життя або сексуальної орієнтації особи.

Використовується також категорія «вразливі персональні дані», зокрема етнічне та расове походження, фотографія особи (Art. 49 GDPR), стан здоров'я (Art. 53 GDPR), до яких встановлюється особлива система їх обробки та вищий ступінь захисту, що передбачено законодавством. Отже, одні й ті ж дані можуть належати до різних категорій.

Варто наголосити, що в Регламенті ЄС використовується однозначний термін «персональні дані», на відміну цьому в Законі України «Про інформацію»

«персональні дані» ототожнюються із поняттям «інформація про фізичну особу» (ст. 11), що спричиняє плутанину у правозастосовчій діяльності. Хоча, відповідаючи на питання «Чи є відмінність між поняттями «персональні дані» і «інформація про особу?» 89,6 % опитуваних респондентів відповіли «так», й лише 10,4 – «ні» **(додаток В)**. Отже, персональні дані як поняття містить чітку прив'язку до ідентифікації за допомогою цієї інформації про певну особу. Персональні дані – це не будь-яка інформація про фізичну особу, а лише інформація про ідентифіковану або таку, що може бути ідентифікована, фізичну особу. А якщо фізична особа не ідентифікована і не може бути ідентифікована, то інформація, що стосується фізичної особи, не є її персональними даними [330, с. 55].

Така позиція аналогічна Регламенту (ЄС) 2016/679 Європейського парламенту та Ради «General Data Protection Regulation» де «персональні дані» є будь-яка інформацію, що стосується ідентифікованої фізичної особи [327]. Отже, у такому випадку під час ідентифікації особи при здійсненні прикордонного контролю варто оперувати не «інформація про особу», а «персональні дані» відносно осіб, що перетинають державний кордон.

У діяльності ДПСУ обсяг інформації обмежений її завданнями. Під час прикордонного контролю необхідно встановити та визначити наявність законних підстав для перетинання державного кордону особами, транспортними засобами та переміщення через нього вантажів. Це може бути два обсяги інформації: «мінімально необхідний обсяг» (що встановлюється під час контролю першої лінії) [154, п. 8 ст. 1] та «додатковий» для вивчення наявності законних підстав для перетинання державного кордону України (здійснюється під час контролю другої лінії) [154, п. 6 ст. 1]. Але у цьому Законі не визначені перелік такої інформація, тому необхідно проаналізувати його норми більш детально, на підставі чого конкретизувати його.

Під час здійснення прикордонного контролю формується База даних «Відомості про осіб, які перетнули державний кордон України» (далі – База даних осіб) відповідно до наказу Адміністрації ДПСУ «Про затвердження Положення

про базу даних «Відомості про осіб, які перетнули державний кордон України»». База даних осіб є автоматизованим банком даних відомостей про громадян України, іноземців та осіб без громадянства, зареєстрованих у пунктах пропуску через державний кордон та відповідно документів громадян України на право виїзду з України і в'їзду в Україну, у тому числі паспорта громадянина України та паспортних документів іноземців та осіб без громадянства [92, п. 3].

У додатку (Реквізити бази даних «Відомості про осіб, які перетнули державний кордон України») до п. 10 до Бази даних осіб міститься перелік інформації, яка вводиться посадовими особами підрозділів органів охорони державного кордону ДПСУ, які в установленому порядку призначені і несуть службу в прикордонному наряді «Перевірка документів». Зокрема, вводяться такі групи даних:

Дата та місце перетинання державного кордону: дата і час перетинання державного кордону; назва пункту пропуску та підрозділу ДПСУ; ділянка державного кордону; напрямок перетинання (в'їзд, виїзд, скасовано).

Відомості про особу: прізвище, ім'я; дата народження; стать; статус особи (видворений, не пропущений, біженець тощо); дія відносно особи (пропуск/ не пропуск/ передача/ затримання/ інформування/ огляд); мітка, що особа є водієм транспортного засобу (тільки в пунктах пропуску для автомобільного сполучення); дані про реєстрацію громадянина України в межах відповідної адміністративно-територіальної одиниці (місто, вулиці, будинок, квартира). Крім того, необхідно додати ще біометричні дані окремих категорій осіб (що походять з країн ризиків, у тому числі і з РФ). До яких, крім того, належать також відцифровані відбитки пальців рук, відцифроване зображення обличчя [337].

С. О. Філіппов підкреслює, що застосування біометричних технологій у найближчі роки є однією з умов ефективності інформаційного забезпечення протидії транскордонній злочинності [338, с. 111], дозволяє мінімізувати можливості вчинення окремих злочинів і зменшити рівень транскордонної злочинності [339]. О. М. Царенко та С. І. Царенко доречно вказують на важливий зв'язок біометричної ідентифікації осіб із посиленням національної безпеки у

прикордонній сфері [340]. Отже, сукупність біометричних даних сьогодні є невід'ємним елементом відомостей про особу та перспективою посилення сучасної системи прикордонної безпеки держави.

Документи: громадянство; вид, серія та номер документа; тип і номер візи; кратність візи; термін дії візи;

Особи, вписані до паспорта: імена та дати народження дітей.

Дані про поїздку: мета прибуття/вибуття; назва сторони що приймає; адреса сторони, що приймає; дата передбачуваного виїзду; пункт пропуску (пункт контролю) передбачуваного виїзду.

Сукупність перелічених даних очевидно формує «мінімально необхідний обсяг».

У Законі України «Про прикордонний контроль» закріплено, що посадові особи ДПСУ можуть вимагати від іноземців надати інші (окрім паспортних) документи, що підтверджують законність їх перебування в Україні, а саме: які підтверджують факт туристичного обслуговування, навчання, стажування, працевлаштування, лікування в Україні, бронювання або оплату житла, харчування в Україні та повернення до держави свого громадянства або постійного місця проживання, або до третьої держави (у разі необхідності – інші документи, що підтверджують мету та умови перебування в Україні) [154, п. 16 ст. 1]. У зв'язку із цим у пункті пропуску іноземці можуть надавати й іншу персональну інформацію для додаткового вивчення наявності законних підстав для перетинання державного кордону України, що утворює «додатковий» обсяг інформації. Крім того, додаткова інформація може бути отримана у ході проведення опитування.

Такі обсяги інформації виправдовують мету діяльності ДПСУ під час здійснення прикордонного контролю у пунктах пропуску через державний кордон України та відповідають належному рівню безпеки держаного кордону.

Отже, чітке визначення у законодавстві поняття «персональні дані» та деталізація його змістовного наповнення сприяє відмежуванню та чіткому розумінню всіма посадовими особами, що надають інформаційні послуги,

обробляють персональні дані меж приватного та публічного життя, що є одним зі шляхів збереження та захисту інформації про ідентифіковану особу. Крім того, для захисту персональних даних необхідно створити надійні відповідні умови та бар'єри з метою недопущення розповсюдження та витоку інформації про ідентифіковану фізичну особу, яка стала відомою під час виконання завдань посадовими особами ДПСУ.

FRONTEX відповідно до Регламенту забезпечує захист персональних даних фізичних осіб під час їх обробки в установах, органах, офісах та агентстві ЄС. Особливими положеннями щодо захисту персональних даних у практиці ЄС є те, що у зв'язку із цим у FRONTEX призначено особу, службовця із захисту персональних даних – члена персоналу, на якого покладено головне завдання забезпечення незалежного внутрішнього застосування Регламенту про захист даних. З урахуванням цього загальним принципом Агентства є обробка лише тих персональних даних, які необхідні для виконання завдань, що реалізуються в інтересах суспільства, на підставі Договорів про створення ЄС, Регламенту фінансування або під час здійснення службових повноважень, наданих агентству [341] (аналогічна норма вже впроваджена в практичній діяльності ДПСУ).

Про всі операції з обробки персональних даних повідомляється службовцю із захисту даних FRONTEX, у передбачених випадках така інформація вноситься до відповідного реєстру **(додаток И)**. Основні відомості, які до нього вносяться: підрозділ, що здійснював обробку даних, дата, підстава, мета, суб'єкти, персональні дані яких оброблялись, категорії даних, що оброблялись тощо. Ведення такого реєстру дозволяє здійснювати контроль фактів і правомірності обробки персональних даних, його доцільно впровадити і у діяльність ДПСУ щодо обробки персональних даних.

FRONTEX гарантує, що зібрана інформація у межах повноважень обробляється та/або доступна лише співробітникам Агентства, відповідальним за такі операції. У виключних випадках й лише під наглядом особисті дані надаються третім сторонам (підрядникам). Суб'єкти даних (фізичні особи, дані яких обробляються) мають право на доступ, виправлення та припинення обробки

своїх даних, якщо відповідна вимога буде надіслана на адресу Агентства [341]. Суб'єкти даних можуть у будь-який час звернутися до посадової особи із захисту даних FRONTEX або до Контролера даних, відповідального за певну операцію обробки даних. Суб'єкти даних звертаються до Європейського наглядача за захистом персональних даних (European Data Protection Supervisor).

FRONTEX має право на дуже жорстких умовах, передбачених ст. 48 Регламенту фінансування, обробляти персональні дані певних груп повернених осіб. Крім того, FRONTEX має право згідно зі статтею 47 (1) (a) Регламенту у межах фінансування обробляти персональні дані осіб, які підозрюються в причетності до сприяння незаконній міграції, торгівлі людьми або інших транскордонних злочинів, у тому числі тероризму, але лише у передбачених випадках. Якщо така обробка обумовлена інтересами суспільства (забезпеченням безпеки), виконанням покладених державою завдань на посадових осіб прикордонних органів [342].

Опитані респонденти відповіли «так» 15,2 %, що вони зазнавали порушення інформаційних прав у службовій діяльності й «ні» 84,8 %. При цьому зазначили, що у них виникала потреба у захисті персональних даних з приводу службової діяльності «так» 25,1 % і «ні» 74,9 %, але 12,1 % звертались Ви для захисту своїх персональних даних до посадових осіб ДПСУ, а 87,9 % «ні». Отже, майже половина серед опитаних військовослужбовців, у яких виникала потреба у захисті таких прав, із різних мотивів не звертались за їх захистом. Серед причин можна назвати результати відповідей на такі питання, що 58 % про функціонування Департаменту у сфері захисту персональних даних Уповноваженого ВРУ з прав людини, а 75,3 % не знають про посадову особу із захисту персональних даних у ДПСУ **(додаток В)**. Сьогодні у ДПСУ призначаються такі відповідальні посадові особи, але це, як правило, офіцери підрозділів зв'язку. На наш погляд, доцільно створити окремий відділ (у Адміністрації ДПСУ, Регіональних управліннях) та призначити посадову особу (прикордонні загони), військовослужбовці яких повинні мати юридичну освіту й забезпечувати захист персональних даних громадян, іноземців та ОБГ. У практичній діяльності виникає багато питань з

приводу «персональних даних» для з'ясування яких посадові особи ДПСУ звертаються до Уповноваженого ВРУ з прав людини, що вимагає часових та ресурсних витрат, це можна оптимізувати за допомогою фахівці із захисту персональних даних у ДПСУ.

Цікавим є також аналіз досвіду, проведений експертом з інформаційного права А. Апетик, про ефективні практики регулювання питань захисту персональних даних в Естонії [343]. В Естонське інформаційне середовище, у зв'язку зі зростанням нових електронних послуг і платформ, що з'являються в Інтернеті, було впроваджено програмне забезпеченні X-Road [344]. У 2017 році X-Road Естонія передала Україні, яка заощаджує громадянам Естонії 1 407 робочих годин щорічно та забезпечує належний захист персональних даних.

Ця система дозволяє державним органам мати доступ тільки до тих персональних даних громадян, що зберігаються в електронних реєстрах, які потрібні для надання профільних послуг. Для цього кожна людина в Естонії отримує код, який відкриває їй світ 2 595 цифрових послуг. За допомогою персонального он-лайн кабінету кожен громадянин має змогу відслідковувати всі запити на свої персональні дані і знати, хто, коли і з якою метою до них звертався. Якщо людина вважає, що запит був необґрунтованим, вона може подати скаргу в Інспекцію захисту персональних даних (Інспекція є незалежною від уряду!). При цьому співробітники інспекції мають право перевіряти всі органи державної влади на предмет дотримання правил захисту персональних даних. Також ця система X-Road дозволяє обмінюватись державним органам даними реєстрів у режимі реального часу.

Функціонування цієї системи має значні позитивні досягнення, так з моменту прийняття GDPR (Загального регламенту про захист даних) в Естонії досі ніхто не отримував штрафу за його порушення [343].

Порівняльний аналіз законодавства (ЄС та України), а також механізми його правозастосування, з приводу персональних даних та їх захисту дозволяє визначити кращі позитивні напрямки розвитку дотримання та захисту

інформаційних прав людини у будь-яких ситуаціях, зокрема й в умовах здійснення прикордонних процедур, а також діяльності ДПСУ.

Проаналізовані положення відносно поняття персональних даних, їх обсягу та захисту у законодавстві ЄС та Української держави (у контексті дослідження) дозволили визначити ті сучасні тенденції, які позитивно сприятимуть здійсненню прикордонних процедур на державному кордоні України, а саме:

необхідно на національному законодавчому рівні уточнити та закріпити поняття та обсяг персональних даних, що це є «будь-які» дані, які дозволять ідентифікувати особу;

розмежувати категорії «інформація про фізичну особу» та «персональні дані»;

впровадити у практику інформаційних відносин систему обробки персональних даних на базі програмного забезпечення X-Road (за досвідом Естонії);

розвивати впровадження структурних підрозділів із захисту персональних даних у ДПСУ, що дозволить вирішувати багато питань, пов’язаних з обігом та захистом персональних даних, посилить інститут захисту персональних даних у межах діяльності ДПСУ, зокрема й здійснення прикордонних процедур;

доцільно ввести реєстр з обробки персональних даних, що надасть можливості зміцнить захист персональних даних, забезпечить упорядкування роботи з обробки таких даних й дозволить здійснювати контроль фактів і правомірності обробки персональних даних.

3.3 Реалізація прав громадян на звернення та запит на публічну інформацію у діяльності Державної прикордонної служби України

Як ми уже з’ясували у попередніх підрозділах, відносини ДПСУ з інформаційною сферою суспільства будуються за принципом інформаційної відкритості. Дієвість цього принципу зумовлена отриманням громадянами

необхідної інформації у сфері компетенції прикордонного відомства за їх потребами й інтересами. Зрілість громадянського суспільства виявляється через активність громадян, зокрема через такі його правові форми, як право на звернення та запит на публічну інформацію. Тому невід'ємним елементом становлення та розвитку сучасного інформаційного суспільства є розширення перспективних взаємозв'язків громадян і держави. У межах діяльності ДПСУ удосконалення такого спілкування сприяє формуванню ефективного механізму комунікації з громадськістю для реалізації державної політики у сфері охорони державного кордону України. Розширення такого формату інформаційних відносин стає можливим за умови забезпечення відкритості, коли кожен отримує інформацію (у межах, визначених законодавством), яка необхідна для особистого розвитку й потреб, підвищення рівня правосвідомості, дотримання норм прикордонного законодавства, а також здійснення громадського контролю за діяльністю ДПСУ. При цьому ДПСУ отримує інформацію про діяльність підпорядкованих підрозділів, завдяки чому покращується контроль за ними, усуваються недоліки в охороні державного кордону, підвищується якість та ефективність охорони державного кордону України.

Забезпечення розгляду звернень і запитів громадян у ДПСУ належить до одного з основних напрямків діяльності – формування ефективного механізму комунікації з громадськістю для реалізації державної політики у сфері охорони державного кордону [59].

Реалізація права на звернення громадян у Державній прикордонній службі України

Сьогодні демократизація суспільства й держави невід'ємні від активної участі громадян у функціонуванні органів державної влади. Крім цього, громадяни можуть вирішувати особисті проблеми, з'ясовувати питання, відновлювати порушене право шляхом подання звернення до органів державної влади. Такі можливості позитивно відображаються в діяльності держави (влада наближу-на до народу) і в реалізації прав та свобод громадян [345, с. 56]. Недарма

право людини на звернення до органів державної влади, посадових і службових осіб цих органів закріплене в ст. 40 Конституції України [126, ст. 40].

Однією з актуальних можливостей для громадян України стало безвізове перетинання державного кордону країн ЄС. «Відкриття Європи» збільшило пасажиропотік як на виїзд, так і на в'їзд в Україну громадян України та ЄС. Нові правила та умови перетинання державного кордону країн ЄС, установлення порядку в'їзду на тимчасово окуповану територію України та виїзду з неї [155], а також інші нюанси, пов'язані із реалізацією права вільно залишати територію України [126, ч. 1 ст. 33] чи вільно повертатись в Україну її громадян [126, ч. 2 ст. 33] та іноземців, викликають багато запитань і потребують уточнень для осіб, що планують перетнути державний кордон України. Державна прикордонна служба України – орган влади, відповідальний за роботу зі зверненнями громадян з питань перетинання державного кордону України, що здійснюється шляхом запровадження кращих практик у сфері управління кордонами та виконання завдань Стратегії розвитку ДПСУ.

Звернення зумовлені потребою у спілкуванні громадян із суб'єктами влади для вирішення ними питань державного чи суспільного життя або особистих питань. Особливість таких звернень визначається специфічною роллю того суб'єкта, якому вони адресовані, тобто владними функціями державних органів [346, с. 186].

Важливим для держави і громадян є забезпечення реальних механізмів звернення до компетентних органів державної влади. З цього приводу, Б. А. Кормич підкреслює, що суб'єктивному праву на подання звернення кореспондує обов'язок органів публічної влади дати обґрунтовану відповідь на такі звернення у встановлені законом строки [25, с. 87]. У статті 5 Закону України «Про Державну прикордонну службу України» закріплено, що діяльність ДПСУ провадиться на основі дотримання прав і свобод людини і громадянина [79, ч. 1 ст. 5], одним із яких є конституційне право на звернення до органів державної влади, у тому числі і до ДПСУ. Закон України «Про звернення громадян» забороняє відмовляти у прийнятті та розгляді належно оформленого

звернення [347, ч. 1 ст. 7]. З урахуванням вимог законодавства та практичних потреб удосконалення роботи над зверненнями громадян керівництвом ДПСУ акцентується увага на актуальних питаннях, що повинні бути забезпечені у відомстві: якісний моніторинг дотримання законодавства з питань звернень громадян та їх запитів на отримання публічної інформації, їх кваліфікований, об'єктивний, усебічний і оперативний розгляд; розв'язання соціальних питань у разі звернення окремих категорій громадян (учасники бойових дій, ветерани війни та праці, особи з інвалідністю, пенсіонери-прикордонники та інші громадяни, які потребують соціального захисту та підтримки) [348, п. 3.5.1]; створити належні умови для подання письмових звернень і запитів громадян з обмеженими фізичними можливостями, розробити збірник відповідних нормативно-правових актів [348, п. 3.5.2].

Закон України «Про звернення громадян» визначає, що громадянин може звернутись до органів влади із пропозицією (зауваженням), заявою (клопотанням) і скаргою, які можуть бути викладені у письмовій або усній формі [347, ч. 1. ст. 3]. Отже, Закон закріплює два способи звернення: усно та письмово. Усне звернення викладається громадянином на особистому прийомі або за допомогою засобів телефонного зв'язку через Контактний центр, телефон «гарячої лінії» та записується (реєструється) посадовою особою [347, ч. 5. ст. 5].

Письмове звернення надсилається поштою або передається громадянином до відповідного органу, установи особисто чи через уповноважену ним особу, повноваження якої оформлені відповідно до законодавства. Письмове звернення також може бути надіслане з використанням мережі Інтернет, засобів електронного зв'язку (електронне звернення) [345, с. 57].

Усні звернення можна подавати особисто на прийомі у посадової особи ДПСУ, за допомогою засобів телефонного зв'язку через Контактний центр ДПСУ (служба «Довіра»). Особистий прийом громадян у ДПСУ здійснюють керівники структурних підрозділів у визначені дні та години. Так, наприклад, наказом Адміністрації ДПСУ від 24 січня 2018 р. № 50 АГ затверджено «Графік особистого прийому громадян, осіб для надання безоплатної первинної правової

допомоги та запитувачів на отримання публічної інформації керівництвом та керівниками структурних підрозділів Адміністрації Державної прикордонної служби України» [349]. Інформація про прийомні дні, години начальників та їх заступників регіональних управлінь, прикордонних загонів міститься на офіційних сайтах відповідних структурних підрозділів ДПСУ.

Письмові звернення у ДПСУ можуть надходити через поштовий зв'язок, листом або їх можуть принести до розташування органу чи підрозділу, до керівника якого особа звертається. У цьому разі всі письмові звернення, які надійшли до керівників ДПСУ, підлягають обов'язковій реєстрації у день їх надходження (або у перший робочий день, якщо звернення надійшло у вихідний день), відповідно до постанови КМУ від 14 квітня 1997 р. № 348, якою затверджена Інструкція з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, у засобах масової інформації [350, п. 2]. Письмове звернення може надсилатись поштою або громадянин передає його до відповідного органу, установи особисто чи через уповноважену ним особу, повноваження якої оформлені відповідно до законодавства. Використання мережі Інтернет та засобів електронного зв'язку (електронне звернення) є різновидом письмового звернення [347, ч. 6 ст. 5].

Окремою формою задоволення інформаційних потреб та реалізації інформаційних прав громадян шляхом звернення до ДПСУ є консультації з використанням електронної пошти в режимі on-line та телефонів «гарячих ліній». На думку Л. В. Гонюкової, досить дієвими формами налагодження двостороннього зв'язку із громадськістю є вироблення та реалізація державної політики через електронні консультації та «гарячі» телефонні лінії. Актуальність та ефективність цих форм зумовлені їх доступністю для громадян, а також відсутністю обмежень часовими рамками та місцем проведення. Для таких комунікацій характерне: оперативний зворотний зв'язок, дотримання анонімності, зменшення матеріальних витрат і кількості організаційних заходів [351].

Головним у функціонуванні «гарячої лінії» є отримання (опрацювання) інформації, з одного боку, громадянами про діяльність ДПСУ, особливості умов та порядку перетинання державного кордону тощо, з іншого – отримання інформації ДПСУ про події, які відбуваються на державному кордоні і належать до її компетенції. Отже, головну роль відіграє інформація, яка задовольняє інформаційні інтереси та потреби всіх суб'єктів прикордонних відносин [352].

Оперативне реагування на проблемні питання громадян і своєчасний розгляд звернень, які надходять на «гарячу лінію» ДПСУ або електронні пошти (dovira@dpsu.gov.ua і zvernennia@dpsu.gov.ua) забезпечує Контактний центр Державної прикордонної служби України (далі – Контактний центр).

Контактний центр є структурним елементом Національної системи опрацювання звернень до органів виконавчої влади [353]. Персонал Контактного центру цілодобово приймає, реєструє, передає, розглядає та реагує на інформаційні повідомлення, що надходять телефоном, на електронну пошту до служби «Довіра», надає відповіді у визначений час на запитання консультативного характеру в межах компетенції ДПСУ, опрацьовує усні звернення, викладені громадянами за допомогою засобів телефонного зв'язку за телефоном служби «Довіра», письмові звернення, надіслані поштою на адресу Контактного центру, а також усі звернення, надіслані з використанням мережі Інтернет, засобів електронного зв'язку на електронну скриньку, та звернення від Урядового контактного центру [352].

У своїй роботі Контактний центр керується Конституцією України, законами України «Про звернення громадян», «Про персональні дані», постановами КМУ «Про взаємодію органів виконавчої влади, Секретаріату КМУ та державної установи «Урядовий контактний центр»», «Деякі питання документування управлінської діяльності», «Про затвердження Інструкції з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, в засобах масової інформації» та іншими законодавчими актами. На жаль, сьогодні відсутнє положення про

відповідний Контактний центр, проект якого вже було подано на затвердження в МВС України [352].

Особисте усне звернення громадян за телефоном «гарячої лінії» забезпечує можливість вирішення проблеми чи питання в режимі реального часу, це є досить важливим, коли особа перебуває в пункті пропуску чи контрольному пункті в'їзду-виїзду та допомагає швидко вирішити проблему чи урегулювати конфліктну ситуацію. Громадяни України мають право звернутися за телефоном служби «Довіра» у межах функціональних обов'язків ДПСУ із зауваженнями, скаргами та пропозиціями, що стосуються їх статутної діяльності, заявою або клопотанням щодо реалізації своїх соціально-економічних, політичних та особистих прав і законних інтересів та скаргою про їх порушення [347, ч. 1 ст. 1].

Відповідно до ч. 3 ст. 1 Закону України «Про звернення громадян» встановлені обмеження щодо подання звернення для осіб, які не є громадянами України, вони мають право їх подавати, якщо законно знаходяться на території України [347, ч. 3 ст. 1]. Тобто коли особи, які не є громадянами України, перебувають за межами території України, вони мають право звертатись до ДПСУ лише через відповідні дипломатичні установи своєї країни, а в ДПСУ не зобов'язані приймати звернення, що надіслані особисто такими особами, за умови, що вони перебувають за кордоном [352].

У такому випадку обов'язковим елементом є встановлення місця перебування іноземця на момент подання звернення. Якщо за письмовим зверненням можливо з'ясувати місце відправлення (на конверті є інформація про відправника, населений пункт, країну, а також є відповідні відбитки поштових організацій держав), то у разі отримання в електронній формі чи телефонним зв'язком звернення встановити остаточно таке місце (в Україні чи за кордоном) неможливо [352].

Під час телефонної розмови представник Контактного центру може запитати, з якої країни телефонує особа, але відповідь не буде гарантованою, а «лише зі слів особи». Можна припустити, що іноземець, якого не пропустили на територію України, перебуваючи у пункті пропуску через державний кордон

України (який фактично є територією України), міг одразу подати звернення у будь-якій його формі. Відповідно до ч. 3 ст. 1 Закону України «Про звернення громадян» воно ніби підлягає розгляду, але у цій статті вказана ще одна умова, що під час подання такого звернення іноземець має перебувати на території України «на законних підставах» [352].

Закон України «Про правовий статус іноземців та осіб без громадянства» встановлює, що «перебування на території України на законних підставах» означає, що іноземець у встановленому законодавством чи міжнародним договором України порядку в'їхав в Україну та постійно або тимчасово проживає на її території, або тимчасово перебуває в Україні [354, ч. 7 ст. 1]. Отже, у разі відмови у в'їзді на територію України іноземцю подавати звернення особисто він не має права (може лише через дипломатичні установи своєї країни), а Контактний центр може їх не приймати. Закон України «Про прикордонний контроль» надає право іноземцю у разі відмови йому в перетинанні державного кордону України оскаржити відповідне рішення згідно із Законом України «Про звернення громадян». Але ж ми з'ясували, що таке звернення (скаргу) відповідно до ч. 3 ст. 1 «Про звернення громадян» та ч. 7 ст. 1 «Про правовий статус іноземців та осіб без громадянства» іноземний громадянин подавати особисто не має права. Отже, виникає потреба узгодження цих норм у питаннях щодо прав іноземних громадян подавати звернення, перебуваючи в пункті пропуску через державний кордон України, за умови відмови на в'їзд та законне перебування на території України. Узгодження цих норм установить однозначність у діяльності посадових осіб ДПСУ, у тому числі і в діяльності Контактного центру при прийнятті таких звернень [352].

Відповідно до ч. 7 ст. 5 Закону України «Про звернення громадян» обов'язковими елементами звернення має бути прізвище, ім'я, по батькові, місце проживання громадянина, суть порушеного питання, зауваження, пропозиції, заяви чи скарги, прохання чи вимоги. При цьому письмове звернення повинно бути підписано заявником (заявниками) із зазначенням дати. Щодо направлення

електронного звернення, зазначена норма ст. 5 Закону України «Про звернення громадян» електронного цифрового підпису не вимагає [347].

Зважаючи на такі положення, органи державної влади по-різному сприймають і застосовують ст. 5 згаданого вище Закону. Деякі органи влади (наприклад, МВС України, ДФС України) при надсиланні до них звернення вимагають направити сканований підпис, хоча при встановленні особи потрібні оригінали підписів. У ДПСУ такого підтвердження не вимагається у зв'язку з дотриманням вимог ч. 7 ст. 5 Закону України «Про звернення громадян» [352].

У випадку, коли у зверненні міститься вимога, у тому числі про надання інформації про перетинання фізичною особою державного кордону України, про наявність або відсутність стосовно фізичної особи тимчасового обмеження у праві виїзду з України, а також обмеження права в'їзду іноземцю в Україну необхідно керуватись нормами Закону України «Про захист персональних даних». Стаття 14 цього Закону зобов'язує отримання згоди від суб'єкта персональних даних щодо передачі відомостей про цю фізичну особу (поширення персональних даних) [335, ч. 1 ст. 14]. Виключенням є випадки, визначені законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини [335, ч. 2 ст. 14].

Надання такої інформації про особу ставить перед персоналом Контактного центру завдання встановити особу запитувача інформації. Сьогодні активно впроваджується електронна ідентифікація. Якщо стосовно письмових та електронних звернень законодавство, а саме механізм дій щодо порядку їх отримання, реєстрації, передачі, зберігання нормативно урегульований постановами КМУ «Деякі питання документування управлінської діяльності» [355] та «Про затвердження Інструкції з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, в засобах масової інформації» [356], то відносно сучасного засобу ідентифікації особи – електронного кваліфікованого підпису аналогічний механізм сьогодні відсутній.

Електронний кваліфікований підпис визнається електронним підписом і підтверджується електронним ключем.

Отже, прийняття Закону України «Про електронні довірчі послуги» та виникнення нових відносин, пов’язаних з електронною ідентифікацією особи, що подає звернення, обумовлює необхідність нормативного закріплення механізмів і чітких алгоритмів дій для органів влади, у тому числі для Контактного центру, у зв’язку із тим, що ці питання стосуються персональних даних, які перебувають під захистом [352].

Стаття 8 Закону України «Про звернення громадян» визначає підстави відмови у розгляді та вирішенні питань. Отже, у разі коли письмове звернення без зазначення місця проживання, не підписане автором (авторами), а також таке, з якого неможливо встановити авторство, визнається анонімним і розгляду не підлягає (окрім повідомлень, що містять інформацію про корупційні правопорушення) [347, ч. 1 ст. 8]. Якщо не виконана одна з умов, установлених до письмового звернення, такі звернення не підлягають розгляду.

У постанові КМУ «Про взаємодію органів виконавчої влади, Секретаріату Кабінету Міністрів України та державної установи «Урядовий контактний центр»» викладена дещо інша позиція щодо анонімних звернень, а саме: у разі коли заявник не називає своє прізвище, ім’я, по батькові або не надає інші відомості, звернення реєструється як анонімне і надсилається в установленому порядку органу виконавчої влади, до компетенції якого належить розгляд порушеного у ньому питання, який самостійно визначає доцільність його розгляду та вносить відповідну інформацію до бази даних [357, п. 5]. З урахуванням навантаження (у 2016 році опрацьовано – 134 864 дзвінків, у 2017 році – 154 874 дзвінків, у 2018 році – 183 269 дзвінків, у 2019 року – 142 852 дзвінків **(додаток Ж.2),** при цьому збільшення дзвінків спостерігається у період відпусток **(додаток Ж.3)** на Контактний центр, усунення пересилання між органами анонімних звернень, які згідно із законом не підлягають розгляду, що зі свого боку підвищить якість і результативність консультативної роботи тих звернень, які оформлені з дотриманням вимог законодавства. Варто зазначити, що

більшість (72–87 %) звернень та повідомлень надходять від громадян України, іноземних громадян та ОБГ, які перетинають або мають намір перетнути державний кордон України, а не від персоналу ДПСУ **(додаток Ж.4)** [352].

Робота зі зверненнями громадян, переважно забезпечує зовнішні комунікації з інформаційною сферою суспільства.

Згідно з офіційними даними ДПСУ до органів управління ДПСУ у 2019 році надійшло 29 065 звернень громадян, що на 5,2 % більше, порівняно з 2018 роком (у 2018 році – 27 634), з них:

до Адміністрації ДПСУ – 19 583 (у 2018 році – 20 162) – зменшення на 2,9 %;

до регіональних управлінь, органів охорони державного кордону та забезпечення ДПСУ – 5 614 (у 2018 році – 4 217) – збільшення на 33,1 %;

до підрозділів центрального підпорядкування – 3 868 (у 2018 році – 3 255) – збільшення на 18,8% **(додаток К.1)**.

Для порівняння з 2014 та 2015 роками до органів управління ДПСУ у 2015 році надійшло 12 061 звернення громадян, що на 11,2 % більше, порівняно з 2014 роком (у 2014 році – 10 843), з них:

до Адміністрації ДПСУ – 7 698 (у 2014 році – 7 397) – збільшення на 4,1 %;

у регіональні управління, органи охорони державного кордону та забезпечення ДПСУ – 3 656 (у 2014 році – 2 628) – збільшення на 39,1 %;

у підрозділи центрального підпорядкування – 707 (у 2014 році – 818) – зменшення на 15,6 % **(додаток К.1)**.

Згідно з офіційними даними ДПСУ до органів управління ДПСУ у 2019 році надійшло 29 065 звернень громадян, що на 5,2 % більше, порівняно з 2018 роком (у 2018 році – 27 634), з них: до Адміністрації ДПСУ – 19 583 (у 2018 році – 20 162) – зменшення на 2,9 %; до регіональних управлінь, органів охорони державного кордону та забезпечення ДПСУ – 5 614 (у 2018 році – 4 217) – збільшення на 33,1 %; до підрозділів центрального підпорядкування – 3 868 (у 2018 році – 3 255) – збільшення на 18,8% **(додаток К.1)**.

Для порівняння з 2014 та 2015 роками до органів управління ДПСУ у 2015 році надійшло 12 061 звернення громадян, що на 11,2 % більше, порівняно з 2014 роком (у 2014 році – 10 843), з них: до Адміністрації ДПСУ – 7 698 (у 2014 році – 7 397) – збільшення на 4,1 %; у регіональні управління, органи охорони державного кордону та забезпечення ДПСУ – 3 656 (у 2014 році – 2 628) – збільшення на 39,1 %; у підрозділи центрального підпорядкування – 707 (у 2014 році – 818) – зменшення на 15,6 % [358] **(додаток К.1)**.

Збільшення кількості звернень може свідчити про таке:

по-перше, про поінформованість громадян щодо їх можливостей звертатись до органів управління ДПСУ;

по-друге, про високу довіру громадян до ДПСУ у вирішенні питань, пов’язаних із перетинанням державного кордону, тощо;

по-третє, про необхідності отримання консультації у зв’язку зі змінами правил перетинання державного кордону України.

У першій половині 2020 року у зв’язку зі зменшенням пасажиропотоку пов’язаного із пандемією відмічається тенденція до зменшення звернень. Зокрема, на 28,7% зменшилася загальна кількість звернень громадян до Адміністрації ДПСУ порівняно з першим півріччям 2019 року (з 9496 – у першому півріччі 2019 року до 6772 – у першому півріччі 2020 року) [359].

Основні питання, які порушували громадяни у зверненнях у 2019 році до Адміністрації ДПСУ:

порядок перетинання державного кордону, непропуск через державний кордон тощо – 1 207 (6,1%);

надання інформації про перетинання кордону – 8 661 (44,2 %);

тимчасове обмеження права виїзду за межі України – 8 282 (42,3 %);

неправомірні дії посадових осіб – 14 (0,1 %);

неправомірні дії прикордонників – 2;

фінансове забезпечення – 549 (2,8 %);

порядок проходження служби, поновлення на службі, переведення по службі – 168 (0,9 %);

виділення санаторно-курортних путівок на лікування – 246 (1,2 %);

отримання житла, поновлення в черзі на його отримання – 148 (0,8 %);

інші питання – 285 (1,5 %) [360] **(додаток К.6)**.

З урахуванням цих статистичних показників можна визначити, що більшу частку звернень становлять питання, пов'язані із перетинанням державного кордону України, тобто пов'язані із виконанням основних завдань ДПСУ. Менше надходить звернень з приводу особистих питань від підлеглих.

Звернення громадян у діяльності ДПСУ є необхідним для забезпечення права вільного виїзду з України та в'їзду на її територію, створюються умови для надання інформації громадянам про особливості перетинання державного кордону в індивідуальному порядку та вирішення особистих питань у зв'язку із функціонуванням ДПСУ. З урахуванням проведеного дослідження можна констатувати, що в ДПСУ створені дієві механізми для реалізації конституційного права на звернення громадян, та відпрацьовуються шляхи удосконалення вирішення порушених у зверненнях питань та задоволення законних прав та інтересів громадян, але є і такі проблемні моменти які знаходяться у площині відсутності (зокрема, механізм забезпечення ідентифікації особи за електронним кваліфікаційним підписом) нормативно-правового регулювання.

Особливості правових відносини щодо забезпечення запиту на публічну інформацію, розпорядником якої є Державна прикордонна служба України

«Незнання законів не звільняє від юридичної відповідальності», – цей загальновідомий вираз є не тільки закріпленою нормою Конституції України [126, ч. 2 ст. 68], але і формулою, принципом, догмою, яка передбачає, що кожна свідома людина повинна знати вимоги законів. Володіти такою інформацією потрібно не тільки, щоб не порушувати заборони, за які передбачена відповідальність, але й для того, щоб додержуватися Конституції України та

законів України, не посягати на права і свободи, честь і гідність інших людей [126, ч. 1 ст. 68].

Така позиція закріплена в Основному Законі нашої держави, але в сучасному суспільстві існують потреби в отриманні різної інформації, пов'язаної не тільки зі знанням законодавства в широкому розумінні, але і з порядком діяльності органів державної влади та пов'язаною з ними реалізації правових можливостей, що є необхідною умовою сучасного інформаційного суспільства й утвердження демократичних засад розвитку діяльності органів державної влади. Саме тому сучасній людині необхідно знати не тільки свої обов'язки, права та свободи, порядок їх реалізації, а також володіти відомостями про функціонування державних органів влади, які повинні діяти виключно в межах чинного законодавства й інтересах своїх громадян, отримувати від них інформацію за своїми інтересами та потребами [345].

Усвідомлення недостатності наявних знань про адміністративно-правові механізми й результати діяльності ДПСУ чи забезпечення прав, пов'язаних із вільним пересуванням через державний кордон України тощо, породжує виникнення інформаційної потреби. Брак інформації для здійснення діяльності людини відображає інформаційна складова, яка характерна для всіх видів потреб людини. Виникнення та формування інформаційної потреби розпочинається в той момент, коли під впливом факторів зовнішнього і внутрішнього середовища перед людиною постає завдання, реалізація якого вимагає необхідної інформації [345].

Л. В. Коновал зазначає, що прийнято виділяти два основних типи інформаційних потреб: поточні, обумовлені притаманною людині допитливістю, які полягають у його прагненні бути в курсі всього, що відбувається у світі; конкретні (спеціальні), що відображаються у прагненні отримати інформацію, необхідну для вирішення конкретного завдання – дослідного, професійного, управлінського і т. д. [361]. Такі інформаційні потреби реалізуються відповідно до Закону України «Про доступ до публічної інформації», основною метою якого є забезпечення прозорості та відкритості суб'єктів владних повноважень і

створення механізмів реалізації права кожного на доступ до публічної інформації [97, ч. 1 ст. 2]. Одним зі шляхів забезпечення доступу до інформації є надання інформації за запитами на інформацію [97, ч. 2 ст. 5].

Надання інформації за запитами на інформацію в межах інституту доступу до публічної інформації і механізм його забезпечення є новим в теорії та практиці інформаційних правовідносин, упровадження якого пов'язано із прийняттям у 2011 р. Закону України «Про доступ до публічної інформації». Кількість опрацьованих запитів з питань публічної інформації в Адміністрації ДПСУ (2011 р. – 311, 2012 р. – 835, 2013 р. – 1 646, 2014 р. – 2 431, 2015 р. – 4 006, 2016 р. – 6 30, 2017 р. – 529, 2018 р. – 959, січень-листопад 2019 – 2 197) [360] **(додаток Л)** свідчить про вагому інформаційну потребу та зростання вимог громадян в отриманні публічної інформації у сфері діяльності ДПСУ. Новизна та високий інтерес до такої інформації обумовлюють актуальність дослідження правових відносин, пов'язаних із порядком доступу до інформації, розпорядником якої є ДПСУ.

Питання доступу до публічної інформації, зважаючи на нетривалий період (з 2011 р.) державно-правового визнання, відображені у численних наукових дослідженнях і публікаціях: Е. Е. Аблякімової, І. В. Арістової, Р. А. Калюжного, Н. П. Каменської, О. В. Копана, Б. А. Кормича, А. І. Марущака, О. Г. Марценюка, І. М. Сопілко, О. І. Яременко та інші. У цих працях розкриті окремі питання забезпечення права на доступ до публічної інформації, поняття та механізм доступу до публічної інформації, стадії адміністративного провадження щодо доступу до публічної інформації, доступ до публічної інформації з позиції забезпечення відкритості органів влади тощо. Однак специфіка правових відносин, що виникають з питань доступу до публічної інформації шляхом подання запиту, розпорядником якої є ДПСУ, залишилась поза увагою наукового аналізу.

Р. А. Калюжний, О. В. Копан та О. Г. Марценюк пояснюють необхідність постійного інформування населення про всі сторони життєдіяльності держави й оперативного сприйняття і реагування її органів на звернення і пропозиції з боку

громадян із реалізацією на практиці принципу гласності [24, с. 79]. Правовідносини, що виникають щодо реалізації права на доступ до публічної інформації, полягають у тому, що відповідному суб'єктивному праву кореспондують позитивні зобов'язання суб'єктів владних повноважень та інших розпорядників, які охоплюють питання зберігання, оприлюднення та надання інформації [24, с. 5].

Основою правового регулювання відносин, які виникають у сфері доступу до публічної інформації за запитами на інформацію, що знаходиться у володінні ДПСУ, є закони України «Про інформацію», «Про доступ до публічної інформації», наказ Адміністрації ДПСУ «Про забезпечення доступу до публічної інформації у Державній прикордонній службі України». Такі відносини виникають щодо публічної інформації, яку Закон України «Про доступ до публічної інформації» визначає як відображену та задокументовану будь-якими засобами та на будь-яких носіях інформацію, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації [97, ч. 1 ст. 1]. Дане поняття визначає межі таких правовідносин. Вони виникають щодо інформації, яка була отримана, створена під час реалізації правосуб'єктності суб'єктом влади чи якою він володіє, тобто у сфері компетенції державного органу.

З урахуванням основних функцій, які реалізує ДПСУ, її повноваження з надання публічної інформації стосуються: охорони державного кордону України з метою недопущення незаконної зміни проходження його лінії, забезпечення дотримання режиму державного кордону та прикордонного режиму; здійснення в установленому порядку прикордонного контролю і пропуску через державний кордон України та до тимчасово окупованої території і з неї осіб, транспортних засобів, вантажів, а також виявлення і припинення випадків незаконного їх переміщення; охорони суверенних прав України в її виключній (морській)

економічній зоні тощо [79, ч. 1 ст. 2] за умови, що така інформація не належить до інформації з обмеженим доступом.

Нормативно закріплено три основні критерії віднесення інформації до категорії «публічна інформація», поєднання яких є підставою для виникнення зобов'язань розпорядника щодо надання доступу до неї: належність інформації до сфери відання суб'єкта владних повноважень; матеріалізована форма представлення інформації; володіння такою інформацією суб'єктом владних повноважень [362, с. 5]. Законодавство з урегулювання доступу до публічної інформації не поширюється на відносини щодо отримання її суб'єктами владних повноважень під час здійснення ними своїх функцій, а також на відносини у сфері звернень громадян, які регулюються спеціальним законом [97, ч. 2 ст. 2]. Інструкція про порядок забезпечення доступу до публічної інформації у Державній прикордонній службі України (далі – Інструкція), затверджена наказом Адміністрації ДПСУ від 3 квітня 2012 р. № 222, крім того, визначає, що органи ДПСУ не є розпорядниками публічної інформації: стосовно інформації інших державних органів України, органів влади інших держав, міжнародних організацій; стосовно інформації, яка може бути отримана шляхом узагальнення, аналітичної обробки даних або яка потребує створення в інший спосіб [113, п. 1.4].

Е. Е. Аблякімова зазначає, що «надання доступу до публічної інформації – це відносини, що виникають між запитувачем і розпорядником публічної інформації» [362, с. 5]. Крім цього, Закон України «Про доступ до публічної інформації» називає ще одного суб'єкта відносин у сфері доступу до публічної інформації – структурний підрозділ або відповідальна особа з питань доступу до публічної інформації розпорядників інформації [97, ч. 1 ст. 12], які конкретизовані в Інструкції, а саме:

управління забезпечення діяльності Голови Державної прикордонної служби України (безпосередньо забезпечує доступ до публічної інформації в Адміністрації ДПСУ) [113, п. 2.2];

підрозділ документального забезпечення (безпосередньо забезпечує доступ до публічної інформації у регіональних управліннях, органах охорони державного кордону, загонах Морської охорони, навчальних закладах, науково-дослідних установах, підрозділах спеціального призначення та органах забезпечення ДПСУ) [113, п. 2.2];

інформаційне агентство ДПСУ (наповнює публічною інформацією офіційний веб-сайт ДПСУ) [113, п. 2.3];

директор департаменту відповідно до функціональних повноважень (приймає до розгляду запит на інформацію, що надійшов на адресу Адміністрації ДПСУ) [113, п. 3.1];

підпорядкований структурний підрозділ (уповноважений структурний підрозділ), до компетенції якого належить запитувана публічна інформація (визначається директором департаменту під час розгляду запиту на інформацію) [113, п. 3.1].

Отже, досліджувані правові відносини виникають між запитувачем інформації, з одного боку, та посадовими особами ДПСУ, що здійснюють владні управлінські функції, компетентними структурними підрозділами, що реалізують інформаційну функцію у ДПСУ, підрозділами документального забезпечення та структурними підрозділами до компетенції якого належить запитувана інформація, – з іншого [363].

Досліджувані нами інформаційні відносини носять процедурний, формалізований характер і складаються із певної послідовності дій. Право на доступ до публічної інформації реалізується через адміністративно-процедурну діяльність розпорядника такої інформації [362, с. 5] та включає такі стадії:

1. Оформлення особою запиту на інформацію та направлення (подання) його до компетентного структурного підрозділу ДПСУ. Це можна зробити усно, письмово чи в іншій формі (поштою, факсом, телефоном, електронною поштою).

Запит на інформацію про особу з бази даних «Відомості про осіб, які перетнули державний кордон України» не може бути наданий третій особі або поширений будь-яким іншим чином без письмової згоди особи, відомості про яку

занесені до Бази даних осіб, крім випадків, передбачених законами України [154, п. 22].

Існує особливість подання запиту на отримання інформації про перетинання фізичною особою державного кордону України та про наявність або відсутність стосовно фізичної особи тимчасового обмеження у праві виїзду з України або в'їзду в Україну, – тільки за письмовим запитом на інформацію (поштовим зв'язком по системі Укрпошта або особисто до громадської приймальні Адміністрації ДПСУ) [364]. Такі запити необхідно подавати особисто та/або направляти письмово (запечатане у конверт) [365].

З метою спрощення процедури оформлення письмового запиту запитувач може використати відповідну форму запиту на інформацію (міститься у додатку 1 Інструкції) або на інформацію про особу з бази даних «Відомості про осіб, які перетнули державний кордон України» (міститься у додатку 2 Інструкції), що подається фізичними, юридичними особами й об'єднаннями громадян без статусу юридичної особи [113, п. 2.5]. Тобто в ДПСУ встановлено дві форми запиту.

2. Отримання та реєстрація запитів на інформацію.

Отримання запитів на інформацію на особистому прийомі здійснюється через громадські приймальні посадовими особами, що здійснюють особистий прийом громадян [113, п. 2.8].

Запити на інформацію, що надійшли на адресу органів ДПСУ, приймаються, реєструються підрозділом документального забезпечення, до обов'язків яких належить безпосереднє забезпечення доступу до публічної інформації, та подаються на розгляд начальникам цих органів, якими визначається уповноважений структурний підрозділ, до компетенції якого належить запитувана публічна інформація [113, п. 3.2]. Реєстрація запитів на інформацію здійснюється в автоматизованій системі електронного документообігу або в журналах реєстрації запитів на інформацію [113, п. 3.4].

При цьому залишається незрозумілим, яким чином фіксуються запити під час особистого прийому? Оскільки ні в Законі України «Про доступ до публічної інформації», ні в Інструкції цього не зазначено. Автори Науково-практичного

коментаря до Закону України «Про доступ до публічної інформації» також зазначають, що усна форма запиту процедурно є найскладнішою на етапі прийому, оскільки відсутня чітка фіксація самого запиту запитувачем. З огляду на це при прийомі такого запиту відповідальним працівником останній має перенести його зміст у документальну (текстову) форму, яка дозволить опрацьовувати запит у подальшому. Тобто необхідно у процесі спілкування із запитувачем зафіксувати у внутрішньому документі розпорядника ім'я (найменування) запитувача, контактні дані для зворотного зв'язку, опис запитуваної інформації чи документа. Доцільно, щоб спілкування із запитувачем при отриманні усних запитів проводилося відповідальною особою з питань запитів або працівником відповідного структурного підрозділу, оскільки такі працівники є найбільш компетентними в питаннях розрізнення запитів від звернень або інших форм взаємодії приватних суб'єктів із розпорядником, вимог до змісту запиту тощо [366, с. 259].

Закон України «Про доступ до публічної інформації» визначає, що запит на інформацію має містити: ім'я (найменування) запитувача, поштову адресу або адресу електронної пошти, а також номер засобу зв'язку, якщо такий є; загальний опис інформації або вид, назву, реквізити чи зміст документа, щодо якого зроблено запит, якщо запитувачу це відомо [97, ч. 5 ст. 19].

Ще один елемент, але він стосується письмової форми подання запиту: підпис і дату [97, ч. 5 ст. 19], але вражаємо, що для дотримання належного порядку роботи із запитами на публічну інформацію під час особистого прийому доцільно вести окрему графу підпису заявника, щоб така особа була впевнена в прийнятті її звернення відповідно до змісту її запиту.

У зв'язку із тим, що пункти постійної дислокації органів ДПСУ є режимними об'єктами, а інформація, яку запитує особа може мати персональний характер для усного звернення потрібно встановити особу. Тому необхідно зазначити в Інструкції, що при зверненні для отримання запиту на інформацію на особистому прийомі обов'язкова наявність документа, що посвідчує особу [363].

3. Опрацювання запитів на інформацію. Для надання компетентної відповіді розпорядника інформації визначається підпорядкований структурний підрозділ, до компетенції якого належить запитувана публічна інформація. Залежно від характеру запитуваної інформації розгляд запиту може бути до 48 годин, до 5 і 20 робочих днів [97, ст. 20].

Відповідь на запит надається уповноваженим структурним підрозділом органу ДПСУ за вказаними запитувачем публічної інформації адресою, номером засобу зв'язку та формою: листом, у вигляді електронного документа, засобами факсимільного зв'язку чи усно за телефоном [113, п. 5.1]. Проект листа з відповіддю на запит на інформацію підлягає обов'язковому погодженню з підрозділами правового забезпечення та режиму і захисту інформації [113, п. 5.9].

Відповідь у задоволенні запиту на інформацію може мати як позитивний (задоволено), так і негативний (відмовлено) характер для запитувача. Відмова в задоволенні запиту може бути в таких випадках: орган ДПСУ не володіє і не зобов'язаний відповідно до його компетенції, передбаченої законодавством, володіти інформацією, щодо якої зроблено запит; інформація, що запитується, належить до категорії інформації з обмеженим доступом; особа, яка подала запит на інформацію, не оплатила фактичні витрати, пов'язані з копіюванням або друком; не дотримано вимог до оформлення запиту на інформацію [113, п. 5.5]. Мотивована відмова в задоволенні запиту на інформацію надається в письмовій формі.

4. Оскарження. Рішення, дії чи бездіяльність органів ДПСУ можуть бути оскаржені до Голови ДПСУ, вищого органу або суду. Запитувач має право оскаржити: відмову в задоволенні запиту на інформацію; відстрочку задоволення запиту на інформацію; ненадання відповіді на запит на інформацію; надання недостовірної або неповної інформації; несвоєчасне надання інформації; інші рішення, дії чи бездіяльність органів ДПСУ, що порушили законні права та інтереси запитувача [363].

Проаналізований звіт про зареєстровані запити в Адміністрації ДПСУ надає інформацію щодо загальної їх кількості, що не відображає повної інформації про

роботу відомства у цьому напрямку для широкого загалу. Тому доцільно конкретизувати та відобразити у цих звітах такі дані: загальну кількість отриманих запитів, у тому числі за окремими суб'єктами (громадяни, юридичні особи, громадські організації, ЗМІ); за формою отримання запиту (особисто на прийомі, письмово, поштою, телефоном, електронною поштою); результати розгляду (інформацію надано, надіслано за належністю, відмовлено, продовжено термін, знаходиться на опрацюванні) [363].

З урахуванням сфери діяльності ДПСУ у напрямку задоволення запиту на публічну інформацію правові відносини характеризуються такими особливостями: по-перше, особливості процедури надання доступу до публічної інформації регулюються внутрішньовідомчим наказом – Інструкцією про порядок забезпечення доступу до публічної інформації у ДПСУ; по-друге, в Інструкції конкретикзовано структурні підрозділи ДПСУ (відповідальна особа) з питань доступу до публічної інформації; по-третє, для спрощення порядку оформлення письмового запиту визначені дві форми запиту: запит на інформацію і на інформацію про особу з бази даних «Відомості про осіб, які перетнули державний кордон України»; по-четверте, виключно письмова форма подання запиту на інформацію встановлена для інформації, яка регулюється Законом України «Про захист персональних даних», а саме: перетинання державного кордону України громадянами; можливе існування стосовно громадянина тимчасового обмеження у праві виїзду за кордон; можливе існування стосовно іноземця та особи без громадянства рішення про заборону в'їзду [345].

Отже, дієвість прав громадян на звернення та запит на публічну інформацію є формами реалізації інформаційних прав у прикордонній сфері. Механізми обробки та захисту цих прав у ДПСУ намагаються наблизити до вимог сучасного інформаційного суспільства й стандартів ЄС, але динамічний характер інформаційних відносин, а також мінливість загроз прикордонній безпеці потребують його постійного удосконалення. Актуальним сьогодні є питання формування нормативно-правового підґрунтя та адаптація у практичній діяльності органів ДПСУ механізму ідентифікації особи за електронним

кваліфікаційним підписом, зокрема порядок прийняття, зберігання, підтвердження, передача звернень із таким підписом компетентній особі ДПСУ для розгляду, надання відповідних повноважень посадовим особам.

Висновки до розділу 3

Інформаційні відносини у діяльності ДПСУ відбуваються у постійній, безперервній комунікації з інформаційною сферою суспільства, у межах правового простору обігу інформації у сфері охорони державного кордону. З урахуванням предмета нашого дослідження визначено, що під «інформаційною сферою суспільства» необхідно розглядати, урегульовані національним законодавством інформаційні відносини, інформаційні повноваження, сукупність інформаційних ресурсів ДПСУ, які дозволяють реалізувати інформаційні права, інтереси та потреби громадян, суспільства, органів і підрозділів ДПСУ у сфері охорони державного кордону.

Інформаційна сфера суспільства в діяльності ДПСУ конкретизована через суб'єктну складову (компетентні структурні підрозділи й посадові особи уповноважені здійснювати комунікацію з суспільством, громадськістю та громадянами), а також суб'єкти приватного права (фізичні особи), що реалізують свої особисті інтереси у сфері охорони державного кордону (перетинають або мають намір перетнути державний кордон України, висловлюють відповідно до законодавства потребу у сприянні, задоволенні чи захисті інформаційних прав) та предметну складову (межі відомчих повноважень ДПСУ – сфера охорони державного кордону України).

Основною засадою комунікації ДПСУ з інформаційною сферою суспільства є реалізація принципу відкритості перед громадянами, що є пріоритетом державної політики в інформаційній сфері, закріпленою Доктриною інформаційної безпеки України, та становить вимогу керівництва ДПСУ. Комплексний аналіз інформаційної відкритості у діяльності ДПСУ дозволяє

виокремити такі її елементи: нормативно врегульований механізм забезпечення отримання інформації про діяльність прикордонного відомства та його структурні підрозділи; стан забезпечення реалізації прав громадян на інформацію у прикордонній сфері; прозорі способи оприлюднення інформації у прикордонній сфері через доступні процедури; простота та доступність електронного урядування у ДПСУ; визначення змісту інформації, яка підлягає оприлюдненню, а отже і її чітке розмежування на інформацію, що може бути доведена до всіх (публічна відкрита); стосується окремої особи (конфіденційна); чи групи осіб або безпеки держави (службова чи таємна), які результати діяльності та дії посадових осіб ДПСУ підлягають оприлюдненню; рівень інформаційної культури персоналу ДПСУ.

Вимогою сучасного інформаційного суспільства є дотримання приватності як однієї з основ розвитку демократизації. Приватність у діяльності ДПСУ зумовлена дотриманням меж приватного життя, зокрема отримання, обробка та захист тільки тієї інформації про громадян, що необхідна для виконання завдань. Виявлені прогалини та запропоновані нормативні й організаційні рішення з питань: необхідності формулювання мети обробки персональних даних; фіксації отримання згоди на обробку персональних даних під час прикордонного контролю; упровадження структурних підрозділів із захисту персональних даних у ДПСУ; ведення реєстру з обробки персональних даних у ДПСУ; розмежування персональних даних, необхідних для прикордонного контролю на «мінімально необхідний» і «додатковий» обсяг; упровадження у практику інформаційних відносин Естонську систему обробки персональних даних на базі програмного забезпечення X-Road.

Організаційні засади відносин ДПСУ з інформаційною сферою суспільства набувають реальних форм через інститути звернення та запиту на публічну інформацію. У діяльності ДПСУ їх механізм наближений до вимог сучасного інформаційного суспільства і стандартів ЄС. Разом з тим динамічний характер інформаційних відносин, а також мінливість загроз прикордонній безпеці потребують його постійного удосконалення. Серед актуальних питань його

поліпшення виділено необхідність формування нормативно-правового підґрунтя та адаптація у практичній діяльності органів ДПСУ механізму ідентифікації особи, яка подає запит на інформацію за електронним кваліфікаційним підписом, зокрема порядок прийняття, зберігання, підтвердження, передача звернень із таким підписом компетентній особі ДПСУ для розгляду, надання відповідних повноважень посадовим особам.

РОЗДІЛ 4
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДІЯЛЬНОСТІ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

4.1 Аналіз та оцінка сучасних інформаційних загроз у діяльності Державної прикордонної служби України

Важливим та першочерговим фактором стану безпеки у будь-якій галузі є оцінювання реальних та потенційних загроз, оскільки складовою національної й державної безпеки є захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру [158, п. 4, п. 9 ст. 1]. Неодмінним складовим елементом державної політики у сфері національної, державної та прикордонної безпеки є забезпечення інформаційної та кібербезпеки України [158, ч. 4, ст. 3].

Інформаційні загрози у прикордонній сфері завжди були, є і будуть, вони змінюються з удосконаленням прикордонних та інформаційних відносин, а завдання ДПСУ полягає у тому, щоб реально оцінювати існуючі та передбачати майбутні небезпеки, у зв’язку із цими обставинами планувати подальшу діяльність щодо їх попередження, недопущення та своєчасного усунення [367, с. 147]. Як справедливо підкреслює І. Ф. Корж, виклики, небезпеки, загрози «неможливо повністю нейтралізувати чи усунути», але можна враховувати «рівень впливу на оточуюче середовище та масштаби наслідків цього впливу» [163].

Недооцінювання чи ігнорування інформаційних загроз може призвести до серйозних проблем та прогалин у цілісній системі прикордонної безпеки, адже інформаційна складова як інтегроване явище відіграє одну із фундаментальних ролей. З цього приводу О. Є. Цевельов зазначає, що до втрати контролю над ділянкою українсько-російського державного кордону (у Донецькій та частково в

Луганській областях), та анексія РФ АРК, спричинила розв'язана РФ «гібридна» війна, що супроводжується здійсненням повного спектра спланованих і скоординованих воєнно-політичних заходів, спрямованих на дестабілізацію політичної, економічної та гуманітарної ситуації в Україні, розвитком сепаратизму, терористичних виявів і загроз їх поширення вглиб її території [169, с. 31]. Отже, у результаті своєчасно невиявленої та неочікуваної інформаційної загрози з боку РФ, а також відсутність відповідної протидії їй стала втрата частини української території (Автономна Республіка Крим, частина Донецької та Луганської областей). Інформаційні загрози наносять 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 й імідж прикордонного відомства тощо [367, с. 147].

У ДПСУ вже вдруге розробляється система орієнтирів розвитку ДПСУ із урахуванням існуючих потреб і загроз у прикордонній сфері. Першою була Концепція розвитку Державної прикордонної служби України на період до 2015 року затверджена Указом Президента України від 19 червня 2006 р. Дана Концепція запровадила реформування у напрямку європейських стандартів і відкритості в охороні державного кордону України, розширення формату інформаційного забезпечення, а саме:

завершення розгортання системи цифрового зв'язку, запровадження новітніх технологій і переоснащення відділів прикордонної служби сучасними засобами радіозв'язку;

запровадження в діяльність органів і підрозділів автоматизованих інформаційних систем, у тому числі з опрацювання електронних зображень і дактилоскопічних даних із використанням геоінформаційних технологій, та інтегрування їх у єдину інформаційну телекомунікаційну систему ДПСУ, інших правоохоронних органів України;

переоснащення органів і підрозділів сучасною комп'ютерною технікою та відповідними програмними продуктами, створення мережі передачі даних;

розвиток інформаційно-аналітичної діяльності у напрямку вдосконалення інформаційного забезпечення як керівництва ДПСУ, так і її органів і підрозділів під час виконання завдань з охорони державного кордону;

створення спеціалізованих аналітичних центрів і підрозділів для опрацювання інформації;

здійснення комплексу заходів щодо запровадження системи управління ризиками [368].

Основними загрозами на момент прийняття згаданої вище Концепції були: транскордонна організована злочинність у сфері незаконної міграції, торгівля людьми, незаконне переміщення через державний кордон зброї та інших засобів терору, товарів військового призначення і подвійного використання, наркотичних засобів, психотропних речовин і прекурсорів, радіоактивних речовин, вантажів та іншого майна [368]. У такому разі загрозу становить своєчасне невиявлення, а також приховування інформації про наміри, способи та характер правопорушення, виток чи передача інформації про оперативно-службову діяльність прикордонних підрозділів, яку можуть використати зловмисники для своїх протиправних цілей.

Концепцією розвитку ДПСУ на період до 2015 року було створено підґрунтя для формування окремого напрямку інформаційної діяльності у ДПСУ – аналізу ризиків. Така діяльність сьогодні становить сукупність процедур і методів обробки інформації з метою визначення наявних, потенційно можливих ризиків у сфері безпеки державного кордону, а також є невід'ємною складовою інтегрованого управління кордонами [369]. Аналіз та оцінка сучасних інформаційних загроз у прикордонній сфері враховуються під час планування та організації оперативно-службової діяльності з урахуванням конкретних особливостей кожного органу (підрозділу) охорони державного кордону [370]. Проводиться стратегічний аналіз ризиків, під час якого обов'язково здійснюється оцінка загроз (визначаються зовнішні та внутрішні фактори, які негативно впливають на сферу безпеки державного кордону), оцінка вразливості та визначається спроможність органів і підрозділів охорони державного кордону

(аналізуються складові частини системи охорони державного кордону, а також фактори, що притягують загрозу), оцінка впливу (визначаються наслідки реалізації загрози для сфери безпеки державного кордону, у тому числі наслідки, що впливають на пропуск через кордон осіб, транспортних засобів, вантажів, а також інших сфер національної безпеки тощо), а також визначаються рівень ризиків та їх прогноз [370, п. 4].

Наступним нині чинним програмним документом стала Стратегія розвитку Державної прикордонної служби України, яка переорієнтована на нові види загроз, таких як: військова агресії РФ проти України, тимчасова окупація нею території АРК і м. Севастополя, розпалювання збройного конфлікту в східних регіонах України, що супроводжується здійсненням заходів, спрямованих на дестабілізацію політичної та економічної ситуації в Україні, розвиток тероризму та загроза його поширення територією України [59]. Але небезпека транскордонної злочинності та нелегальної міграції тощо, які були визначальними загрозами у Концепції розвитку ДПСУ на період до 2015 року, і сьогодні залишаються актуальними.

Перелічені у Стратегії загрози військового характеру й активізація тероризму має переважно локальний характер на ділянках кордону Донецької та Луганської областей. При цьому способи та засоби агресії РФ проти України із застосування інформації як одного із засобів розв’язання та утримання конфлікту не тільки на теренах усієї території України, її прикордонних регіонів, але і на міжнародній арені, визначає актуальність дослідження інформаційних загроз у прикордонній сфері як складової забезпечення національної та державної безпеки.

У зв’язку із цим справедливо зазначили О. О. Золотар та І. О. Трубін, що «окремим предметом наукових дискусій є питання щодо безпеки та захищеності відносин, пов’язаних зі збором, обробкою, зберіганням й використанням інформації». А з урахуванням співвідношення понять: «безпека» – «загроза», «захищеність» – «загроза» можна розглядати її як потенційну небезпеку, – будь-які дії чи події, що можуть настати за різних обставин у

навколишньому середовищі та стати передумовою порушення безпеки і завдання збитків [371, с. 106].

У чинному Законі України «Про національну безпеку України» змістовне відображення інформаційних загроз має бланкетний характер: «Стратегія національної безпеки України – документ, що визначає актуальні загрози національній безпеці України…» [158, п. 19 ст. 1]. Для порівняння у попередньому Законі України «Про основи національної безпеки України», що втратив чинність, окремо у ст. 7 закріплювались такі основні реальні та потенційні загрози національній безпеці України в інформаційній сфері:

вияви обмеження свободи слова та доступу до публічної інформації;

поширення засобами масової інформації культу насильства, жорстокості, порнографії;

комп'ютерна злочинність та комп'ютерний тероризм;

розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави;

намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [372, ст. 7].

У Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 р. № 392/2020, серед актуальних загроз національній інформаційній безпеці України визначено:

ведення інформаційної війни проти України, діяльність спецслужб іноземних держав, розвідувально-підривна діяльність ,зокрема РФ; відсутність цілісної інформаційної політики держави [373, п. 19, 20];

щодо загрози кібербезпеці і безпеці інформаційних ресурсів: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак [373, п. 27].

Отже, з розвитком інформаційних систем і технологій відокремлюються загрози, пов'язані з уразливістю зберігання, обробки й передавання інформації в інформаційно-комунікаційних системах. При цьому у чинному законодавстві

(зокрема, у Стратегії національної безпеки України) не згадується про загрози в інформаційній сфері щодо обмеження свободи слова, доступу до публічної інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; розголошення інформації з обмеженим доступом.

Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації, саме це обумовило прийняття Радою національної безпеки і оборони України – Доктрини інформаційної безпеки України (далі – Доктрина інформаційної безпеки) [148], яка визначила національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері.

Отже, наступним нормативно-правовим актом, що розширює перелік загроз в інформаційній сфері, є Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 р., у якій загрози безпосередньо пов’язані із цілеспрямованим небезпечним впливом РФ проти України. Використання РФ технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства шляхом використання найновіших інформаційних технологій впливу на свідомість громадян, спрямовану на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України [148]. Такі загрозливі дії насамперед відчувають і повинні своєчасно виявляти та уміло їм протистояти прикордонники на суміжних із РФ ділянках державного кордону України.

Зокрема у Доктрині інформаційної безпеки актуальними загрозами національним інтересам і національній безпеці України в інформаційній сфері визначено:

здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу ЗС України та інших

військових формувань, провокування екстремістських виявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

проведення державою-агресором (РФ) спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

інформаційне домінування держави-агресора на тимчасово окупованих територіях; недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіакультури суспільства; поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [148].

Інформаційні загрози у чинних нормативно-правових актах мають зовнішній характер та є серйозним викликом для нашої держави, визначають необхідність нормативно-правового й організаційного удосконалення інформаційної безпеки на сучасному етапі розвитку інформаційного суспільства, також ці загрози вказують на уразливі елементи національної інформаційної сфери.

Отже, ми маємо два чинних нормативних документи: Стратегію національної безпеки України та Доктрину інформаційної безпеки, у яких визначені інформаційні загрози. Зокрема, у Стратегії національної безпеки України стисло вказується на загрози як внутрішнього, так і зовнішнього

характеру, а у Доктрині інформаційної безпеки деталізовано більше на зовнішніх. Але, на наш погляд, загальну загрозу становить неспроможність можливостей державного характеру упереджувати, своєчасно виявляти та протистояти будь-яким загрозам. Тобто необхідно створити такі умови, щоб інформаційні загрози не змогли негативно (протиправно) вплинути та порушити національну, державну та прикордонну безпеку. У зв'язку із цим необхідна загальнодержавна програму розвитку інформаційного суспільства в Україні, яка повинна була бути розроблена та подана КМУ до ВРУ на 2016–2020 роки [374], що досі не було зроблено, а також систематизувати інформаційне законодавство, про що неодноразово наголошувалось у наукових працях [231, с. 164–165; 375, с. 178; 376, с. 66; 377, с. 6; 378, с. 23].

Для детального аналізу предмета нашого дослідження необхідно з'ясувати генезис та різноманітність загроз інформаційній безпеці в доктрині інформаційного права.

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 для кого-, чого-небудь; те, що може заподіювати яке-небудь зло, якусь неприємність [43, с. 387]. О. О. Золотар та І. О. Трубіна зауважують, що інформаційні загрози створюють інформаційну небезпеку, яка поширюється в інформаційному просторі [371, с. 107]. Інформаційні загрози породжують інформаційну небезпеку або посягають на безпеку, установлений правовий порядок обігу інформації. При цьому небезпека зумовлює можливість якогось лиха, нещастя, якоїсь катастрофи і т. ін., стан, коли кому-, чому-небудь щось загрожує [379]. 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 виявами одного більш широкого поняття – загрози національним інтересам та національній безпеці в

інформаційній сфері [380], коли безпека є стан захищеності та відсутності інформаційних загроз.

Інформаційні загрози безпеці держави розглядають як сукупності 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 [381, с. 89]. Отже, інформаційні загрози знаходяться серед площин 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 [367, с. 148].

В. О. Олійник у своєму дисертаційному дослідженні зазначає, що інформаційна безпека, яка є складовою національної безпеки в узагальненому вигляді, ґрунтується на таких базових елементах: національні інтереси – загроза – захист [267, с. 8].

О. О. Золотар запропонувала більш 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 [382, с. 4–5]. Вважаємо, що необхідно комплексно й системно підходити до інформаційних загроз і визначення їх місця у системі інформаційних відносин, з урахуванням інформаційних потреб у сфері охорони державних кордонів у сучасному інформаційному суспільстві. Така система повинна бути втілена у чіткому нормативному регулюванні інформаційної діяльності, зокрема органів влади, механізмів задоволення інформаційних вимог усіх суб'єктів інформаційних відносин, а також установлення відповідних дієвих заходів впливу до осіб, що порушують інформаційну безпеку. Отже, 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 [367, с. 148].

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 прикордонної. Саме тому система загроз інформаційній безпеці має комплексний, системний характер і містить загрози безпеці інформації та інформаційної інфраструктури; 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 [383, с. 183]. При цьому джерелами загроз можуть бути людина, технічні пристрої, моделі, алгоритми, програми; технологічні схеми обробки; зовнішнє середовище тощо [384, с. 67].

Н. А. Савінова вказує на існування таких новітніх суспільно небезпечних інформаційних загроз, як: кібернетична інтервенція (агресивні дії у кіберпросторі) [385, с. 303]; інформаційна експансія (умисне захоплення з метою подальшого використання на свою користь інформаційного простору, інформаційна війна) [385, с. 307]; умисний вплив на свідомість населення з метою спонукання індивідів (певної групи) до участі в екстремістських діях – кібернетичний екстремізм, а також умисні впливи на свідомість населення з метою залучення осіб в участь у сумнівних релігійних та фінансових утвореннях – втягнення населення у релігійні (фінансові) структури з використанням ЗМІ [385, с. 315].

Найбільш повно розкрити інформаційні загрози у досліджуваній сфері можуть підходи до видів загроз, сформульовані у доктрині інформаційного права:

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 (право на виробництво інформації, її поширення,

пошук, одержання, передавання та використання; право на інтелектуальну власність на інформацію, у тому числі й речову) [386];

дані навмисно перехоплюються, читаються або змінюються; користувачі ідентифікують себе неправильно (з шахрайською метою); користувач отримує несанкціонований доступ з однієї мережі до іншої [387, 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 [388, 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 [389, 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) [390, с. 8];

випадкові загрози: помилки обслуговуючого персоналу і користувачів; втрата інформації внаслідок неправильного її збереження; випадкове знищення або заміна; збій у роботі устаткування, електроживлення, дискових систем, комплектуючих елементів мережі; некоректна робота програмного забезпечення, зокрема внаслідок зараження комп'ютерними вірусами тощо [391, с. 46–47];

навмисні загрози: несанкціонований доступ до інформації і мережевих ресурсів; розкриття і модифікація даних і програм, їх копіювання; розкриття, модифікація або підміна трафіка обчислювальної мережі; розробка і поширення комп'ютерних вірусів, введення в програмне забезпечення логічних бомб;

крадіжка магнітних носіїв і розрахункових документів; руйнування архівної інформації або навмисне її знищення; фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому; перехоплення та ознайомлення з інформацією, яка передана по каналах зв'язку [392, с. 50].

Усебічно дослідивши державне реагування на загрози національній безпеці у сфері безпеки державного кордону України, О. Є. Цевельов зазначає, що реальними та потенційними загрозами для безпеки державного кордону сьогодні є: намагання змінити лінію державного кордону України або відторгнути частину її території; прикордонні конфлікти, озброєні та неозброєні провокації; незаконне перетинання державного кордону великою кількістю прикордонного населення через виникнення регіональних або прикордонних конфліктів; незаконне ввезення чи вивезення зброї, боєприпасів, вибухових речовин і засобів масового ураження, радіоактивних і наркотичних речовин, вантажів без митного та інших видів контролю, екологічно небезпечних технологій, речовин і матеріалів; незаконне ввезення літератури та магнітних носіїв, що мають зміст антидержавного, терористичного, сепаратистського, націоналістичного і екстремістського напряму; перетинання державного кордону поза пунктами пропуску; використання підроблених, недійсних, чужих паспортних документів або їхня відсутність під час перетинання державного кордону в пунктах пропуску [392, с. 161].

Крім того, виділяє науковець і інші загрози: неможливість або протидія виконанню законних функцій ДПСУ через незавершеність договірно-правового оформлення державного кордону та його недостатнє облаштування; зміна проходження лінії державного кордону, руйнування об'єктів ДПСУ, забруднення її території через надзвичайні події природного та техногенного характеру; незаконне втручання в діяльність ДПСУ, використовуючи технічні засоби прослуховування та спостереження, напад на об'єкти чи персонал з метою оволодіння зброєю, технікою, майном; діяльність злочинних угруповань на державному кордоні та в межах прикордонних районів тощо [392, с. 162]. Такі загальні загрози для безпеки державного кордону прямо чи опосередковано породжують інформаційні загрози у цій сфері.

Загрози національній безпеці України на державному кордоні М. Плахотний пропонує класифікувати за такими різноманітними критеріями, що відображають ступінь їх небезпеки:

сферою діяльності: політичні, економічні, соціальні, військові, міжнаціональні, екологічні, демографічні, науково-технічні, технологічні, інформаційні тощо;

місцем знаходження джерела загрози: внутрішні та зовнішні; масштабом: загальнодержавні, локальні та часткові; імовірністю та часом реалізації: реальні та потенційні [153, с. 106]. При цьому науковець визначає, що серед основних зовнішніх загроз на державному кордоні, що здійснює негативний зовнішній вплив на інформаційний простір України, є передача через державний кордон антиукраїнських інформаційних матеріалів [153, с. 107].

Крім інформаційних загроз спрямованих безпосередньо проти безпеки державного кордону, існують загрози опосередкованого характеру. Найчастіше сьогодні використовується дезінформація, обман, втягування, схиляння військовослужбовців ДПСУ до дій в інтересах супротивника. Так, в кінці травня 2020 року з’явилось повідомлення про те, що агентура управління прикордонної служби ФСБ РФ по Брянській області активізувала роботу по залученню до провокацію співробітників ДПСУ. Представники російських спецслужб намагалися налагодити тісний контакт відразу з декількома українськими прикордонниками з метою виманити останніх на зустрічі безпосередньо на російсько-українському кордоні або території суміжної держави з метою подальшого викрадення і відповідної «обробки» для отримання інформації, яку використовують в пропагандистських цілях [393].

Отже, розглянута видова різноманітність інформаційних загроз та їх критичний аналіз дозволив сформувати власну, характерну для діяльності ДПСУ, класифікацію загроз такими критеріями:

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

інформації); внутрішньовідомчі (витікання інформації через персонал ДПСУ або суб'єктів інтегрованого управління кордонами);

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, охорона та захист інформації;

за характером вияву: відомчі (посягають на прикордонну безпеку держави), корпоративні (зазіхають на безпеку окремого підрозділу), особисті (відносно окремих військовослужбовців чи 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 їх тактики та способів дій, щоб у подальшому планувати порушення прикордонного законодавства чи здійснення диверсійних операцій); стихійні лиха (пожежі, повені тощо) [367, с. 149].

Інформаційні загрози у діяльності ДПСУ – це фактори, які утворюють небезпеку чи заподіюють шкоду інформаційним відносинам, інформаційним правам, інформаційним ресурсам ДПСУ та посягають на прикордонну безпеку. Отже, нами встановлено, що інформаційні загрози в діяльності ДПСУ мають комплексний характер і створюють небезпеку прикордонній безпеці як складовій державної інформаційної безпеки. Поняття «загроза» є спорідненим із поняттям «небезпека», яка створює умови заподіяння або реально заподіює шкоду не лише інформаційним відносинам, 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 правової охорони та захисту інформації набуває неабиякої актуальності й важливості у діяльності ДПСУ та є перспективним для наступних підрозділів нашого дослідження.

4.2 Правові засоби охорони інформаційних відносин у функціонуванні Державної прикордонної служби України (кримінальна, адміністративна, дисциплінарна та цивільно-правова відповідальність)

Збереження та захист інформації як об'єкта інформаційних відносин сьогодні є досить важливими питаннями державно-правової сфери, особливо коли йде мова про діяльність органів публічної адміністрації, які є розпорядниками інформації у ввіреній їм державою і громадянами (як реалізація безпосередньої демократії) сфері правового регулювання. Державна прикордонна служба України здійснює інформаційну діяльність в інтересах охорони державного кордону та реалізації права кожної людини, пов'язаного з вільним перетинанням державного кордону [223, с. 166].

Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України [57, ч. 1 ст. 27]. Отже, право на інформацію є об'єктом правової охорони. Дослідження особливостей окремого виду юридичної відповідальності за порушення норм інформаційного законодавства, охорона та захист інформації є міжгалузевим інститутом системи галузі інформаційного права [14, с. 204]. Як справедливо зазначає О. О. Тихомиров, «інститут юридичної відповідальності є фундаментальним правовим засобом, механізмом, гарантом, який покликаний забезпечувати регулятивну й охоронну дієвість права, дуже необхідну сьогодні в інформаційному житті українського суспільства» [394, с. 37].

Отже, нормативно закріплено та теоретично обґрунтовано, що інформація, правові відносини, які виникають, змінюються та припиняються на підставі конкретних відомостей, а також інформаційна правоздатність суб'єктів у визначеній сфері перебувають під державно-правовою охороною та захистом, одним із заходів забезпечення якої, поряд із технічними, організаційними та режимними заходами, є встановлення юридичної відповідальності. Це, безперечно, стосується правових відносин, об'єктом яких є інформації, а однією зі сторін ДПСУ або військовослужбовці (працівники) ДПСУ.

Важливо не лише встановити відповідальність, але й забезпечити знання кожного військовослужбовця про юридичні наслідки невиконання норм інформаційного законодавства, так опитані військовослужбовці коливались у відповідях на питання «Який вид юридичної відповідальності передбачено за незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових повноважень?» 61,5 % відповіли кримінальна, 27,7 % адміністративна, 10,4 % дисциплінарна, 0,4 % цивільна. Отже, менше 30 % респондентів знають, що за такі дії передбачена адміністративна відповідальність. На запитання «Який вид юридичної відповідальності передбачено за несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї?» були отримані такі відповіді: 65,7 % – кримінальна, 23,4 % – адміністративна, 10 % – дисциплінарна, 0,9 % – цивільна **(додаток В)**.

Кримінально-правові засоби охорони інформації у сфері діяльності ДПСУ

Діяльність ДПСУ охоплює різноманітні зовнішні та внутрішні напрямки у межах охорони державного кордну й організації повсякденної діяльності, тому інформація, яка знаходиться в її обігу, є досить різноманітною. Крім цього, за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом [57, ст. 20]. Відкритою є публічна інформація, що була отримана або створена в процесі виконання посадовими особами ДПСУ своїх обов'язків або яка знаходиться у володінні органів ДПСУ як суб'єктів владних

повноважень. Така інформація є відкритою, тому не підлягає захисту, а відповідальність у цьому аспекті може настати для органів ДПСУ як розпорядників такої інформації і лише в адміністративно-правових межах за відмову, ненадання інформації або з інших підстав, передбачених законодавством [97, ч. 2 ст. 23]. Публічна інформація з обмеженим доступом є конфіденційною, таємною та службовою [97, ч. 1 ст. 6]. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, поширювання такої інформації можливе лише за бажанням (згодою) відповідної особи у визначеному нею порядку, відповідно до передбачених нею умов, а також в інших випадках, визначених законом [97, ч. 1 ст. 7].

Порушення права громадянина на недоторканність приватного життя, особисту та сімейну таємницю тягне настання кримінальної відповідальності згідно зі ст. 182 КК України. А. І. Марущак зазначає, що зі складу злочину (ст. 182 КК України) випливає ще один вид неправомірного засобу доступу громадян до інформації – збирання конфіденційної інформації про особу без її згоди [12, с. 475]. Якщо недоторканність приватного життя було порушено службовою особою ДПСУ в результаті службової недбалості, то за наявності підстав для того вчинене можна кваліфікувати за ст. 367 (425) КК України. У даному випадку потерпілим від злочину може бути будь-яка особа (військовослужбовець або особа, яка не має відношення до служби у ДПСУ), без згоди якої збиралася або розповсюджувалася вказана конфіденційна інформація [395, с. 170].

Стаття 163 КК України передбачає відповідальність за порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв’язку або через комп’ютер. Кваліфікуючою ознакою є вчинення тих самих дій щодо державних чи громадських діячів або службовою особою, або з використанням спеціальних засобів, призначених для негласного зняття інформації. Зазначена стаття передбачає цілу низку неправомірних моделей поведінки громадян щодо доступу до інформації [12, с. 474].

Таємна інформація – це інформація, доступ до якої обмежується відповідно до законодавства, розголошення якої може завдати шкоди особі, суспільству і державі. Перелік відомостей, що становлять державну таємницю у сфері охорони державного кордону, передбачений наказом СБ України від «Про затвердження Зводу відомостей, що становлять державну таємницю». За розголошення відомостей такого характеру передбачена у КК України відповідальність згідно зі статтею 328 «Розголошення державної таємниці». У разі втрати документів або інших матеріальних носіїв секретної інформації, що містять державну таємницю, настає відповідальність, передбачена ст. 329 КК України. Так, зокрема *Вирок у справі № 127/19700/15-к Вінницького міського суду Вінницької області від 18 вересня 2015 р., у якому Особу_1 водія – фельд'єгеря Вінницького обласного вузла спеціального зв'язку державного підприємства спеціального зв'язку, який був обізнаним з вимогами нормативно-правових актів, що регламентують діяльність спецзв'язку, у порушення п. 5.16 Інструкції з технології порядку приймання, обробки, зберігання, перевезення та доставки відправлень спеціального зв'язку, затвердженої Державним комітетом зв'язку та інформатизації України від 02 липня 1999 р. № 21 таємно, п.п. 5.1.27, 5.1.30, Технологічної карти робочого місця фельд'єгеря, який виконує автомаршрут з перевезення літерних відправлень, затвердженої заступником директора з питань виробництва ВОВВСЗ 11 серпня 2004 р. № 73 для службового користування, п. 2. 21 посадової інструкції водія ВОВСЗ, що виконує обов'язки фельд'єгеря за суміщенням від 03 січня 2014 р., не перевірив наявність діючого спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею у вказаній установі та вручив вищезазначений пакет з нанесеним реквізитом «Таємно» співробітнику канцелярії ОСОБА_3, що немає допуску та доступу до державної таємниці, яка в свою чергу поставила свій підпис та відтиск гербової печатки установи в реєстрі № 176 фельд'єгеря та в подальшому ознайомилась із змістом пакету, у якому знаходився запит № 15/894 таємно від 17 березня 2015 р. Адміністрації ДПСУ про проведення перевірки, передбаченої Законом України «Про очищення влади» щодо співробітника*

розвідувального підрозділу, з додатком не таємних документів. Було визнано винним у вчиненні злочину за частиною 1 статті 328 КК України [396].

Військовослужбовці ДПСУ в разі розголошення відомостей військового характеру, що становлять державну таємницю, за відсутності ознак державної зради несуть відповідальність відповідно до ст. 422 КК України. Л. Ф. Дадерко, дослідивши питання кримінальної відповідальності за розголошення державної таємниці, зазначає, що військовослужбовці за розголошення відомостей невійськового характеру, але які становлять державну таємницю, несуть відповідальність за ст. 328 КК України. Хоча, продовжує думку науковець, у цій статті прямої вказівки на це немає, усе-таки військовослужбовці є спеціальними суб'єктами [397, с. 84].

Розголошення відомостей військового характеру, що становлять державну таємницю, може відбуватись будь-яким способом, зокрема й з використанням мобільного зв'язку, про що свідчить судова практика. Так *вироком у справі № 760/8755/15-к Солом'янського районного суду м. Києва було визнано винною Особу_1 (військовослужбовця) у вчиненні злочину, передбаченого ч.1 ст. 422 КК України, який під час користування мобільним зв'язком зі своїми знайомими неодноразово, розголошував відомості військового характеру, які згідно зі ст. 4.4.7, 4.4.9, 4.4.5, 4.4.4, 4.4.3, 4.4.12 ЗВДТ становлять державну таємницю за відсутності ознак державної зради. У результаті витоку інформації про організацію розвідувальної діяльності завдано шкоду національній безпеці України у сфері державної безпеки та охорони правопорядку, оскільки розкрито факт використання для отримання розвідувальної інформації штучних супутників зондування земної поверхні іноземних держав, що дозволить заінтересованій стороні вжити заходів технічного характеру для маскування своїх позицій з метою введення в оману, що може призвести до унеможливлення отримання розвідувальної інформації в інтересах підрозділів, що здійснюють розвідувальну діяльність, та до зниження обороноздатності держави* [398].

Кримінальна відповідальність за шпигунство, тобто передачу або збирання з метою передачі іноземній державі, іноземній організації або їхнім

представникам відомостей, що становлять державну таємницю, передбачена статтями 111 КК України (у разі вчинення цих дій громадянином України) та 114 КК України (якщо ці дії вчинені іноземцем або особою без громадянства). Згідно із Законом України «Про військовий обов'язок і військову службу» військову службу у ДПСУ можуть проходити виключно громадяни України, водночас законодавчо не визначено заборони іноземцям та особам без громадянства перебувати на посадах працівників ДПСУ. У зв'язку з цим можемо зробити висновок, що шпигунські дії, вчинені військовослужбовцями ДПСУ, можуть бути кваліфіковані лише за ст. 111 КК України, працівниками ДПСУ – як ст. 111, так і ст. 114 КК України (залежно від їх громадянства).

Суттєвою ознакою державної зради є нанесення конкретної шкоди інформаційним інтересам. Такими інтересами у прикордонній сфері, які перебувають у межах кримінально-правового захисту ст. 111 КК України, на наш погляд, є захищеність відомостей: ДПСУ щодо забезпечення охорони та захисту державного кордону України; в інформаційній та інформаційно-аналітичній діяльності; у функціонуванні телекомунікаційних та інформаційно-телекомунікаційних систем, автоматизованих систем управління; про діяльність персоналу ДПСУ із виконання поставлених завдань тощо.

Аналіз нормативних джерел і наукової літератури показав відсутність єдності в розумінні поняття «інформаційна безпека», що є необхідним для визначення об'єкта складу злочину «державна зрада» та правильної кваліфікації злочинів проти національної безпеки загалом. З огляду на це необхідним є нормативне закріплення даного поняття, а також визначення змісту інформаційної безпеки держави у прикордонній сфері, адже досвід показав, що непорушність територіальної цілісності України перебуває в тісному кореляційному зв'язку із захищеністю державного кордону [399, с. 125].

Службовою інформацією є інформація, що міститься: у документах органів ДПСУ, які становлять внутрівідомчу службову кореспонденцію; доповідних записках; рекомендаціях, пов'язаних з охороною державного кордону або здійсненням контрольних функцій, процесом прийняття рішень і передують

публічному обговоренню та/або прийняттю рішень; інформація, що зібрана в процесі оперативно-розшукової діяльності, у сфері оборони країни і яку не віднесено до державної таємниці. За передачу або збирання з метою передачі іноземним підприємствам, установам, організаціям або їх представникам таких відомостей, зібраних у процесі оперативно-розшукової діяльності, у сфері оборони країни, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства, передбачена кримінальна відповідальність згідно зі ст. 330 КК України.

Указуючи на надмірну деталізацію таємної інформації, що перебуває під кримінально-правовою охороною, О. О. Семенюк пропонує власний підхід до її диференціації. Науковець пропонує застосовувати до таємниці фізичної особи, конфіденційної та державної, поняття – «чужа таємниця». Усі злочини, що посягають на «чужу таємницю», поділяє: на протиправне заволодіння чужою таємницею; розголошення чужої таємниці; втрата матеріальних носіїв, що містять чужу таємницю [400, с. 54]. Цікавим у поглядах О. О. Семенюк є те, що науковець прирівнює всі види обмеженої інформації. Така позиція потребує узгодження видів інформації, закріплених у законодавчих актах, зокрема в Законі України «Про інформацію» та інших законах [400, с. 54].

Наявність окремого розділу у КК України, присвяченого «комп'ютерним злочинам», пов'язана зі зростанням ролі та масштабів використання комп'ютерних інформаційних систем у житті суспільства, популярністю глобальних комп'ютерних мереж Інтернету в усіх сферах, що призвело до появи та перманентної динаміки різноманітних злочинних посягань, пов'язаних з викраденням, перекрученням або знищенням комп'ютерної інформації, неправомірним використанням комп'ютерів, а також умисним порушенням роботи комп'ютерів [401, с. 217].

Завдяки використанню інформаційних технологій здійснюється обробка великого обсягу інформації, що реалізується шляхом створення та застосування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем,

а також автоматизованих систем управління, які мають важливе значення для сфери охорони державного кордону у зв'язку із тим, що забезпечують інформаційну діяльність ДПСУ, яка має відповідати європейським тенденціям прикордонної безпеки, забезпечувати національну безпеку України та є необхідною складовою функціонування інформаційно-телекомунікаційних систем ДПСУ. Це пов'язано з необхідністю забезпечення захисту прав людини на доступ до публічної інформації у прикордонній сфері, захисту інформаційних систем, мереж та електронних інформаційних ресурсів ДПСУ, розширення застосування інформаційних технологій у системі управління прикордонними підрозділами та при наданні державних послуг, надійного обміну інформацією з питань контролю осіб, транспортних засобів і вантажів, які перетинають державний кордон у межах функціонування інтегрованої міжвідомчої автоматизованої системи, а також унеможливлення несанкціонованого втручання в інші відомчі інформаційні ресурси, які потребують захисту.

Органи та підрозділи ДПСУ створюють і використовують в інтересах охорони державного кордону інформаційні системи, у тому числі банки даних щодо осіб, які перетнули державний кордон України, осіб, які вчинили правопорушення, протидію яким віднесено до компетенції ДПСУ, осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або тимчасово обмежується право виїзду з України, недійсних, викрадених і втрачених документів на право виїзду за кордон та в інших випадках, передбачених законами України [79, ст. 20]. У зв'язку із важливістю такої інформації, яка має загальнодержавне, відомче та персональне значення і зберігається в інформаційних ресурсах ДПСУ, важливе впровадження та підтримання комплексних заходів щодо технічного захисту інформації; унеможливлення несанкціонованого доступу до інформації та правових засобів регулювання, охорони та захисту відповідної інформації.

Тому питання захисту змісту інформації, що обробляється (передається, зберігається) в комунікаційних (технологічних) системах ДПСУ, обумовлює необхідність усіх дієвих механізмів захисту не тільки технічних, але і

кримінально-правових. *Так, 2 грудня 2019 року задокументовано черговий факт продажу службових даних, за які старший лейтенант слідчий Національної поліції отримав 1 300 грн., після чого був затриманий у порядку ст. 208 Кримінального процесуального кодексу України військовою прокуратурою Київського гарнізону спільно з територіальним управлінням ДБР в м. Києві та ДПСУ. За несанкціонований збут службової інформації, яка зберігається в комп'ютерах та автоматизованих системах, слідчий отримував кошти з території РФ. «Зловмисник збував інформацію стосовно осіб, яка зберігається та оброблюється в автоматизо-ваній підсистемі «Ризик» інформаційно-телекомунікаційної системи (далі – ІТС) «Гарт-1», базі даних «Аркан», «АРМОР» та інших. Так, 22 січня, 22 березня та 14 травня 2019 року поліцейський одержав кошти за свої «послуги» на загальна суму 16 350 грн»* [402].

Широке використання комп'ютерних технологій у діяльності ДПСУ обумовлює необхідність застосування правових механізмів технічного захисту інформаційної безпеки, що відображено в окремому розділі КК України, а саме в розділі XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». У ньому законодавець закріпив шість складів злочинів (ст. 361, 361-1, 361-2, 362, 363, 363-1 КК України), які можуть мати місце в діяльності ДПСУ. Об'єктивна сторона цих злочинів виражається у таких формах:

несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ч. 1 ст. 361 КК України);

створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ч. 1 ст. 361-1 КК України);

несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства (ч. 1 ст. 361-2 КК України);

несанкціоновані зміна, знищення або блокування інформації (ч. 1 ст. 362 КК України) та несанкціоновані перехоплення або копіювання інформації (ч. 2 ст. 362 КК України), яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації;

порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку (правил) захисту інформації, яка в них оброблюється (ст. 363 КК України);

умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів (ч. 1 ст. 363-1 КК України) [403, с. 64].

Підійшовши ґрунтовно до питання удосконалення кримінально-правового захисту інформаційних відносин в умовах розвитку інформаційного суспільства в Україні, Н. А. Савінова доводить необхідність прийняття ефективної і дієвої Концепції кримінально-правового забезпечення розвитку інформаційного суспільства в Україні. При цьому визначає, що головною метою такої Концепції має визнаватися досягнення заходами кримінального права необхідного для розвитку інформаційного суспільства в Україні рівня безпеки його основних ресурсів і цінностей від суспільно небезпечних посягань, безпеки інформаційного простору як стану інформаційної безпеки [404, с. 63].

Концепція кримінально-правового забезпечення розвитку інформаційного суспільства України має відображати державне ставлення до комплексного послідовного запровадження і реалізації всіх етапів дії Концепції та її реалізації, адже лише їх гармонійність обумовлюватиме ефективну протидію суспільно

небезпечним діянням, які посягають на ресурси та цінності інформаційного суспільства в державі [404, с. 63].

Розвиток інформаційного суспільства зумовив появу різного характеру деструктивного впливу на свідомість, які перебувають за межами законодавства про кримінальну відповідальність, до таких Н. А. Савінова відносить:

1) трансформована злочинність – група злочинів, які можуть вчинюватися з використанням дистанційних комунікацій;

2) кібернетичний тероризм – сукупність дій терористичної спрямованості, які здійснюється у спосіб дистанційних комунікацій у кіберпросторі;

3) кібернетична інтервенція – сукупність агресивних дій у кіберпросторі, спрямованих на втручання у спосіб дистанційних комунікацій у внутрішні та зовнішні справи держав з метою заподіяння шкоди їх суверенітету або належному функціонуванню її керівних органів або основних сфер життєдіяльності, а рівно аналогічні дії стосовно впорядкованої діяльності міждержавних об’єднань та їх керівних органів;

4) інформаційна експансія – суспільно небезпечні дії, спрямовані на умисне захоплення з метою подальшого використання на свою користь інформаційного простору, або значної частини інформаційного простору певної держави, або групи держав;

5) маніпулювання свідомістю населення – умисні впливи на свідомість населення або його певної групи, що здійснюється з використанням інформаційного простору [385, с. 327].

Складність, багатогранність і важливість інформації у сучасному суспільстві відображається на відносинах у сфері охорони державного кордону. Відповідно, це враховано у кримінальному законодавстві. Злочини, пов’язані з інформацією у прикордонній сфері, передбачають кримінальну відповідальність:

за порушення встановленого порядку доступу до інформації, яка охороняється законом;

надання завідомо неправдивої інформації (злочинний обман);

застосування інформації для злочинного впливу (погроза); приховування інформації, коли є обов'язок її надання.

Кримінально-правова охорона інформаційних відносин та інформації також здійснюється шляхом установлення санкцій за втручання в роботу інформаційних технологій, ресурсів, баз даних, їх пошкодження, порушення цілісності інформації тощо. Інформація може бути об'єктом, предметом і засобом вчинення злочинів у прикордонній сфері.

Загалом розвиток інформаційного суспільства обумовлює створення відповідних умов в діяльності ДПСУ за двома основними напрямками:

по-перше, доступу громадян чи зацікавлених органів влади до відкритої публічної інформації;

по-друге, забезпечення захисту інформації з обмеженим доступом, яка стала відома й обробляється у зв'язку з виконанням завдань держави (незалежно від носія збереження) [405, с. 88]. Настання кримінальної відповідальності за найбільш тяжкі порушення законодавства України про інформацію **(додаток М)** як одного із видів відповідальності, яка застосовується поряд із дисциплінарною, цивільно-правовою та адміністративною, є одним із засобів охорони інформаційних відносин з урахуванням доступу до інформації і її захисту у прикордонній сфері.

Адміністративна відповідальність за порушення законодавства про інформацію у сфері діяльності ДПСУ

Ще одним засобом охорони інформаційних прав є застосування адміністративної відповідальності у разі їх порушення чи недотримання. Охоронні норми адміністративного права утворюють правовий фундамент протидії загрозам в інформаційній сфері [406, с. 148], а з урахуванням теми нашого дослідження і загрозам у сфері діяльності ДПСУ. Ю. Є. Максименко наголошує, що тривалий час інформаційні правопорушення розглядалися крізь призму загроз інформаційній безпеці України, та зазначає, що сьогодні правопорушення в інформаційній сфері стосуються поширення фактів протизаконного збору і використання інформації, несанкціонованого доступу до

інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з баз даних, порушення технологій оброблення інформації, запуску програм-вірусів, троянів, фішингових програм, знищення та модифікація даних в інформаційних системах, перехоплення інформації в технічних каналах її витоку, маніпулювання суспільною та індивідуальною свідомістю тощо [407].

Л. П. Коваленко зазначає, що Кодекс України про адміністративні правопорушення (далі – КУпАП) передбачає адміністративну відповідальність за порушення права на окремі види інформації, відмову в наданні інформації, надання неповної або недостовірної інформації, втрату інформації [408, с. 162]. Обсяг і характер таких правопорушень постійно розширюється із розвитком інформаційного суспільства, інформаційних ресурсів та потребує своєчасного виявлення й застосування відповідальності за їх вчинення, зокрема й у прикордонній сфері. Підставою для застосування адміністративно-деліктних норм і настання адміністративної відповідальності за невиконання інформаційного законодавства є вчинення інформаційного правопорушення.

Юридичною ознакою, що виділяє інформаційні правопорушення серед усіх інших, виступає присутність інформаційних компонентів у їхньому складі:

1) як об’єкта правопорушення – якщо протиправне діяння спрямоване проти інформаційних відносин, або як предмета правопорушення – якщо протиправне діяння спрямоване проти інформації та її носіїв, інформаційних систем;

2) як елемента об’єктивної сторони правопорушення, що вказує спосіб, шлях здійснення протиправного діяння – у разі його вчинення з використанням інформаційних технологій і засобів. Усі інші юридичні ознаки інформаційного правопорушення відповідають традиційній конструкції правопорушення в теорії права, проте можуть мати певні особливості, зумовлені інформаційною природою [13, с. 217].

О. В. Стоєцький пропонує поділяти адміністративні правопорушення, що посягають на суспільні відносини у сфері: збирання інформації; зберігання інформації; використання інформації; поширення інформації [409, с. 10].

Аналогічної думки дотримується Л. П. Коваленко [408, с. 158]. Такі підходи відображають посягання на окремі види інформаційної діяльності, закріплені в ст. 9 Закону України «Про інформацію» (створення, збирання, одержання, зберігання, використання, поширення), а отже, у такому випадку адміністративні правопорушення посягають на порядок інформаційної діяльності. А. В. Шапка вказує, що інформаційні правопорушення у діяльності ДФС України, посягають на встановлений законодавством правопорядок у податковій чи митній сферах держави щодо обробки персональних даних, доступу до інформації, її захисту, а також посягає на функціонування інформаційних технологій та інформаційних ресурсів ДФС України, за яку законом передбачено юридичну відповідальність [410, с. 117].

Загальною рисою правопорушень в інформаційній діяльності органів ДФС України, наголошує Н. А. Литвин, є зв'язок з інформаційними процесами – обігом інформації, інформаційними ресурсами, інформаційними технологіями, інформаційно-телекомунікаційними системами тощо [19, с. 289]. Загалом науковець пропонує відокремлювати такі види правопорушень, за які настає адміністративна відповідальність за порушення норм інформаційного законодавства: правопорушення проти інформації, інформаційних ресурсів, що посягають на відповідні правовідносини (конфіденційності, цілісності, доступності, спостережності); правопорушення проти інформаційного простору, які посягають на певні правовідносини, пов'язані із якістю і цінністю інформації (її повнотою, об'єктивністю, своєчасністю, нешкідливістю тощо); правопорушення проти інформаційної інфраструктури, що посягають на правовідносини, які виникають у сфері використання об'єктів інформаційної інфраструктури (інформаційно-телекомунікаційних систем, комп'ютерів, серверів, їхнього програмного забезпечення тощо); інші інформаційні правопорушення, для яких властиве використання інформації, інформаційного простору, інформаційної інфраструктури при здійсненні протиправних діянь, що посягають на інші правовідносини (щодо приватної власності, суспільної та державної безпеки тощо) [19, с. 294–295].

Інформаційне правопорушення характеризується тим, що завдає шкоди (небезпеки) інформаційним правам чи свободам людини та громадянина, інформаційній інфраструктурі держави чи вчиняється за допомогою інформаційно-телекомунікаційних технологій або засобів зв'язку [407]. Інформаційне правопорушення у прикордонній сфері, крім цього, завдає шкоди прикордонній безпеці та може вчинятись з використанням службового становища. Отже, загальними характерними рисами адміністративного інформаційного правопорушення у сфері діяльності ДПСУ є: заподіяння шкоди інформаційним відносинам, що перебувають під охороною норм КУпАП; порушення порядку інформаційної діяльності, а саме: створення, збирання, одержання, зберігання, використання, поширення, аналізу тощо; використання інформаційних ресурсів для порушення норм інформаційного законодавства чи завдання іншої шкоди; пов'язання зі сферою охорони державних кордонів.

Ураховуючи особливості прикордонної сфери у разі порушення законодавства про інформацію, наслідком якого є настання адміністративної відповідальності, варто зупинитись на характеристиці суб'єктного складу правопорушення. З цього приводу А. І. Марущак звертає увагу на те, що відповідальності підлягають як винні посадові особи (у необґрунтованій відмові в наданні інформації, порушенні встановленого терміну її представлення без поважних причин, безпідставній відмові від поширення певної інформації тощо), так і громадяни (які мають бажання і інтерес до отримання певної інформації і які у своєму бажанні можуть перейти межі дозволеної правомірної поведінки) [12, с. 456].

Відповідно до КУпАП суб'єктами адміністративного правопорушення є особи, які досягли на момент вчинення адміністративного правопорушення шістнадцятирічного віку [411, ст. 12], та посадові особи за недодержання установлених правил, забезпечення виконання яких входить до їх службових обов'язків [411, ст. 14]. Отже, для досліджуваного різновиду адміністративних правопорушень у прикордонній сфері характерним є як загальний, так спеціальний суб'єкт.

Загальним суб'єктом досліджуваних правопорушень у прикордонній сфері може бути громадянин України, іноземний громадянин і особа без громадянства, на яких може розповсюджуватись адміністративна відповідальність за статтями 204-1 «Незаконне перетинання або спроба незаконного перетинання державного кордону України» та 204-4 «Порушення порядку в'їзду до району проведення антитерористичної операції або виїзду з нього» КУпАП, у частині перетинання або спроби перетинання державного кордону України в пунктах пропуску через державний кордон України (в контрольних пунктах в'їзду-виїзду) з використанням підробленого документа чи таких, що містять недостовірні відомості про особу.

Зважаючи на поняття «паспортний документ», визначене Законом України «Про прикордонний контроль» [154, п. 12 ч. 1 ст. 1], який є підставою для перетинання державного кордону України [154, ч. 1 ст. 1], підроблений документ може містити неправдиву інформацію про особу, яка перетинає державний кордон, щодо її громадянства, підтвердження особи пред'явника, дійсного права на в'їзд або виїзд з держави. Отже, за подання неправдивої та недостовірної інформації про особу та з приводу наявної підстави перетинання державного кордону настає адміністративна відповідальність за статтями 204-1 та 204-4 КУпАП.

Спеціальними суб'єктами є посадові особи ДПСУ. Відповідно до ст. 14 Закону України «Про Державну прикордонну службу України» особовий склад ДПСУ складається із військовослужбовців і працівників ДПСУ. Щодо працівників ДПСУ як суб'єктів адміністративної відповідальності, на них розповсюджуються загальні підстави відносно посадових осіб, що порушили законодавство про інформацію з урахуванням повноважень ДПСУ за такі правопорушення:

незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових або інших визначених законом повноважень (ст. 172-8 КУпАП);

порушення порядку подання або використання даних державних статистичних спостережень (ст. 186-3 КУпАП);

порушення законодавства у сфері захисту персональних даних (ст. 188-39 КУпАП);

порушення законодавства про державну реєстрацію нормативно-правових актів (ст. 188-41 КУпАП);

незаконне зберігання спеціальних технічних засобів негласного отримання інформації (ст. 195-5 КУпАП);

порушення законодавства про державну таємницю (ст. 212-2 КУпАП);

порушення права на інформацію та права на звернення (ст. 212-3 КУпАП);

порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію (ст. 212-5 КУпАП);

здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем (ст. 212-6 КУпАП).

Загалом, КУпАП містить більше, ніж 20 статей, які безпосередньо стосуються інформаційної сфери, і у своєму складі містять по декілька правопорушень, хоча, зауважує А. Благодарний, правопорушень значно більше, ніж статей [412, с. 123]. Наприклад, лише ч. 2 ст. 212-3 КУпАП («Порушення права на інформацію та права на звернення») встановлює відповідальність за сім різних адміністративних правопорушень у сфері обігу інформації. Вчинення інформаційного правопорушення, передбаченого КУпАП у прикордонній сфері, посягає на суспільні інформаційні правовідносини загалом та підриває основи державної інформаційної безпеки [19, с. 294]. У ч. 1 ст. 212-2 КУпАП («Порушення законодавства про державну таємницю») містить дев’ять пунктів, більшість із яких встановлюють відповідальність за декілька різних адміністративних порушень у сфері інформаційної безпеки [411, с. 123].

Суб’єктом інформаційного правопорушення згідно зі статтею 212-6 КУпАП (здійснення незаконного доступу до інформації в інформаційних

(автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем) може бути будь-яка особа, що посягає на встановлений порядок оброблення та зберігання інформації у базах даних ДПСУ, яка досягла віку адміністративної відповідальності. Тобто як загальний, так і спеціальний суб'єкт (посадові особи ДПСУ) підлягає адміністративній відповідальності в даному випадку.

З приводу військовослужбовців як суб'єктів адміністративної відповідальності існують особливості, визначені у статті 15 КУпАП, згідно з якою військовослужбовці як посадові особи, що вчинили адміністративне правопорушення, несуть відповідальність за дисциплінарними статутами. Винятком щодо інформаційних правопорушень є порушення правил, норм і стандартів, що стосуються: вчинення правопорушень, пов'язаних з корупцією; здійснення незаконного зберігання спеціальних технічних засобів негласного отримання інформації; порушення законодавства про державну таємницю; порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію [411, ч. 1 ст. 15]. У цих випадках військовослужбовці ДПСУ несуть адміністративну відповідальність на загальних підставах за порушення законодавства про інформацію [411, ч. 1 ст. 15]. За вчинення військових адміністративних правопорушень несуть відповідальність, передбачену главою 13-Б КУпАП, за умови, якщо ці правопорушення не тягнуть за собою кримінальну відповідальність [411, ч. 4 ст. 15]. Така нормативна регламентація, зазначає А. Ф. Мота, була успадкована з часів існування радянського адміністративного і військового законодавства та пояснювалася тим, що в інтересах обороноздатності країни, підтримання дисципліни у військах юрисдикція цивільних органів повинна була поширюватися на військовослужбовців лише за окремі адміністративні проступки [413, с. 2].

Для військовослужбовців – посадових осіб ДПСУ за порушення інформаційного законодавства згідно зі статтею 15 може бути застосована адміністративна відповідальність за такими статтями КУпАП:

172-8 (незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових або інших визначених законом повноважень);

195-5 (незаконне зберігання спеціальних технічних засобів негласного отримання інформації);

212-2 (порушення законодавства про державну таємницю);

212-5 (порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію).

За вчинення інших інформаційних правопорушень, передбачених ст. 188-39, 188-41; 212-3, 212-6 КУпАП, військовослужбовці несуть дисциплінарну відповідальність (**додаток М**).

Тому з урахуванням розвитку інформаційного суспільства, інформаційних відносин у прикордонній сфері та вимог часу вважаємо за необхідне внести зміни до статті 15 КУпАП в частині, що адміністративна відповідальність для військовослужбовців на загальних підставах, передбачених КУпАП, настає у порушення законодавства про інформацію. Вважаємо, що до військовослужбовців за вчинення окресленого нами вище різновиду адміністративних правопорушень повинні застосовуватись не дисциплінарні стягнення, а заходи адміністративної відповідальності.

Сьогодні у правовій доктрині обґрунтовується думка про необхідність визнання суб'єктом адміністративної відповідальності юридичною особи. А. Благодарний обґрунтовує це аналогічним досвідом іноземних країн, зокрема Федеративної Республіки Німеччини, РФ, Республіки Білорусь, Республіки Молдови, а також наявністю у чинному українському законодавстві норм, які передбачають накладення стягнень на юридичних осіб, зокрема, за правопорушення в інформаційній сфері. Так, згідно з ч. 6 ст. 20 Закону України «Про державну таємницю» [237] дозвіл на провадження діяльності, пов'язаної з державною таємницею, може бути скасовано СБ України на підставі акта проведеної нею перевірки, висновки якого містять дані про недотримання органом державної влади, органом місцевого самоврядування, підприємством, установою, організацією умов, передбачених цією статтею Закону [412, с. 125]. З

цього приводу В. Ю. Баскаков, О. В. Стоєцький також констатують, що чинне вітчизняне законодавство, передбачає притягнення до відповідальності за порушення інформаційного законодавства не тільки фізичних, а й юридичних осіб [414]. Загалом, законодавство про адміністративну відповідальність юридичних осіб в Україні недостатньо розроблене [103, с. 175].

Адміністративні інформаційні правопорушення можуть вчинятись із поєднанням інших правопорушень, про що свідчить судова практика. Наприклад, розглянуті справи за *Незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових повноважень №: 297/1691/16-п 10 листопада 2016 р. Берегівського районного суду Закарпатської області відносно інспектора прикордонної служби 1 категорії 2 відділення інспекторів прикордонної служби ВПС «Вілок» ДПСУ 3 категорії (тип Б)* [415] *та № 503/2299/15-п Кодимський районний суд Одеської області від 08 квітня 2016 р. відносно заступника начальника відділу прикордонної служби «Тимкове» з персоналу ДПСУ* [416], *за ст. 172-8 КУпАП* пов'язувались із корупційними діяннями.

Крім характерних для прикордонної сфери прогалин, у КУпАП існують і загальні проблемні питання, вирішення яких сприятиме підвищенню дієвості адміністративних заходів впливу охоронного характеру для інформаційних відносин. З урахуванням аналізу змісту КУпАП варто наголосити на відсутності у ньому системності норм за порушення законодавства про інформацію, що значно ускладнює пошук інформації про склади адміністративних правопорушень даного виду [417, с. 50].

В. А. Ліпкан та Ю. Є. Максименко, дослідивши основи формування інформаційної деліктології, роблять акцент на не систематизованості в окремому розділі та розпорошенні в різних розділах (главах) КУпАП адміністративних деліктів інформаційного характеру [418]. З цього приводу О. А. Заярний зазначає, що за таких умов формування законодавства про адміністративні інформаційні правопорушення значно знижується ефективність діяльності з профілактики цього виду деліктів, утрачається правовий і функціональний зв'язок між проступками та встановленими за їх вчинення адміністративними стягненнями

[419]. Крім цього, проблемність у цій сфері, зазначає О. В. Стоєцький, полягає у тому, що норми КУпАП, які встановлюють відповідальність у сфері інформаційної безпеки, дублюються нормами інших нормативно-правових актів, які, у свою чергу, інколи навіть прямо суперечать його нормам [409, с. 9].

Питання відсутності систематизації у КУпАП норм, що передбачають відповідальність за вчинення інформаційних правопорушень, є наріжним каменем у теорії інформаційно-правової думки. Виходячи з таких правових позицій можна підтримати науковий погляд, відповідно до якого передбачені в нормах адміністративно-деліктного законодавства склади адміністративних інформаційних правопорушень мають знайти своє закріплення в окремому розділі проекту Адміністративно-деліктного кодексу України «Адміністративні правопорушення в інформаційній сфері», положення якого мусять бути поділені на глави за видами інформаційної діяльності [419].

Зі свою боку, А. Благодарний зробив висновок у своєму дослідженні, що впровадження логічно завершеної, ефективної правової регламентації адміністративної відповідальності за правопорушення в інформаційній сфері потрібно передбачити у чинному КУпАП розділі, який би містив правопорушення у сфері обігу інформації, а також закріпити у чинному КУпАП (або у новому Кодексі України про адміністративні проступки) норму, яка б передбачала адміністративну відповідальність юридичних осіб за вчинення правопорушень в інформаційній сфері [412, с. 126]. В. Ю. Баскаков, О. В. Стоєцький пропонують для створення єдиної збалансованої системи адміністративно-правових норм, що забезпечують охорону суспільних відносин в сфері інформаційної безпеки, об’єднати статті, що передбачають адміністративну відповідальність за порушення окремих аспектів інформаційної безпеки в окремий розділ «Адміністративні правопорушення в сфері інформаційної безпеки України» Особливої частини КУпАП, родовим об’єктом якого буде інформаційна безпека України [414]. Г. М. Писаренко вважає виправданим створення єдиного закону, наприклад, Інформаційного кодексу України, з повним переліком складів інформаційних правопорушень [420, с. 17].

Законотворча практика суміжних з Україною країн свідчить про виділення в окремих розділах норм, що передбачають адміністративну відповідальність за інформаційні правопорушення. Так, у Кодексах про адміністративні правопорушення Республіки Білорусь [421] та РФ [422] передбачена глава «Адміністративні правопорушення у сфері зв'язку та інформації». У Кодексі про правопорушеннях Республіки Молдова інформаційні правопорушення переважно містяться у трьох главах: XIV «Правопорушення у галузі електронних комунікацій, поштового зв'язку та інформаційних технологій» (глава XIV), «Правопорушення, що зачіпають діяльність органів публічної влади (глава XVI), «Правопорушення, що посягають на громадський порядок і громадську безпеку» (глава XIX) [423].

Тому очевидною є необхідність здійснення упорядкування адміністративно-деліктних інформаційних норм у межах окремого розділу діючого КУпАП, чи нового Кодексу з приводу адміністративних проступків та відповідальності за їх вчинення, який би відповідав вимогам сучасного суспільства. На наш погляд, було б доцільним урахувати пропозицію О. А. Заярного й назвати цю главу «Адміністративні правопорушення в інформаційній сфері», яка лаконічно та загально охоплює об'єктний склад досліджуваних проступків.

Отже, адміністративній відповідальності за порушення законодавства про інформацію у сфері функціонування ДПСУ характерні такі особливості:

є різновидом адміністративної відповідальності, що передбачена за вчинення правопорушень, що містяться у різних розділах КУпАП та інших нормативно-правових актах, які врегульовують інформаційну діяльність та забезпечення права на інформацію (закони України «Про інформацію», «Про державну таємницю», «Про захист персональних даних», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо);

адміністративній відповідальності підлягають особи, що перетинають державний кордон України; посадові особи ДПСУ (військовослужбовці та працівники); будь-яка особа у межах ст. 212-6 КУпАП;

до військовослужбовців ДПСУ передбачено (ст. 15 КУпАП) застосовування як дисциплінарних, так і адміністративних стягнень [417, с. 50].

Дисциплінарна відповідальність

За вчинення інформаційних правопорушень законодавством передбачено застосування, крім кримінальної і адміністративної, ще й дисциплінарної відповідальності.

Дисциплінарна відповідальність у сфері обігу інформації має певні особливості, які зумовлені специфікою виконання особою службових обов'язків, пов'язаних зі створенням, збиранням, одержанням, зберіганням, використанням, поширенням, охороною та захистом інформації [4243, с. 73]. Дисциплінарна відповідальність застосовується за недотримання вимог службової дисципліни військовослужбовцями, а, отже, ставить під загрозу законність реалізації наданих військовослужбовцям інформаційних повноважень, і як наслідок – є передумовою порушення прав і свобод громадян [425, с. 139]. За такої умови підривається авторитет державної влади загалом і унеможливлюється виконання соціального призначення саме того чи іншого органу державного управління. Тому дисциплінарну відповідальність також слід розглядати як один із правових засобів забезпечення службової дисципліни державних службовців, підвищення рівня їх сумлінності при реалізації інформаційної компетенції [426, с. 86].

Основні правові засади дисциплінарної відповідальності військовослужбовців ДПСУ урегульовані Дисциплінарним статутом ЗС України (далі – Дисциплінарний статут) [427]. Аналіз норм Дисциплінарного статуту показав, що у ньому не загадується ні про інформаційні правопорушення, ні про аналогічні адміністративні правопорушення, за вчинення яких настає дисциплінарна відповідальність згідно зі ст. 15 КУпАП [411]. Такий стан стосовно охорони інформаційних відносин у військових формуваннях суперечить загальнотеоретичним підставам настання юридичної відповідальності, а саме: фактичної (наявність факту реально вчиненого правопорушення, що відповідає складу конкретного правопорушення, за яке в законі передбачено конкретну санкцію) та юридичної підстави (порушення правової норми, яка визначає діяння

протиправним і неправомірним). За допомогою діалектичного принципу загального зв'язку можемо визначити, що в межах Дисциплінарного статуту за порушення норм інформаційного законодавства не може наставати відповідальність, передбачена КК України, КУпАП (у межах ст. 15 КУпАП) та ЦК України). Отже, у такому випадку дисциплінарна відповідальність може наставати для військовослужбовців ДПСУ за порушення внутрішньовідомчих нормативних актів (наказів, інструкцій, листів, вказівок командирів/начальників) для підрозділів і посадових осіб, що здійснюють інформаційну діяльність (інформаційно-аналітичні підрозділи, оперативно-розшукові підрозділи, прес-служба ДПСУ тощо), та пов'язана з управлінським та внутрішньо-організаційним забезпеченням такої діяльності [428, с. 81–82].

Дисциплінарна відповідальність для військовослужбовців настає за порушення військової дисципліни, яку в Дисциплінарному статуті визначено як бездоганне і неухильне додержання всіма військовослужбовцями порядку і правил, установлених військовими статутами та іншим законодавством України [427, п. 1 Р. 1]. Дане поняття виходить за межі військової служби, адже не кожне порушення військовослужбовцем законодавства України є порушенням військової дисципліни. Наприклад, договірні чи позадоговірні зобов'язання у межах цивільного законодавства стосуються військовослужбовця як і будь-якого іншого громадянина України. А отже, дана норма потребує уточнення, що порушення законодавства має бути пов'язане із виконанням обов'язків військової служби. Тому після слів «та іншим законодавством України» необхідно додати фразу «що врегульовує порядок проходження військової служби» [428, с. 82].

Дисциплінарне стягнення застосовується командиром до військовослужбовця за невиконання (неналежне виконання) ним своїх службових обов'язків, порушення військовослужбовцем військової дисципліни або громадського порядку [427, ст. 45], а саме – за вчинення дисциплінарного правопорушення.

Дисциплінарний статут надає перелік дисциплінарних стягнення для різних категорій військовослужбовців без конкретизації за які правопорушення. Так, на

молодших та старших офіцерів можуть бути накладені такі дисциплінарні стягнення: а) зауваження; б) догана; в) сувора догана; г) попередження про неповну службову відповідність; д) пониження в посаді; е) пониження військового звання на один ступінь; ж) звільнення з військової служби за службовою невідповідністю; и) позбавлення військового звання [427, ст. 68].

За вчинення інформаційних правопорушень у межах КУпАП військовослужбовці несуть дисциплінарну відповідальність у таких випадках:

1. Порушення законодавства у сфері захисту персональних даних (ст. 188-39 КУпАП), зокрема недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних (ч. 4) та повторне протягом року вчинення порушення, передбаченого частиною четвертою цієї статті, за яке особу вже було піддано адміністративному стягненню (ч. 5) [411].

2. Порушення законодавства про державну реєстрацію нормативно-правових актів (ст. 188-41 КУпАП), що виявляється у неподанні, несвоєчасному поданні для державної реєстрації нормативно-правових актів, які відповідно до закону підлягають державній реєстрації, направлення на виконання нормативно-правових актів, що не пройшли державної реєстрації та не опубліковані в установленому законом порядку, а також надіслання для виконання вказівок, роз'яснень у будь-якій формі, що встановлюють правові норми [411].

3. Порушення права на інформацію та права на звернення (ст. 212-3 КУпАП). Таке правопорушення відносно досліджуваної нами сфери може мати вияв у п'яти окремих складах адміністративних правопорушень: не оприлюднення інформації, обов'язкове оприлюднення якої передбачено законами України «Про доступ до публічної інформації», «Про відкритість використання публічних коштів» та «Про засади запобігання корупції» (ч. 1); порушення Закону України «Про доступ до публічної інформації», а саме: необґрунтоване віднесення інформації до інформації з обмеженим доступом, ненадання відповіді на запит на інформацію, ненадання інформації, неправомірна відмова в наданні

інформації, несвоєчасне або неповне надання інформації, надання недостовірної інформації (ч. 2); обмеження доступу до інформації або віднесення інформації до інформації з обмеженим доступом, якщо це прямо заборонено законом (ч. 4); неправомірна відмова в наданні інформації, несвоєчасне або неповне надання інформації, надання інформації, що не відповідає дійсності, у відповідь на адвокатський запит, запит кваліфікаційно-дисциплінарної комісії адвокатури, її палати або члена відповідно до Закону України «Про адвокатуру та адвокатську діяльність» (ч. 5); незаконна відмова у прийнятті та розгляді звернення, інше порушення Закону України «Про звернення громадян» (ч. 7) [411].

4. Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем (ст. 212-6 КУпАП), а саме: здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах (ч. 1); дія, передбачена ч. 1 цієї статті, вчинена стосовно інформаційних (автоматизованих) систем, призначених для зберігання та обробки інформації з обмеженим доступом (ч. 3); незаконне копіювання інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі (ч. 4); безоплатне незаконне розповсюдження інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі (ч. 5); незаконний збут інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі (ч. 6) [411].

У цих чотирьох статтях КУпАП передбачені діяння, які можуть вчинити спеціальні суб’єкти інформаційної діяльності (підрозділи документального забезпечення, режиму та захисту інформації, зв’язку та інформаційних систем, Контактний центр ДПСУ, а також посадових осіб, відповідальних за збереження персональних даних, реєстрацію нормативно-правових актів тощо. Такі підрозділи та посадові особи уповноважені на здійснення спеціальних функцій з інформацією, розпорядником яких є ДПСУ, або з інформаційно-телекомунікаційними системами ДПСУ, але за передбачені вище склади

інформаційних правопорушень застосовується дисциплінарна відповідальність, що, на нашу думку, послаблює режими інформації, її охорону та захист прав на інформацію у межах діяльності не тільки ДПСУ, але й іншого військового формування. Такий стан тільки підсилює висловлену нами вище думку про необхідність застосування за вчинення інформаційних адміністративних правопорушень до військовослужбовців заходів не дисциплінарного стягнення, а саме – адміністративного стягнення.

Різноманітність виявів об'єктивної сторони дисциплінарних проступків у сфері обігу інформації фактично унеможливлює надання їхнього виключного переліку в одному законодавчому акті. Саме тому на практиці нерідко виникають питання стосовно правомірності застосування заходів дисциплінарного впливу за відповідні діяння [424, с. 67]. Це може бути і недотримання механізму інформування громадськості про діяльність ДПСУ у соціальних мережах, передбачені у Методичних рекомендаціях щодо формування єдиних підходів до інформування громадськості у соціальних мережах про діяльність ДПСУ [323] тощо.

На думку О. О. Тихомирова, О. К. Тугарова, для України пріоритетом повинно стати чітке нормативне закріплення як переліку дисциплінарних правопорушень, так і санкцій за їхнє вчинення. Тобто склади конкретних проступків у сфері обігу інформації, а також заходи дисциплінарного впливу за їхнє вчинення мають визначатись у загальних і локальних нормативних актах, відповідних посадових інструкціях. За таких умов відпаде необхідність у визначенні меж правомірності дій командира (начальника), які на сьогодні переважно розглядаються як оціночна категорія, а військовослужбовець буде найбільш захищеним у процесі реалізації права на працю [424, с. 68].

Сьогодні питання дисциплінарної відповідальності, зокрема за інформаційні правопорушення, залишають не визначеними, переважна більшість із яких за порушення норм інформаційного законодавства, під час обробки, надання, збереження тощо інформації перебувають на вирішенні командирів (начальників) ДПСУ у межах їх дисциплінарної влади, а не у компетенції органів юстиції. При

цьому дисциплінарні відносини між командиром (начальником) й особою, що вчинила інформаційне правопорушення будуються тільки згідно з принципом субординації та мають односторонній характер. Допускаємо, що у такому разі можливі випадки, коли порушенням інформаційного законодавства не надається розголосу, тобто факт вчинення правопорушення замовчується з метою приховування належного стану правопорядку, дисципліни, якщо звісно такі факти не будуть виявлені контролюючими органами, чи є потерпілі особи, які захищають свої права. Крім цього, вирішення справи може мати суб'єктивний характер, залежно від ставлення начальника до підлеглого. Також можливе застосування невідповідних стягнень вчиненому інформаційному правопорушенню, адже, наприклад, за недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних, передбачено накладення штрафу на посадових осіб – від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян (ч. 4 ст. 188–39 КУпАП) чи у разі здійснення незаконного збуту інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі, – тягне за собою накладення штрафу від двадцяти до ста неоподатковуваних мінімумів доходів громадян з конфіскацією незаконно збутих чи призначених для збуту копій баз даних, а також грошей, отриманих від їх продажу (ч. 6 ст. 212-6 КУпАП), чи зможуть такі санкції замінити догана чи сувора догана тощо. Вважаємо, що таке становище зменшує значення основних функцій юридичної відповідальності, зокрема виховну (превентивну), чим порушується порядок охорони та захисту інформаційних відносин.

Отже, загальними особливостями, які притаманні дисциплінарній відповідальності за порушення інформаційного законодавства, є те, що за вчинення окремих адміністративних проступків (ст. 188-39, 188-41, 212-3, 212-6 КУпАП) військовослужбовці несуть дисциплінарну відповідальність, яка

позбавлена конкретизації складів правопорушень, на нашу думку, за їх вчинення повинна наставати адміністративна відповідальність.

Цивільно-правова відповідальність

Ще одним видом юридичної відповідальності, що застосовується за порушення законодавства України про інформацію є цивільна відповідальність. *Цивільно-правова (майнова) відповідальність* настає в тих випадках, коли в результаті недотримання відповідних норм інформаційного права заподіюється шкода підприємствам, установам, організаціям і громадянам. Таку відповідальність несуть як юридичні, так і фізичні особи, а заподіяна майнова шкода відшкодовується винною стороною в повному обсязі [408, с. 164]. Положення про орган охорони державного кордону ДПСУ, затверджене наказом МВС України, визначає, що «ООДК є юридичною особою, має печатки із зображенням малого Державного Герба України і дійсним або умовним найменуванням, інші печатки і штампи, рахунки в органах Державної казначейської служби України та може мати рахунки в банках, у тому числі в іноземній валюті» [100, п. 4. Р. 4]. Отже, органи ДПСУ, будучи юридичними особами виступають повноправними учасниками цивільних відносин і мають право на захист інформаційних прав й обов'язок відшкодовувати завдану іншим фізичним чи юридичним особам шкоду пов'язану з реалізацією інформаційних прав у межах ЦК України.

Всеосяжність та універсальність об'єкта інформаційних відносин – інформації у галузях як публічного, так і приватного права визначає її особливу роль у цивільному обігу. Згідно з главою 15 ЦК України інформація є об'єктом цивільно-правової охорони як нематеріальне благо. Таке закріплене правове становище інформації у цивільному законодавстві, зазначають О. О. Тихомиров та О. К. Тугарова, надає передусім немайнового характеру безпосередньому протиправному впливу інформаційного правопорушення. Навіть коли йдеться про майнову шкоду, спричинену таким правопорушенням, вона завдається саме через нематеріальну інформаційну сферу [424, с. 51]. О. В. Кохановська зазначає, що саме нематеріальний характер є характерною рисою інформації у цивільному

обігу. Інформація – благо неспоживче, яке піддається лише моральному, але не фізичному старінню [430, с. 37–44]. Цивільні інформаційні обов'язки як у межах договірних, так і позадоговірних відносин, як правило, пов'язані з необхідністю надання, повідомлення, закріплення певної інформації, невиконання чого може завдати особі шкоди та зумовити цивільно-правову відповідальність [424, с. 51].

В інформаційно-правових відносинах у прикордонній сфері охорона інформаційних прав здійснюється щодо: ДПСУ, а точніше її юридичних осіб – органів охорони державного кордону, інших юридичних осіб згідно з договірними або позадоговірними зобов'язаннями з ДПСУ; фізичних осіб, військовослужбовців, працівників ДПСУ, пов'язаних з ДПСУ виконанням військового та службового обов'язку, громадян України, іноземних громадян й ОБГ, пов'язаних потребою та інтересом щодо перетинання державного кордону чи іншим інтересом про діяльність ДПСУ.

1. Серед інформаційних прав органів охорони державного кордону як юридичних осіб, що підлягають захисту у разі їх порушення можна зазначити:

право юридичної особи на найменування. Юридична особа повинна мати своє найменування, яке містить інформацію про її організаційно-правову форму та назву. Найменування установи має містити інформацію про характер її діяльності. Юридична особа може мати крім повного найменування скорочене найменування [107, ст. 90];

право юридичної особи на особисті немайнові права. Юридична особа має право на недоторканність її ділової репутації, на таємницю кореспонденції, на інформацію та інші особисті немайнові права, які можуть їй належати [107, ст. 94].

2. Щодо фізичних осіб військовослужбовців, працівників ДПСУ, керівників органів та підрозділів охорони державного кордону, підрозділи кадрового забезпечення ДПСУ здійснюють облік і збереження особових справ військовослужбовців, працівників ДПСУ, які повинні враховувати такі інформаційні права останніх, а саме:

право на ім'я. У разі перекручення імені фізичної особи воно має бути виправлене. Якщо перекручення імені було здійснене в документі, такий документ підлягає заміні [107, ч. 3 ст. 294];

право на особисте життя та його таємницю (ст. 301 ЦК України). Фізична особа має право на особисте життя (ч. 1), на збереження у таємниці обставин свого особистого життя (ч. 3). Обставини особистого життя фізичної особи можуть бути розголошені іншими особами лише за умови, що вони містять ознаки правопорушення, що підтверджено рішенням суду, а також за її згодою (ч. 4) [107, ст. 301];

право на особисті папери (ст. 303 ЦК України). Ознайомлення з особистими паперами, їх використання, зокрема шляхом опублікування, допускаються лише за згодою фізичної особи, якій вони належать (ч. 2). Якщо особисті папери фізичної особи стосуються особистого життя іншої особи, для їх використання, у тому числі шляхом опублікування, потрібна згода цієї особи (ч. 3) [107, ст. 303].

3. З приводу інформаційних прав інших фізичних осіб, то можна навести до прикладу такі норми, які передбачають цивільно-правову охорону:

право на інформацію (ч. 1 ст. 302 ЦК України), під цим розуміється, що будь-яка фізична особа має право вільно збирати, зберігати, використовувати і поширювати інформацію [107, ст. 302];

право на використання імені (ст. 296 ЦК України), у тому числі ім'я фізичної особи, яка затримана, підозрюється чи обвинувачується у вчиненні кримінального правопорушення, або особи, яка вчинила адміністративне правопорушення, може бути використане (обнародуване) лише в разі набрання законної сили обвинувальним вироком суду щодо неї або винесення постанови у справі про адміністративне правопорушення та в інших випадках, передбачених законом (ч. 4) [107, ст. 296].

Сутність юридичної природи цивільно-правової відповідальності за порушення норм інформаційного права має загальне підґрунтя застосування даного виду юридичної відповідальності та виявляється у поєднанні двох її складових частин:

1) права потерпілого на відновлення власного порушеного становища шляхом відшкодування (компенсації) збитків, майнової та моральної шкоди, здійснення інших правовідновлювальних дій;

2) обов'язку правопорушника добровільно чи примусово перетерпіти негативні наслідки майнового чи особистого характеру, передбачені законом чи договором, а у випадках застосування примусу – підтверджені рішенням суду, що забезпечує захист і відновлення прав потерпілого [394, с. 38].

Сьогодні в Україні перспективи цивільно-правової відповідальності за інформаційні правопорушенні зумовлені багатьма різноплановими факторами; зокрема: підвищенням рівня правової та інформаційної культури, еволюцією наукових уявлень щодо правової природи інформаційних явищ, розвитком інформаційного права і законодавства, удосконаленням діяльності судової системи тощо [394, с. 39]. Головна роль цивільно-правової відповідальності в охороні інформаційного законодавства та захисті усієї сукупності інформаційних прав суб'єктів інформаційних відносин, у тому числі і в прикордонній сфері, полягає у забезпеченні відновлення таких прав майновими і спеціальними немайновими засобами.

Інформаційна відповідальність

На сучасному етапі розвитку інформаційних відносин, інформаційного законодавства, а також існування потреби в ефективних правових заходах реагування на значне поширення інформаційних правопорушень науковці обговорюють можливість визнання окремого виду юридичної відповідальності, а саме – інформаційної.

«Наразі науково-доктринальна концепція «інформаційної відповідальності» ще не сформована, не вироблене належне розуміння як самої «інформаційної відповідальності», так і її співвідношення з іншими видами юридичної відповідальності. Можна напевне стверджувати тільки про наявність інформаційного характеру обмежувальних заходів юридичної відповідальності за правопорушення у сфері інформаційної діяльності, зокрема позбавлення

телерадіоорганізації ліцензії на право мовлення, проте за своєю юридичною природою такі заходи досить близькі до адміністративних» [13, с. 230].

Тому повністю підтримуємо погляди, що сьогодні актуальним напрямком юридичної доктрини є розроблення теоретичних засад інформаційної деліктології [431, с. 143].

Ю. Є. Максименко зазначає про існування теоретичного вакууму щодо концептуального оформлення інформаційно-правової відповідальності й умов, коли відповідальність за вчинення інформаційних правопорушень передбачена нормами різних кодексів утворення штучних колізій, а загалом нівелюється принцип невідворотності покарання. Так само невирішеними залишаються процедурні питання процесуального порядку притягнення до інформаційно-правової відповідальності [407]. Г. М. Писаренко зробив висновок про те, що сьогодні очевидним є існування поряд із кримінальною, адміністративною, цивільною та дисциплінарною ще й інформаційної відповідальності, яка існує об’єктивно [432, с. 57].

Сьогодні відповідальність за порушення норм інформаційного законодавства окремі науковці (М. І. Дімчогло, В. А. Залізняк, В. А. Ліпкан, К. П. Череповський) [47, с. 293; 48, с. 272; 375, с. 207] пропонують визначати у межах проектів Інформаційного кодексу України (назви пропонуються різні у зв’язку із невизначеністю предмета правого регулювання) окремий розділ «Відповідальність за порушення норм інформаційного законодавства». У цьому розділі пропонується консолідувати норми із відповідними інститутами деліктного права, зазначеними в ЦК України, а також КУпАП, КК України.

Таку позицію не підтримує О. О. Тихомиров, який зазначає, що нормативні моделі, необхідні для притягнення до юридичної відповідальності за такі правопорушення, вже закладені у відповідні нормативно-правові акти. Разом з тим підкреслює, що система державно-правового реагування на інформаційні правопорушення наразі більшою мірою потребує організаційних і освітніх заходів, тому що безпосередньо залежить від усвідомлення природи протиправності в інформаційній сфері та адекватного ставлення до неї всіх

суб'єктів, як правоохоронних, так і тих, кому вона загрожує. Удосконалення ж положень чинного вітчизняного законодавства, які передбачають відповідальність за інформаційні правопорушення, передусім кримінального, може здійснюватись поступовим, але невідкладним шляхом – переоцінкою небезпечності вже визначених видів правопорушень, учинених з використанням інформаційних технологій та за необхідності відповідне розширення їх юридичних складів додатковими кваліфікуючими ознаками [433].

Ураховуючи проаналізовані види юридичної відповідальності, які створюють правові гарантії охорони та захисту інформаційних відносин у прикордонній сфері, слід наголосити на таких її особливостях:

по-перше, кожному окремому виду притаманні характерні риси для кримінальної, адміністративної, цивільної та дисциплінарної відповідальності, які відображують процесуальний порядок, ступінь санкції тощо;

по-друге, для окремих видів відповідальності властива відсутність системного розташування норм у Кодексах (КК України, КУпАП, ЦК України), що передбачають відповідальність за порушення інформаційного законодавства;

по-третє, інформація може бути як об'єктом, так і засобом правопорушення;

по-четверте, за вчинення окремих адміністративних проступків військовослужбовці несуть дисциплінарну відповідальність;

по-п'яте, дисциплінарна відповідальність позбавлена конкретизації складів правопорушень.

Правові засоби охорони та захисту інформаційних відносин потребують комплексного підходу до вдосконалення норм, що визначають підстави, порядок та міри застосування негативних правових засобів до порушників, незалежно від їх правого становища. На нашу думку, для цього першочергово повинні бути: згруповані у межах окремих підрозділів КК України, КУпАП, ЦК України. За вчинення правопорушень, зазначених у КУпАП, де передбачена відповідальність за адміністративні, інформаційні правопорушення, військовослужбовці повинні нести адміністративну, а не дисциплінарну відповідальність, що сприятиме розмежуванню останніх (за порушення законів, постанов, розпоряджень –

адміністративна, за порушення внутрішньовідомчих організаційних нормативно-правових актів – дисциплінарна). Такі кроки будуть сприяти покращанню правового забезпечення інформаційних відносин та підвищить ефективність правового впливу.

4.3 Організаційно-правові засади інформаційної безпеки в мережі Інтернет та в інформаційних системах Державної прикордонної служби України

В інформаційному просторі держави, що охоплює частину інформаційної сфери, яка обмежена матеріальною та нематеріальною територією поширення, здійснюють інформаційну діяльність компетентні суб’єкти. Окремою частиною інформаційного простору є інформаційне середовище, що може охоплювати окрему сферу правового регулювання, у тому числі сферу охорони державного кордону. Загалом під інформаційним середовищем, необхідно розуміти, частину інформаційного простору, що характеризується мінімальною територією поширення та обмеженою кількістю суб’єктів інформаційної діяльності, а також обумовлюється своєрідним інформаційним мікрокліматом, що включає сукупність способів, прийомів, заходів та умов безпосереднього здійснення інформаційної діяльності [434].

Інформаційне середовище ДПСУ охоплює функціонування прикордонного відомства, щоденне виконання обов’язків його персоналом щодо забезпечення недоторканності державного кордону, невід’ємною складовою яких є інформаційна безпека держави, що забезпечується окремими видами інформаційної діяльності: поширення, охорона та захист інформації.

Головним завданням ДПСУ у напрямку інформаційної безпеки є створення таких відповідних умов, які б унеможливлювали вияви будь-яких інформаційних загроз. Досягнення цього можливе завдяки таким основним організаційним факторам, як: установлення чітких правил у роботі з інформацією та безпечне

використання інформаційних систем. Такі організаційні засади відображають динамічні процеси інформаційних відносин у діяльності ДПСУ, ефективність яких забезпечується дотриманням своїх обов'язків військовослужбовцями та працівниками ДПСУ щодо правил та порядку створення, збирання, одержання, зберігання, використання, поширення, охорона та захисту інформації. При цьому підґрунтям залишається статична частина цих відносин, знання та розуміння основних категорій, їх змісту, таких як: «персональні дані», «конфіденційна інформація», «службова інформація», «державна таємниця» тощо.

Інформаційне середовище ДПСУ охоплює функціонування прикордонного відомства, щоденне виконання обов'язків його персоналом щодо забезпечення недоторканності державного кордону, невід'ємною складовою яких є інформаційна безпека держави, що забезпечується окремими видами інформаційної діяльності: поширення, охорона та захист інформації.

Головним завданням ДПСУ у напрямку інформаційної безпеки є створення таких відповідних умов, які б унеможливлювали вияви будь-яких інформаційних загроз. Досягнення цього можливе завдяки таким основним організаційним факторам, як: установлення чітких правил у роботі з інформацією та безпечне використання інформаційних систем. Такі організаційні засади відображають динамічні процеси інформаційних відносин у діяльності ДПСУ, ефективність яких забезпечується дотриманням своїх обов'язків військовослужбовцями та працівниками ДПСУ щодо правил та порядку створення, збирання, одержання, зберігання, використання, поширення, охорона та захисту інформації. При цьому підґрунтям залишається статична частина цих відносин, знання та розуміння основних категорій, їх змісту, таких як: «персональні дані», «конфіденційна інформація», «службова інформація», «державна таємниця» тощо.

Широке використання соціальних мереж, а також реальна військова агресія РФ у формі гібридної (інформаційної) війни зумовлюють встановлення правил інформаційної безпеки не лише у межах виконання службових обов'язків (наприклад, постанова КМУ Порядок організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на

підприємствах, в установах і організаціях [238]), а поза ними. Такі правила встановлюються з метою недопущення розповсюдження як службової інформації, так і персональних даних, зокрема військовослужбовців.

Комунікація у соціальних мережах, зокрема: обмін повідомленнями, опублікування особистих фото, відео, місце роботи (служби), місце перебування, відомості про колег, друзів тощо та інша приватна інформація про військовослужбовця та його оточення у разі її потрапляння до зацікавлених осіб може поставити під загрозу як службову діяльність, так і приватне життя військовослужбовця, його керівників, колег. Тому СБ України розроблено «Пам'ятку щодо забезпечення інформаційної безпеки при роботі в мережі Інтернет» (далі – Пам'ятка) [435]. Ця Пам'ятка містить перелік основних чинників, що впливають на стан інформаційної безпеки у зв'язку із використанням загальнодоступних та соціально орієнтованих ресурсів мережі Інтернет, а також характеристику ключових факторів ризику та рекомендацій щодо їх нейтралізації (зберігання та передача даних, соціальні мережі, використання російських соціально орієнтованих ресурсів мережі Інтернет, використання додатків до смартфонів, електронне листування, вихід до мережі Інтернет, перелік російських веб-ресурсів, якими не рекомендовано користуватись, рекомендації посадовій особі органу виконавчої влади, місцевого самоврядування, представникам міністерств та відомств) [435] (**додаток Н**). Але здебільшого ця Пам'ятка носить рекомендаційний характер, а її дотримання переважно перебуває у площині інформаційної культури окремого військовослужбовця чи працівника ДПСУ, а настання відповідальності можливе лише коли у діях буде встановлено склад правопорушення норм інформаційного законодавства, передбачений КК України, КУпАП та іншими нормами законодавства.

Питання індивідуального безпечного використання поза межами службового користування, мережі Інтернет, соціальними мережами залишається на рівні свідомості військовослужбовця. Опитані респонденти відповіли «так» 85,3 %, що можуть розпізнати негативний інформаційний вплив під час

користування соціальними мережами чи Інтернетом, і «ні» – 16,5 %, але це усього припущення кожного, реально ці показники можуть бути протилежними. На запитання «Чи є обмеження для військовослужбовців щодо опублікування фото- та відеоматеріалів, інформації про себе та членів своєї сім'ї у соціальних мережах?», отримано 82,7 % позитивних відповідей і 17,3 % негативних. При цьому 83,1 % респондентів відмітили, що вони особисто обмежують висвітлення інформації про себе та свою сім'ю у соціальних мережах, і 16,9 % – ні **(додаток В)**. З урахуванням таких результатів відмітимо позитивну тенденцію, але все ж відсоток із відповідями «ні» необхідно мінімізувати.

Розвиток інформаційного суспільства дозволяє оперативно вирішувати багато питань у роботі органів державної влади завдяки досягнутому рівню інформатизації. Загалом процеси інформатизації формують умови для задоволення інформаційних потреб, реалізації прав громадян і суспільства шляхом формування, розвитку, використання інформаційних систем, мереж, ресурсів та інформаційних технологій, створених на основі застосування сучасної обчислювальної та комунікаційної техніки [198]. Ю. Є. Максименко підкреслює, що перехід суспільства до інформаційного змінив статус інформації. Наразі вона може бути як засобом забезпечення безпеки, так і загрозою та небезпекою [436, с. 1]. Отже, інформація та її захист залишається ключовим, відправним началом та основою у функціонуванні інформаційних систем.

Переваги, пов'язані із впровадженням процесів інформатизації, розширюються та конкретизуються в окремих сферах діяльності держави та суспільства. У сфері охорони державного кордону це і обробка великого обсягу персональних даних осіб, що перетинають державний кордон, і спрощення управління персоналом, і зменшення часу для здійснення прикордонного контролю, і своєчасне реагування на повідомлення про загрози прикордонній безпеці тощо. Використання ІС у сфері охорони державного кордону безперечно має багато переваг, разом з тим актуальним залишається питання збереження цілісності та захисту інформації, що зберігається (обробляється) в ІС, саме це зумовлює дослідження проблематики обраної теми [437, с. 81].

Завдяки розвитку й активному використанню інформаційних технологій здійснюється обробка великого обсягу інформації, що реалізується шляхом створення та використання інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, а також автоматизованих систем управління [438, с. 96]. Важливе значення ці системи мають для сфери охорони державного кордону у зв'язку із тим, що забезпечують інформаційну діяльність ДПСУ, яка має відповідати європейським тенденціям прикордонної безпеки. Інформаційна безпека та кібербезпека є невід'ємними елементами національної безпеки України [158, ст. 3] та невіддільною складовою функціонування інформаційно-телекомунікаційних систем ДПСУ. Це пов'язано з необхідністю забезпечення: захисту різних видів інформації, що актуальні в діяльності ДПСУ; захисту прав людини на доступ до публічної інформації у прикордонній сфері; захищеності інформаційних систем, мереж та електронних інформаційних ресурсів ДПСУ; застосування інформаційних технологій у системі управління прикордонними підрозділами та при наданні державних послуг; надійного обміну інформацією з питань контролю осіб, транспортних засобів і вантажів, які перетинають державний кордон у межах функціонування інтегрованої міжвідомчої автоматизованої системи, а також унеможливлення несанкціонованого втручання в інші відомчі інформаційні ресурси, які потребують захисту. Тому ретельного дослідження потребує комплекс заходів, спрямованих на захист інформації, що обробляється (передається, зберігається) в комунікаційних (технологічних) системах ДПСУ [437, с. 81].

Питання інформаційної безпеки та захисту інформації сьогодні є предметом дослідження багатьох сфер наукового пізнання, зокрема: управління, юридичної, технічної, економічної, військової тощо. Перед наукою та практикою поступово виникають нові питання, пов'язані з удосконаленням і розширенням меж інформаційної діяльності, такі як збереження, забезпечення порядку доступу, обмін інформацією, а також її захист у межах цілісної системи програмного та апаратного обладнання державних органів влади з урахуванням існуючих загроз.

Науковою розробкою юридичних аспектів інформаційної безпеки та захисту інформації займалися такі вчені, як: І. В. Діордіца, О. О. Климчук, Б. А. Кормич, О. І. Крюков, В. А. Ліпкан, О. В. Логінов, Ю. Є. Максименко, О. В. Олійник, О. О. Тихомиров, Н. А. Ткачук, Т. Ю. Ткачук, О. В. Шепета та багато інших.

Окремі питання технічного захисту інформації досліджені Б. Б. Ахметовим (вдосконалення кіберзахисту інформаційно-комунікаційних систем транспорту шляхом мінімізації навчальних вибірок у системах виявлення вторгнень), С. А. Носок, А. Е. Мазуренком (моделі багаторівневої безпеки баз даних), П. В. Пашковим (митні інформаційні технології), І. В. Яковим, О. В. Корнейко, О. О. Черноног (класифікація і аналіз моделей систем захисту інформації в комп'ютерних систем), В. В. Шорошевим (базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах), А. Є. Ільніцьким (безпека інформації в комп'ютерних системах та деякі підходи до її експертної оцінки) тощо.

Питання забезпечення стану захищеності інформаційно-телекомунікаційних систем у сфері прикордонної безпеки підняті у працях: Д. А. Мула, Є. В. Прокопенка, Р. П. Хоптинського (аналіз та обґрунтування вимог до системи захисту корпоративної телекомунікаційної мережі, аналіз функціонування інформаційно-телекомунікаційних систем ДПСУ у контексті забезпечення інформаційної безпеки); С. Л. Євсеєва, В. М Федорченка, О. С. Андрощука (побудова систем безпеки інформаційно-телекомунікаційних систем на основі комплексного криптографічного підходу); Р. В. Рачка (формування концепції розбудови геоінформаційної системи у сфері забезпечення прикордонної безпеки). Однак на сьогодні питання правового захисту інформації в ІС ДПСУ потребує нових досліджень.

У ДПСУ з урахуванням кращих європейських прикордонних практик упроваджені інформаційні, телекомунікаційні, інформаційно-телекомунікаційні системи ДПСУ, у тому числі міжвідомчі, бази (банки) даних та інші електронні інформаційні ресурси за компетенцією [110]. Такі комунікаційні системи повинні забезпечувати високий рівень безпеки інформації та відповідати сучасним

вимогам прикордонної безпекової політики. Розвиток ІС у ДПСУ сьогодні є об'єктивною потребою, яка реалізується з урахуванням світової тенденції побудови та інтеграції мереж, засобів і послуг зв'язку [439, с. 168]. Функціонування та постійний розвиток ІС базується на захисті інформації, розпорядником якої є ДПСУ. В ІС захист інформації від різних загроз відбувається синхронно, з обробкою інформації під час використання технічних і програмних засобів [437, с. 81].

На виконання положення Стратегії розвитку у ДПСУ забезпечується «розвиток інформаційної складової частин системи охорони державного кордону» через модернізацію: центральної підсистеми системи «Гарт» для забезпечення фіксації біометричних даних іноземців; інтегрованої міжвідомчої інформаційно-телекомунікаційної системи щодо контролю осіб, транспортних засобів і вантажів, які перетинають державний кордон («Аркан»); інформаційно-телекомунікаційної системи «Гарт-5» [440, 9.4, с. 13], «Гарт-10» [349]. З удосконаленням ІС посилюються захисні спроможності, які знижують рівень загрозливого впливу, спрямованого проти інформації, яка в них обробляється.

Під час використання ІС для накопичення, оброблення та збереження інформації, розпорядником якої є ДПСУ, повинні постійно підтримуватись умови для виключення несанкціонованого витоку такої інформації, тобто створення умов для безпечного функціонування кіберпростору ДПСУ. Ю. Є. Максименко у цьому контексті застосовує термін «інформаційно-технічна безпека», управління потенційними чи реальними загрозами з метою захисту інформаційно-телекомунікаційної інфраструктури, зокрема від комп'ютерної злочинності та комп'ютерного тероризму [436, с. 9].

Інформаційні технології та технології у сфері телекомунікації відіграють чи не найважливішу роль у розвитку країн, але разом із запровадженням нових технологій і відкриттям величезного інформаційного простору з'являються й невідомі до цього моменту проблеми, серед яких слід назвати кібернетичні злочини й правопорушення, що становлять загрозу не лише для окремих громадян, а й державній безпеці країн [441, с. 96]. Так, 12 травня 2017 р.

комп’ютери Донецького прикордонного загону «підхопили» вірус, що призвело до блокування комп’ютерів і втрати інформації. Але своєчасні правильні рішення та рішучі дії зв’язківців завадили розповсюдженню вірусу у мережі [442, с. 26].

З урахуванням цього випадку у межах ДПСУ було проведено низку роз’яснювальних заходів, прийнято нормативні акти на різних ланках управління ДПСУ та вжиті організаційні заходи стосовно правил користування автоматизованим робочим місцем у службовій діяльності, але досі не всі знають, що негайно після виявлення шкідливого програмного забезпечення необхідно відключити телекомунікаційну мережу. Такий висновок сформульований на підставі проведеного опитування, респонденти якого обрали такі варіанти: доповісти по команді (56,9 %), відключити телекомунікаційну мережу (32,6 %), закрити програму, заражену вірусом (6,6 %), вимкнути комп’ютер (3,9 %). Варіант «продовжувати працювати» не обрав жоден з респондентів **(додаток В)**.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає, що центральні органи виконавчої влади є суб’єктами, які здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки [443, ч. 4 ст. 5]. Державну політику у сфері захисту державного кордону реалізує Адміністрація ДПСУ [159] та забезпечує кібербезпеку у цій сфері. Загалом кібербезпека передбачає захищеність життєво важливих інтересів людини, суспільства та 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 [443, ст. 1]. Тобто стан, при якому будь-які загрози чи інший негативний вплив не можуть порушити цілісність, конфіденційність і режим доступу до інформації в інформаційно-комунікаційному просторі ДПСУ.

Однією із потреб та вимог інформаційного суспільства є дотримання та гарантування кібернетичної безпеки. В умовах глобалізації інформаційних процесів, їх інтеграції у різні сфери суспільного життя керівництво провідних держав світу приділяє посилену увагу створенню та удосконаленню ефективних

систем захисту критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру. У багатьох провідних країнах світу вже сформовані загальнодержавні системи кібернетичної безпеки як найбільш оптимальні організаційні структури, що здатні за короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектору для протидії кіберзагрозам. В Україні також відбувається процес формування системи кібернетичної безпеки [444, с. 312].

На виконання Стратегії розвитку Державної прикордонної служби України у ДПСУ впроваджується державна політика з питань захисту державних інформаційних ресурсів та інформації, розгортання спеціальної телекомунікаційної системи шифр «СТС-Д» для криптографічного захисту службової інформації [440, п. 9.5, с. 13], посилення протидії інформаційним загрозам [440, п. 22.2, с. 15], сучасних засобів криптографічного захисту інформації, кіберзахист критичної інфраструктури [445, с. 15–16], нарощування рівня захищеності об’єктів органів ДПСУ [349, п. 2.2.1].

Інформаційна безпека, кібербезпека та кіберзахист є невід’ємними елементами національної безпеки України та необхідною складовою функціонування ІС ДПСУ, це обумовлено необхідністю забезпечення захисту прав людини на доступ до публічної інформації у прикордонній сфері, захисту ІС, мереж та електронних інформаційних ресурсів ДПСУ, розширення застосування інформаційних технологій у системі управління прикордонними підрозділами та при наданні державних послуг, надійного обміну інформацією з питань контролю осіб, транспортних засобів і вантажів, які перетинають державний кордон у межах функціонування інтегрованої міжвідомчої автоматизованої системи, а також унеможливлення несанкціонованого втручання в інші відомчі інформаційні ресурси. Тому питання захисту змісту інформації, що обробляється (передається, зберігається) в комунікаційних (технологічних) системах ДПСУ, визначає потребу постійного вжиття заходів щодо недопущення втручання у прикордонний кіберпростір [437, с. 82].

Відносини у сфері захисту інформації в ІС регулюються Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» [109]. Відповідно до цього Закону для забезпечення захисту інформації у прикордонній сфері органам управління ДПСУ необхідно виконувати такі його основні положення:

по-перше, визначити чіткий порядок доступу до інформації в ІС [446, ч. 1 ст. 4];

по-друге, надавати доступ до інформації тільки встановленому переліку користувачів, відповідно до їх повноваження стосовно цієї інформації [446, ч. 1 ст. 4];

по-третє, дотримуватись порядку доступу до державних інформаційних ресурсів або інформації з обмеженим доступом і тільки тих користувачів, перелік і повноваження стосовно цієї інформації яких визначено законодавством [446, ч. 2 ст. 4];

по-четверте, забезпечувати доведення до користувачів відомостей про правила і режим роботи ІС та забезпечити їм доступ до інформації в системі відповідно до визначеного порядку доступу [446, ст. 6];

по-п’яте, функціонування служби захисту інформації [446, ст. 9];

по-шосте, контроль з боку керівництва органів і підрозділів ДПСУ за забезпеченням захисту інформації та діяльністю служби захисту інформації [446, ст. 9];

по-сьоме, забезпечення притягнення до відповідальності особи, винної у порушенні законодавства про захист інформації в ІС згідно із законодавством [446, ст. 11].

Загальні вимоги й організаційні засади забезпечення захисту державних інформаційних ресурсів врегульовані постановою КМУ «Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». Положення цієї постанови визначають, що система захисту інформації в ІС призначена для захисту інформації: від витоку технічними каналами, до яких належать канали побічних

електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій; несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів; спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування [447, п. 16].

Забезпечення захисту інформації та інформаційної безпеки в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах ДПСУ покладається на службу захисту інформації – Головний центру зв'язку, автоматизації та захисту інформації, у складі якого діють: група режиму і захисту інформації, центр інформаційних систем, центр телекомунікаційних систем, центр технічного захисту інформації, центр кібербезпеки, які відповідальні за збереження та захист інформації в окремих ІС чи напрямках, відповідно до компетенції [110].

Окремо варто зазначити про створення у 2018 році спеціального структурного підрозділу, призначеного для забезпечення кібербезпеки у сфері охорони державного кордону України, – Центру кібербезпеки. Центр кібербезпеки ДПСУ відповідає: за аналіз стану кіберзахисту інформаційно-телекомунікаційних систем ДПСУ; виявляє та усуває фактори, що негативно впливають на захищеність відомчих інформаційних ресурсів, здійснює контроль за виконанням заходів щодо забезпечення безпеки інформації в інформаційно-телекомунікаційних системах ДПСУ; своєчасно реагує на кіберзагрози тощо. Тобто відповідає за інформаційну безпеку та захист інформації, розпорядником якої є ДПСУ, та обробляє і зберігає у відомчих ІС, на основі використання сучасних інформаційних технологій [110].

Органи та підрозділи ДПСУ створюють та використовують в інтересах охорони державного кордону інформаційні системи, у тому числі банки даних щодо осіб, які перетнули державний кордон України; осіб, які вчинили правопорушення, протидія яким віднесена до компетенції ДПСУ; осіб, яким

згідно із законодавством не дозволяється в'їзд в Україну або тимчасово обмежується право виїзду з України; також банки даних щодо недійсних, викрадених і втрачених документів на право виїзду за кордон та в інших випадках, передбачених законами України [79, п. 10 ч. 1 ст. 20]. У зв'язку із важливістю такої інформації, яка має загальнодержавне та персональне значення й зберігається в інформаційних ресурсах, центр технічного захисту інформації повинен забезпечити: захист інформації від несанкціонованого доступу і захисту інформації від витоку технічними каналами.

Однією з потенційних загроз для інформації в інформаційних системах слід вважати цілеспрямовані або випадкові деструктивні дії персоналу (людський фактор), оскільки вони становлять 75 % усіх випадків. Таке узагальнення сформовано на підставі даних, опублікованих американським Інститутом комп'ютерної безпеки (*Computer Security Institute*, Сан-Франциско, штат Каліфорнія, Сполучені Штати Америки), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин: несанкціонований доступ – 2 %; укорінення вірусів – 3 %; технічні відмови апаратури мережі – 20 %; цілеспрямовані дії персоналу – 20 %; помилки персоналу (недостатній рівень кваліфікації) – 55 % [448].

Для захисту функціонування сумісних (з'єднаних) комунікаційних систем і забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних у ДПСУ повинна вживатись 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 [443, пп. 7, 11 ст. 1]. Тому актуальним у діяльності ДПСУ постає питання забезпечення інформаційної безпеки у межах кіберпростору, належний захист якого забезпечить розвиток інформаційної діяльності ДПСУ, її цифрового

комунікативного середовища та своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз прикордонній безпеці [443, п. 5 ст. 1].

Діяльність ДПСУ як суб'єкта, що безпосередньо здійснює заходи із забезпечення кібербезпеки у прикордонній сфері повинна бути спрямована на подолання загроз кібербезпеці, які актуалізуються через дію таких чинників [449, п. 2]:

невідповідність сучасним вимогам інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності;

недостатній рівень захищеності від кіберзагроз критичної інфраструктури, державних електронних інформаційних ресурсів та, безпосередньо, інформації (вимога щодо захисту якої встановлена законом);

безсистемність заходів кіберзахисту критичної інфраструктури;

недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури, також державних електронних інформаційних ресурсів;

недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки [449].

З метою підвищення рівня захисту інформації, розпорядником якої є ДПСУ, у тому числі інформації з обмеженим доступом, необхідно обробляти її у системі із застосуванням комплексної системи захисту інформації, яка включає взаємопов'язану сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [449, ч. 2 ст. 8]. Крім того, відомчий орган повинен не тільки розробити та впровадити КСЗІ, але й постійно стежити за її якісним функціонуванням, яке є одним з найголовніших аспектів при побудові надійних інформаційних систем будь-яких структурних підрозділів [450, с. 137, 142]. Для цього вживається сукупність організаційних та інженерно-технічних заходів, засобів і методів, які є обов'язковою складовою побудови

будь-якої КСЗІ відповідно до вимог законодавства. Зокрема передбачено, що в інтегрованій ІТС ДПСУ «Гарт» та інтегрованої міжвідомчої ІТС «Аркан» (складовою частиною якої є система «Гарт») інформація повинна оброблятися із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю [92, п. 19; 451, п. 22].

Завданням КСЗІ є забезпечення унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації, що обробляється в системі. При цьому надійний захист інформації повинен відповідати сучасним загрозам і потребує не лише окремих заходів захисту, але і комплексного організаційного підходу, що може бути вирішено шляхом ефективного функціонування у структурі ДПСУ підрозділів кіберзахисту, що сприятиме також реалізації положень Стратегії кібербезпеки України.

Інформаційна безпека в частині кіберзахисту у ДПСУ отримала своє належне врегулювання та організацію як складова національної безпеки України. Разом з тим необхідно враховувати те, що кібератаки стають усе більш комплексними та складними, їх наслідки становлять загрозу ключовим національним інтересам. Тому для побудови системи кібербезпеки необхідно вдосконалювати нормативно-правову базу у цій сфері та управління для створення ефективних механізмів забезпечення такої діяльності [452, с. 179]. Одним із ключових питань організації ефективної роботи національних систем кібербезпеки залишається налагодження взаємодії між компетентними державними органами, які є суб’єктами кібернетичної безпеки [453, с. 76].

Питання захисту змісту інформації, що обробляється (передається, зберігається) в ІС ДПСУ, обумовлює необхідність застосування всіх дієвих механізмів захисту не тільки правових, організаційних, технічних, але і кримінально-правових. Протиправне використання інформаційних технологій являє собою особливу загрозу не тільки прикордонній, але й національній безпеці країни, та є злочинами, передбаченими в розділі XVI КК України «Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку» [437, с. 83].

Інформація у прикордонній сфері, що зберігається в інформаційних ресурсах, має загальнодержавне та персональне значення, тому у межах діяльності ДПСУ повинен забезпечуватись її захист від несанкціонованого доступу і захист інформації від витоку, зокрема технічними каналами і правовими засобами. Безпека та захист інформації у межах функціонування ДПСУ охоплює заходи збереження інформації, пов'язані з всеохоплюючою світовою інформатизацією. У мережі Інтернет та за допомогою ІС інформація розповсюджується та копіюється миттєво, може стати доступною у будь-якій країні, що не завжди відповідає прикордонній безпеці. Саме тому важливо враховувати та перешкоджати таким виявам, зокрема, що стосується інформації, яка обмежена в доступі з урахуванням приватних, службових і державних інтересів. Що стосується порад користування мережі Інтернет використання та викладення інформації (поза виконанням службових обов'язків військовослужбовцями), що передбачені Пам'яткою, вони носять рекомендаційний характер і не мають заходів впливу за їх порушення. Тому необхідно зміцнювати не тільки патріотизм, але й інформаційну культуру, підвищувати рівень правосвідомості, базових знань інформаційного законодавства кожного військовослужбовця. Такі заходи сприятимуть відмежуванню, перш за все, інформації, розповсюдження якої може зашкодити виконанню обов'язків військової служби та прикордонній безпеці, хоча й належить до відкритої інформації та зміцненню інформаційної безпеки.

Активне використання ІС у діяльності ДПСУ сприяє прискоренню не тільки інформаційних процесів, але й виконанню усіх завдань, які стоять перед прикордонним відомством. Разом з тим обробка інформації у таких системах створює додаткову загрозу для порушення її цілісності й безпеки. Тому одночасно з веденням, обробкою, передачею даних у ІС, забезпеченням їх функціонування необхідно постійно вживати заходів з убезпеченням змісту інформації. Такі заходи повинні мати комплексний характер (правові, організаційні, технічні, здійснення контролю, притягнення винних до відповідальності тощо) та реалізовуватись усіма посадовими особами ДПСУ, які мають доступ до

функціонування ІС. Налагоджена робота спеціальних структурних підрозділів, призначених для захисту інформації у межах діяльності Головного центру зв'язку, автоматизації та захисту інформації Адміністрації ДПСУ, залучення кращих фахівців у сфері захисту інформації до їх складу, а також надання можливості їх професійного зростання підвищить ефективність протистояння інформаційним загрозам у досліджуваній сфері [437, с. 83].

Висновки до розділу 4

Інформаційні загрози у сучасному суспільстві можуть нанести шкоди більше, ніж будь-які протиправні фізичні дії. Інформаційні загрози в діяльності ДПСУ мають комплексний характер і створюють небезпеку прикордонній безпеці як складовій державної безпеки. Вони заподіюють шкоду не лише інформаційним відносинам, але й усій прикордонній безпеці, це може бути: порушення цілісності інформації, подання невідповідної інформації, викрадення службової інформації, що спричиняють конкретну шкоду, наприклад, у вигляді прийняття неправильного управлінського рішення, ведення інформаційної війни чи дезінформації. Саме тому питання правової охорони та захисту інформації є достатньо актуальними й важливими у діяльності ДПСУ.

Інформаційні загрози у діяльності ДПСУ – це фактори, які утворюють небезпеку чи заподіюють шкоду інформаційним відносинам, інформаційним правам, інформаційним ресурсам ДПСУ та посягають на прикордонну безпеку.

Багатоаспектний аналіз загроз прикордонній безпеці дозволив запропонувати класифікацію інформаційних загроз у 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 вияву: відомчі (посягають на прикордонну безпеку держави), корпоративні (зазіхають на безпеку окремого підрозділу), особисті (відносно окремих військовослужбовців чи 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 їх тактики та способів дій, щоб у подальшому планувати порушення прикордонного законодавства чи здійснення диверсійних операцій); стихійні лиха (пожежі, повені тощо).

Проаналізовані види юридичної відповідальності, які створюють правові гарантії охорони та захисту інформаційних відносин у прикордонній сфері, дозволили визначити такі їх особливості: кожному окремому виду притаманні характерні риси для кримінальної, адміністративної, цивільної та дисциплінарної відповідальності, які відображують процесуальний порядок, ступень санкції тощо; для окремих видів відповідальності властива відсутність системного розташування норм у Кодексах, що передбачають відповідальність за порушення інформаційного законодавства; інформація може бути як об'єктом, так і засобом правопорушення; за вчинення окремих адміністративних проступків військовослужбовці несуть дисциплінарну відповідальність; дисциплінарна відповідальність позбавлена конкретизації складів правопорушень.

Правові засоби охорони та захисту інформаційних відносин потребують комплексного підходу на шляху їх удосконалення, зокрема норм, що визначають підстави, порядок та заходи застосування негативних правових засобів до порушників, незалежно від їх правого становища. Для цього першочергово необхідно: згруповані у межах окремих підрозділів КК України, КУпАП статті,

що передбачають таку відповідальність; внести зміни до ст. 15 КУпАП та встановити, що за вчинення адміністративних інформаційних правопорушень військовослужбовці повинні нести адміністративну, а не дисциплінарну відповідальність, що сприятиме розмежуванню останньої (за порушення законів, постанов, розпоряджень – адміністративна, за порушення внутрішньовідомчих організаційних нормативно-правових актів – дисциплінарна).

Розвиток інформаційних відносин у діяльності ДПСУ пов'язаний із поширеним використанням і застосуванням глобальних, локальних та відомчих мереж. Розповсюдження у них інформації службового або приватного характеру може як прискорити інформаційні процеси (про особливості й умови перетинання державного кордону на окремих ділянках), так і спричинити негативні наслідки для прикордонної безпеки та безпеки військовослужбовців ДПСУ. Тому безпечне використання Інтернету, ІТС повинно бути пріоритетом для кожного військовослужбовця та працівника ДПСУ, ґрунтуватись на чіткому виконанні службових обов'язків, дотриманні норм законодавства (режиму інформації з обмеженим доступом), усвідомленні значення збереження інформації (правової культури, інформаційної культури) та рекомендацій щодо обмеження розповсюдження приватної інформації (про себе) та користування електронними пристроями (гаджетами тощо).

Під час ведення, обробки, передачі даних у ІС ДПСУ необхідно постійно вживати комплекс заходів (правових, організаційних, технічних, контрольних, притягнення винних до відповідальності тощо) з убезпеченням змісту інформації. Підвищенню ефективності у протистоянні інформаційним загрозам сприяє налагоджена робота спеціальних структурних підрозділів, призначених для захисту інформації у межах діяльності Головного центру зв'язку, автоматизації та захисту інформації Адміністрації ДПСУ, залучення кращих фахівців у сфері захисту інформації до їх складу, а також надання можливості їх професійного зростання.

РОЗДІЛ 5
УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНИХ ВІДНОСИН У ДІЯЛЬНОСТІ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

5.1 Організаційно-правові рекомендації підвищення ефективності інформаційних відносин у діяльності Державної прикордонної служби України

Досліджені теоретичні та організаційні засади нормативно-правового регулювання інформаційних відносин у діяльності ДПСУ дозволяють підкреслити їх міжгалузевий, багатовекторний і динамічний характер, пов’язаний з інтенсивним зростанням потреб інформаційного суспільства та забезпеченням безпеки державного кордону України з урахування кращих практик ЄС. Такі особливості зумовлюють властивості та форми вияву інформації у прикордонній сфері, яка є об’єктом відповідних відносин, а також «предмет, результат, а оперативність її отримання, повнота та достовірність безпосередньо впливає на можливості прикордонників орієнтуватись у складній ситуації, оцінювати її, прогнозувати зміни, чітко планувати свої подальші дії, загалом успішно виконувати підрозділами своїх функцій» [31, с. 119]. Перебуваючи в інтенсивному розвитку, інформаційні відносини потребують відповідного сучасним умовам покращання не тільки їх нормативно-правового регулювання, але й ефективності у сфері обігу інформації та інформаційної діяльності.

Покращити передбачає дії з поліпшення, що означає: «робити кращим, досконалішим за якістю, властивістю; робити більш досконалим що-небудь; удосконалювати; підвищувати показники (в роботі т. ін.) [454]. В основі удосконалення перебуває дійсний стан, показники, проблеми нормативно-правового регулювання та його практичного втілення в інформаційних відносинах у сфері виконання завдань ДПСУ, які необхідно змінити, виправити, зробити досконалішими для оптимізації правових механізмів їх реалізації та задоволення

інформаційних прав та інтересів, забезпечення безпеки всіх суб'єктів цих відносин.

Для визначення підґрунтя удосконалення необхідно з'ясувати проблемні аспекти, які потребують покращання та підвищення ефективності. Одним із факторів встановлення стану правового регулювання є конкретні показники й оцінка.

Діяльність органу влади передбачає оцінку його функціонування за результатами виконання завдань, для ДПСУ – з охорони державного кордону, а саме: відповідність очікуваному та реальному рівню захищеності державного кордону на ділянці відповідальності [455, с. 158]. Інформаційна складова є супутнім невід'ємним елементом прикордонної безпеки та діяльності у цьому напрямку ДПСУ. Але ключовим для визначення рівня забезпечення інформаційної складової діяльності ДПСУ є не тільки показники, але й можливості всіх суб'єктів інформаційних відносин реалізувати свої інформаційні права згідно з чинним законодавством.

В оцінці окремих аспектів інформаційних відносин доступні такі показники, як результати: опитування соціологічною службою Центру Разумкова спільно з Фондом «Демократичні ініціативи» імені Ілька Кучеріва [456], де встановлюється рівень довіри громадян до ДПСУ; рейтинг інформаційної прозорості офіційних веб-сайтів міністерств та інших центральних органів виконавчої влади, що визначається Державним комітетом телебачення і радіомовлення України, за результатами моніторингу інформаційного наповнення офіційних веб-сайтів органів виконавчої влади [457].

Якщо дані за результатами опитування Центру Разумкова носять вибірковий і відносний характер, а теоретична похибка вибірки не перевищує 2,3 %, то у ході моніторингу (проведеного у період з 13 по 18 грудня 2019 року) опитано 2 017 респондентів віком від 18 років, що має більш точні показники та результати. Зокрема, рівень інформаційного наповнення кожного веб-сайту оцінюється за такими показниками:

наявності інформації (визначає рівень наявності інформації на веб-сайті);

якості інформаційного наповнення (ураховує рівень повноти, актуальності, навігаційної доступності розміщеної на веб-сайті інформації, а також наявність функції пошуку та доступність інформації для сприйняття особами з порушеннями зору та слуху);

інформаційної прозорості (характеризує рівень інформаційної прозорості суб'єкта владних повноважень та розраховується як середнє значення двох попередніх показників);

динаміки інформаційної прозорості (демонструє, чи змінився рівень інформаційної прозорості суб'єкта владних повноважень у звітному періоді в порівнянні з попереднім періодом і визначається як різниця між значеннями відповідних показників інформаційної прозорості) [457].

З урахуванням останніх років опитувань (рівня довіри громадян) та моніторингу (інформаційного наповнення офіційних веб-сайтів) відзначаються значні позитивні зміни. Якщо на початку 2019 року рівень довіри був 52 %, то в кінці року довіра становила 60 %. Тому дуже важливим є забезпечення не тільки підвищення такого рівня, але й виправдання та підтримання його всіма військовослужбовцями та працівниками ДПСУ, у зв'язку із тим, що довіру важко отримати, але легко втратити. Будь-які дії з боку представників ДПСУ можуть вплинути (позитивно чи негативно, залежно від характеру дій) на досягнутий рівень довіри, що необхідно враховувати у повсякденній діяльності, у спілкуванні з громадськістю, із ЗМІ, взаємодіючими суб'єктами. За будь-яких умов, зокрема у кризових, необхідно виявляти витримку залишатись зваженими, спокійними, об'єктивними, розсудливими та показувати свій професіоналізм, як це показав начальник Львівського прикордонного загону 17.01.2020 року під час пікетування рівненчанами Львівського аеропорту, по факту не пропуску на територію України турецьких громадян за запрошенням рівненського підприємства [458].

Щодо інформаційного наповнення офіційних веб-сайтів, тут відслідковується стабільна позитивна ситуація. Державна прикордонна служба України останні роки отримує оцінку за всіма показниками 100 %, а у порівнянні першого та другого півріччя 2019 року прикордонне відомство з сьомого місця

перемістилась на перше **(додаток П.1, П.2)**, станом на 2020 рік показники залишаються стабільними **(додаток П.3)**, що дозволяє відзначити професійність та майстерність у цьому напрямку функціонування ДПСУ. Загалом веб-сайт ДПСУ можна відзначити як зручний, зрозумілий, інформаційно наповнений для громадян, такий, що відповідає потребам сучасного інформаційного суспільства.

Емпіричну базу для пізнання окремого напрямку інформаційних відносин – звернень громадян до ДПСУ, становлять звіти про організацію роботи зі зверненнями громадян [459] **(додаток К.1-К.10).**

На веб-сайті ДПСУ висвітлюються статистичні дані за розширеною кількістю показників та відповідно до Закону України «Про звернення громадян», зокрема розподіл проведеної роботи в Адміністрації ДПСУ та загалом у регіональних управліннях ДПСУ:

вид звернень громадян (заяви (клопотання), скарги) **(додаток К.1)**;

характер звернень (усні (подані на особистому прийомі), надіслані поштою, повторні звернення, колективні звернення, анонімні звернення, звернення, що не належать до повноважень суб'єктів звернень) **(додаток К.2)**;

звернення громадян розглянуто (особисто керівником, заступниками керівника, начальниками управлінь (відділів) **(додаток К.3)**;

звернення надійшли від (громадяни України, іноземні громадяни та особи без громадянства) **(додаток К.4)**;

категорії заявників (із загальної кількості звернень) (Герої України, Радянського Союзу, Соціалістичної праці; учасники та інваліди Великої Вітчизняної війни; учасник бойових дій на території інших країн за часів СРСР, учасник бойових дій, який брав безпосередню участь в АТО, ветеран військової служби ДПСУ, пенсіонер з числа військовослужбовців ДПСУ, військовослужбовець запасу ПВ/ДПСУ, ветеран праці ДПСУ, пенсіонер ДПСУ, державний службовець ДПСУ, працівник бюджетної сфери ДПСУ, член сім'ї військовослужбовця ДПСУ, член сім'ї учасника бойових дій, який брав безпосередню участь в АТО, військовослужбовці ДПСУ, з них: офіцерський

склад ДПСУ, сержантський і старшинський склад ДПСУ, рядовий склад ДПСУ **(додаток К.5)**;

основні питання, які порушували громадяни у зверненнях (порядок перетинання державного кордону, не пропуск через державний кордон тощо, фінансове забезпечення, порядок проходження служби, поновлення на службі, переведення по службі, виділення санаторно-курортних путівок на лікування, отримання житла, поновлення в черзі на його отримання, неправомірні дії посадових осіб, неправомірні дії прикордонників, надання інформації про перетинання кордону, тимчасове обмеження права виїзду за межі України, інші питання) **(додаток К.6)**;

структурними підрозділами Державної прикордонної служби України за напрямами службової діяльності розглянуто звернень (Департамент охорони державного кордону (штаб), Управління (відділ) кадрового менеджменту, Управління охорони здоров'я (мед. служба), Управління (відділ) матеріального забезпечення, Управління (відділ) озброєння та техніки, Фінансово-економічний (відділ) департамент, Управління (відділ) соціально-гуманітарного та морально-психологічного забезпечення, Управління юридичного забезпечення (юридична служба), Головний центр обробки спеціальної інформації, інші структурні підрозділи) **(додаток К.7)**;

на звернення громадян відповідь надано у термін (до 15 днів, у місячний термін, до 45 днів, перебуває у стадії розгляду) **(додаток К.8)**;

за результатами розгляду звернень громадян (перебуває у стадії розгляду, надано роз'яснення, вирішено позитивно, відмовлено у задоволенні вимог, звернення, що повернуто авторові відповідно до статей 5 і 7 Закону України «Про звернення громадян», звернення, що не підлягає розгляду відповідно до статей 8 і 17 Закону України «Про звернення громадян», надіслано на розгляд за належністю іншому органу влади, установі тощо) **(додаток К.9).**

Окремо зазначалось, скільки звернень надійшло в окремі частини центрального підпорядкування (у кожне регіональне управління, органи охорони державного кордону та органи забезпечення ДПСУ) **(додаток К.10)**.

Такі зведені статистичні дані надають узагальнену інформацію про роботу ДПСУ зі зверненнями громадян, дозволяють установити кількісну та якісну характеристику звернень громадян до ДПСУ, з'ясувати, які проблемні питання виникають у громадян, пов'язані з діяльністю органів і підрозділів охорони державного кордону, визначити відповідність дотримання термінів, установлених законодавством при розгляді звернень, категорії осіб, що направляли звернення тощо. Вважаємо, що такий розширений статистичний звіт має значний позитивний вплив на розвиток відкритості ДПСУ, збільшення довіри громадян і наукових досліджень, тому повинен і надалі висвічуватись на веб-сайті ДПСУ у такому розширеному форматі. Загальні показники дозволяють зробити висновок, що звернень з кожним роком стає більше, у деяких випадках у двічі, чим показує великий інтерес та довіру до діяльності ДПСУ, а також про збільшення навантаження на персонал ДПСУ, що забезпечує задоволення запитів громадянами.

З приводу узагальнення проблем, з якими стикались респонденти у ході обробки інформації у сфері діяльності ДПСУ, 38,5 % зазначили недосконалий механізм обробки інформації, 31,6 % суперечність норм інформаційного законодавства, 20,8 % недотримання посадовими особами вимог інформаційного законодавства, 16,5 % відсутність норми, яка б врегульовувала обіг інформації, при цьому 44,2 % військовослужбовців не змогли сформулювати відповідь **(додаток В)**.

Ще одним джерелом даних про інформаційну діяльність ДПСУ є дані зі Стратегічного бюлетеня прикордонної безпеки «Біла книга», яка повинна видаватись щорічно, на жаль остання була видана за 2016 рік. Зокрема у Білій книзі-2016 відзвітовано перед громадськістю про проведені за звітній період (2016 р.) заходи та форми висвітлення відкритої публічної інформації: проведено 130 – конференцій і брифінгів; видано Інформаційним агентством 48 номерів газет «Прикордонник України» та 8 номерів журналу «Кордон»; здійснено зйомку та монтаж 37 роликів і фільмів з прикордонної тематики; 4 тис. сюжетів вийшло на телевізійних каналах [460]. Такі щорічні видання ще були опубліковані за 2014

і 2015 рр.. У порівнянні зі ЗС України, аналогічне видання випускається щорічно з 2005 року. Тому вважаємо, що покращенню інформаційної відкритості сприятиме стабільне щорічне видання Стратегічного бюлетеня прикордонної безпеки «Біла книга», як, окрім висвітлення джерел публічної інформації, може надавати й інші дані про діяльність ДПСУ, зокрема варто висвітлювати узагальнену статистику щодо роботи із запитами та зверненнями громадян, а також заходи що вживаються щодо захисту персональних даних.

Питання стосовно висвітлення публічної інформації у ДПСУ реалізуються на достатньо високому рівні, у порівнянні з опрацюванням персональних даних. Так, відповідно до Закону України «Про захист персональних даних» [335, ч. 2 ст. 24] та наказу Уповноваженого з прав людини Типового порядку обробки персональних даних [334, п. 3.15] в ДПСУ повинен бути створений (визначений) структурний підрозділ або відповідальна особа, яка організовує роботу, пов’язану із захистом персональних даних під час їх обробки. Але інформації стосовно такого підрозділу в загальному доступі (зокрема на веб-сайті ДПСУ) не знаходимо. Інформація є про відповідальну особу (Петерчук Олексій Олександрович, e-mail: APeterchuk@pvv.gov.ua) на сайті Департаменту у сфері захисту персональних даних [461]. З урахуванням вимог розвитку відкритості та захисту персональних даних інформація про таку особу та її повноваження повинна бути доступною на сайті ДПСУ.

З досвіду FRONTEX позитивним є діяльність службовця, головним завданням якого є забезпечення незалежного внутрішнього застосування Регламенту ЄС 2018/1725 Європейського парламенту та Ради від 23 жовтня 2018 року про захист фізичних осіб щодо обробки особистих даних установами, органів, офісами та агентствами Союзу та про вільний рух таких даних [341].

Тим більше, що в Україні вже не один рік обговорюється доцільність створення незалежного Уповноваженого з питань захисту права на доступ до публічної інформації та захисту персональних даних (Інформаційного комісара) [462], а відповідні зміни до Конституції України вже знаходяться на розгляді у Конституційному Суді України [463]. Такі пропозиції обґрунтовуються тим, що

Уповноважений ВРУ з прав людини, який зараз контролює ці права, повною мірою не може забезпечити реалізацію політики у цих сферах. Крім того, створення такої інституції є рекомендацією Ради Європи [462]. Сьогодні питання, пов'язані з обігом персональних даних, набули значного широкого поширення, а їх захист є досить актуальним, тому потребує створення окремої інституції як у межах держави загалом, так і в діяльності її органів. Тому створення окремого структурного підрозділу у ДПСУ (а не призначення відповідальної особи) щодо обробки та захисту персональних даних є досить актуальним і перспективним.

Реалізуючи право на інформацію, громадяни, крім звернень, можуть направляти запити у сфері публічної інформації й персональних даних. Варто відмітити, що статистична інформація про запити на публічну інформацію та на інформацію, що містить персональні дані, взагалі відсутня на веб-сайті ДПСУ. Тому необхідно вести роботу та надавати узагальнені дані (кількість отриманих, опрацьованих, переданих за належністю, переданих до інших органі влади) про такі запити на публічну інформацію та на інформацію, що містить персональні дані з урахуванням вимог законодавства та досвіду FRONTEX у цьому питанні, де ведеться відкритий реєстр усіх операцій з обробки персональних даних, які повідомляються службовцю із захисту персональних даних FRONTEX. У цьому реєстрі зазначаються дата, напрямок, підрозділ, назва та призначення обробки, суб'єкти та категорії даних, дані про необхідність отримання консультації у European Data Protection Supervisor (EDPS) (Європейський інспектор із захисту даних) [464].

У зв'язку із наведеними вище аргументами підтримуємо необхідність створення при Адміністрації ДПСУ, регіональних управліннях, окремих структурних підрозділів (відділів) та призначення посадових осіб (у прикордонних загонах) з обробки та захисту персональних даних, військовослужбовці яких повинні мати юридичну освіту й забезпечувати не тільки захист персональних даних громадян, іноземцям та ОБГ, але й надавати консультації посадовим особам ДПСУ з цих питань, ведення реєстру тощо.

Такий відділ (у Адміністрації ДПСУ) може підпорядковуватись Голові ДПСУ та звітувати перед Уповноваженим з прав людини, а саме Департаменту у сфері захисту персональних даних (Інформаційному комісару, якщо такий у майбутньому буде створений). На відділ може бути покладне виконання таких завдань: забезпечення у межах повноважень ДПСУ виконання міжнародних зобов'язань України щодо імплементації міжнародних правових норм і стандартів, зокрема законодавства ЄС, національного законодавства у сфері захисту персональних даних; надання консультацій керівництву Адміністрації ДПСУ з питань застосування законодавства про обробку та захист персональних даних у ДПСУ; повідомлення Голові ДПСУ про порушення порядку захисту персональних даних; звітування перед Уповноваженим з прав людини про стан виконання у ДПСУ законодавства у сфері захисту персональних даних; реалізація права людини і громадянина щодо захисту персональних даних у сфері діяльності ДПСУ; надавання роз'яснень, консультацій органам і підрозділам ДПСУ з питань обробки персональних даних; контролювання дії органів і підрозділів ДПСУ щодо виконання законодавства з обробки та захисту персональних даних; розглядання звернень громадян щодо порушення їх прав на захист персональних даних посадовими особами ДПСУ; у межах компетенції ДПСУ забезпечення поновлення порушених прав людини і громадянина; ведення реєстру операцій з оброки персональних даних; методичне забезпечення органів і підрозділів ДПСУ інформаційними повідомленнями у сфері захисту персональних даних; забезпечення ведення узагальнених (статистичних) даних з питань виконання законодавства про захист персональних даних у межах ДПСУ, що підлягають публічному оприлюдненню; підвищення обізнаності військовослужбовців і працівників ДПСУ щодо вимог законодавства про захист персональних даних.

В. Л. Зьолка, дослідивши окремі аспекти інформаційного забезпечення ДПСУ, обґрунтував необхідність підвищення його ефективності через вирішення таких питань:

- визначити, що в діяльності ДПСУ надаються інформаційні послуги [30, с. 194], хоча в нормативно-правових актах, що визначають компетенцію

ДПСУ про це не згадується, а на практиці ці послуги реально надаються. До них належать і надання публічної відкритої інформації на веб-сайті ДПСУ і у ЗМІ, задоволення інформаційних прав громадян (запит, звернення), це також забезпечення інформаційними продуктами. З 2019 року у ДПСУ почав функціонувати напрямок з надання електронних довірчих послуг виключно для персоналу ДПСУ та посадовим особам інших органів державної влади, які звернулись у встановленому порядку до кваліфікованого надавача електронних довірчих послуг («Військова частина 2428») [465]. А.Ф. Мота для означення окремих повноваження ДПСУ щодо надання адміністративних послуг, використовує термін – «сервісні» повноваження [466, с. 129].

З урахуванням цього пропонуємо статтю 19 Закону України «Про Державну прикордонну службу України» доповнити пунктом 30 «*надання інформаційних послуг згідно з чинним законодавством*»;

- розробити за закріпити критерії оцінки та доцільності віднесення інформації до категорії службової [30, с. 199];

- створити в усіх ланках управління центри правової інформації [30, с. 201];

- розробити та затвердити програму підготовки та перепідготовки фахівців у сфері інформаційно-аналітичної діяльності, до якої включити питання з інформаційного права [30, с. 201];

- ефективно використовувати можливості наявних інформаційно-телекомунікаційних систем ДПСУ [30, с. 201].

З урахуванням цього виділимо ті питання, які потребують підвищення ефективності у межах досліджуваних інформаційних відносин.

Розвиток відкритості та доступності у діяльності ДПСУ

Інформаційну відкритість у діяльності ДПСУ характеризують такі елементи, як: нормативно врегульований механізм забезпечення отримання всіма інформації про діяльність прикордонного відомства та його структурних підрозділів і посадових осіб; стан забезпечення реалізації прав громадян на інформацію у прикордонній сфері; визначені та доступні процедури та способи оприлюднення інформації у прикордонній сфері; простота та доступність

електронного урядування у ДПСУ; визначення змісту інформації, яка підлягає оприлюдненню, отже, і її чітке розмежування на інформацію, що може бути доведена до всіх (публічна відкрита); може стосуватись окремої особи (конфіденційна); стосовно групи осіб (службова чи таємна), які результати діяльності та дії посадових осіб ДПСУ підлягають оприлюдненню.

Для забезпечення інформаційної відкритості у ДПСУ успішно функціонує офіційний сайт відомства (https://dpsu.gov.ua/), на якому в доступній формі можна отримати такі відомості: про щоденні результати діяльності безпосереднього виконання завдань прикордонниками на державному кордоні України; загальні засади діяльності відомства (структура, керівництво, компетенція, керівні нормативно-правові акти тощо); загальну інформацію за окремими напрямками діяльності ДПСУ; зведену інформацію щодо перетинання державного кордону в пунктах пропуску та контрольних пунктах в'їзду-виїзду; публічну інформацію у ДПСУ, порядок подання запиту, його форми, звіти, порядок оскарження, зведені найчастіші питання, що надходять від громадян тощо; порядок, особливості та компетенція ДПСУ щодо роботи зі зверненнями громадян; робота зі ЗМІ: реагування на критику, інформація у ЗМІ про ДПСУ, інтерв'ю посадових осіб, заходи за участю керівництва, контакти для ЗМІ, відомчі видання тощо; контакти та розташування за адресою ДПСУ, підпорядкованих підрозділів.

При цьому гарантією для забезпечення дотримання балансу між інформаційною приватною та публічною сферою, відкритістю та збереженням обмеженої у доступі інформації необхідно, щоб кожен військовослужбовець і працівник ДПСУ чітко розумів та розмежовував такі правові категорії, як: «відкрита публічна інформація»; «інформація з обмеженим доступом», «персональні дані»; «конфіденційна інформація»; «службова інформація», «таємна інформація» тощо, також порядок та підстави обігу окремо взятої такої інформації. Крім цього, у період триваючої війни на сході країни персонал ДПСУ не повинен висвітлювати персональні дані, у першу чергу зображення себе, своїх рідних, колег у мережі Інтернет та іншу інформацію про належність до ДПСУ, щоб уберегти себе, своїх колег, рідних від небезпеки з боку ворога (тривалий час

від початку агресії в мережі Інтернет існували сайти «смертників» із зображеннями та детальною інформацією про окремих військовослужбовців, у тому числі ДПСУ).

У питанні забезпечення балансу між державними та приватними інтересами позиція ЄСПЛ, зокрема у справах «*Aycaguer v. France*» від 22 червня 2017 р. [467] та «*Gaughran v. the United Kingdom»* від 13 лютого 2020 р. [468], є чіткою щодо дотримання справедливості та обґрунтованості у зберіганні органами держави інформації про особу. У згаданих справах мова йшла про зберігання профілю ДНК, відбитків пальців і фотографії заявника, без посилання на серйозність злочину або необхідність безстрокового зберігання, та вирішені позитивно в інтересах громадян.

Отже, інформаційна відкритість полягає у дієвості механізмів оприлюднення та надання інформації, пов’язаної із функціонуванням ДПСУ, а її результатом має бути доступність й отримання безперешкодно громадянами інформації у прикордонній сфері, яка відповідно до чинного законодавства є відкритою, за їх потребами та інтересами. Інформаційна відкритість відображає рівень демократичності системи органів публічної адміністрації, може закріплюватись у законодавстві як принципи діяльності окремого органу влади – гласність, відкритість, прозорість, транспарентність. Тому вбачаємо з урахуванням розвитку інформаційного суспільства та інформаційних потреб визначити у ст. 3 Закону України «Про Державну прикордонну службу України» як окремий принцип діяльності ДПСУ «*транспарентність*», що буде відповідати положенням Закону України «Про доступ до публічної інформації» (ст. 4). Загалом у діяльності прикордонного відомства належним чином організована робота із забезпечення висвітлення публічної інформації, що свідчить про відповідний стан забезпечення інформаційної відкритості у діяльності ДПСУ [296, с. 35]. Лише окремі аспекти потребують урахування, а саме:

надання загальної статистичної інформації результатів роботи з обробки персональних даних, ведення обліку такої інформації;

висвітлення інформації на сайті ДПСУ, про особу (з її контактними даними) на яку покладено виконання обов'язків із захисту персональних даних, а у близькій перспективі створити окремий відділ із забезпечення такої роботи у ДПСУ;

закріпити у статті 3 Закону України «Про Державну прикордонну службу України» принцип «транспарентності».

Розвиток електронного урядування та електронної ідентифікації

Невід'ємною частиною функціонування ДПСУ, як і сучасного життя переважної більшості населення, стало спілкування засобами електронного зв'язку та глобальною мережею Інтернет. Завдяки такій комунікації пришвидшено та з найменшими витратами відбувається обмін й отримання інформації у сфері охорони державного кордону.

Діяльність ДПСУ спрямована на вдосконалення інформаційної складової частини системи охорони державного кордону передбачає запровадження системи електронного документообігу з використанням електронного цифрового підпису [59]. Крім цього, передбачено «створення умов для реалізації прав і свобод людини», у сучасних умовах невід'ємним елементом цих умов є розвиток електронного урядування та забезпечення реалізації інформаційних прав громадян. Аналіз норм Стратегії, яка передбачає створення нової системи захисту державного кордону й Основних напрямків діяльності та подальшого розвитку Державної прикордонної служби України у 2020 році [348], дозволив констатувати відсутність норм, які б передбачали упровадження та використання електронного документообігу з використанням електронного цифрового підпису під час роботи із запитами на публічну інформацію, а також із зверненнями громадян.

Згідно з розпорядженням КМУ «Про схвалення Концепції розвитку електронного урядування в Україні» від 20 вересня 2017 р. № 649-р (далі – Концепція електронного урядування) розвиток електронного урядування визначено одним з першочергових пріоритетів реформування системи державного управління та забезпечення комплексного розвитку електронного урядування

відповідно до європейських вимог [469]. У зв’язку із цим розвиток й удосконалення електронного урядування у діяльності ДПСУ набуває особливої актуальності.

Електронне урядування є формою організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян [469]. Відповідно до цього основна мета впровадження та розвитку електронного урядування у межах діяльності ДПСУ спрямована на задоволення інформаційних потреб громадян у сфері охорони державного кордону через упорядкування управлінських процесів, орієнтованих на забезпечення інформаційної відкритості й реалізації потреб громадян в отриманні інформації про себе, про діяльність органів і підрозділів ДПСУ, про особливості перетинання державного кордону тощо. Ці питання окреслюють загальні принципові положення сучасного демократичного суспільства (електронної демократії) з урахуванням особливої подачі та використання сучасних інформаційних технологій у формі електронного спілкування. Такий спосіб реалізації інформаційних потреб дозоляє, з одного боку, органам і посадовим особам ДПСУ не дублювати актуальну інформацію, яка знаходиться у вільному доступі на веб-сайті ДПСУ (наприклад, документи на право перетинання державного кордону, підстави тимчасової відмови у виїзді за кордон [470], контактна інформація про органи охорони державного кордону [471], про результати діяльності ДПСУ [472]), оперативно обмінюватись інформацією із взаємодіючими структурами та забезпечувати інтегроване управління кордонами тощо, з іншого – громадяни можуть вільно у будь-який час оволодіти відкритою інформацією, що стосується сфери охорони державного кордону про умови перетинання державного кордону, в’їзду до тимчасово окупованих територій та виїзду з них, діючі пункти пропуску через державний кордон, подати запит на інформацію в електронній формі, ознайомитись із відкритими статистичними даними у сфері діяльності ДПСУ тощо.

У зв’язку з такими тенденціями очікуваною метою Концепції електронного урядування є забезпечення виконання комплексних заходів за такими напрямами:

модернізація публічних послуг і розвиток взаємодії влади і громадян за допомогою інформаційно-комунікаційних технологій;

модернізація державного управління за допомогою інформаційно-комунікаційних технологій;

управління розвитком електронного урядування [469]. Отже, удосконалення електронного урядування перебуває на межі двох площин: організаційно-технічної та правової.

Практична важливість та актуальність упровадження електронного урядування не позбавлена наявності недоліків і прогалин як у правовому регулювання, так і механізмах його впровадження. Як зазначає Є. Калішенко, достатній рівень та ефективність електронного урядування прямо залежить від якості, обґрунтованості, адекватності та своєчасності його нормативно-правового регулювання [473, с. 141]. Зважаючи на те, що Україна перебуває на початковому етапі розвитку електронної демократії, відмічається несистемне прийняття нормативно-правових актів, які урегульовують іноді розбіжні або суперечні питання у здійсненні управлінських процесів і рішень з використанням інформаційно-телекомунікаційних технологій та диференціації інформації за порядком доступу до неї. Наприклад, забезпечення балансу між нормами законів України «Про доступ до публічної інформації» та «Про захист персональних даних».

Крім того, варто зазначити про відсутність у ДПСУ достатнього правового підґрунтя у врегулюванні порядку застосування електронної форми інформаційного обміну та отримання інформації з використанням електронного цифрового підпису. Загалом можна відмітити про відсутність відокремлення електронної форми звернення від звернень, що подаються в інших формах, про що свідчать статистичні дані. Так, у звіті про стан роботи зі зверненнями громадян, що надійшли до Адміністрації ДПСУ у 2019 році зазначається, що усних (поданих особисто) 204 звернення, надіслано поштою 19 379 звернень [459]

(додаток К.2). При цьому не вказується кількість отриманих звернень та наданих відповідей за допомогою засобів електронного зв'язку (електронне звернення). Хоча веб-сайт ДПСУ достатньо інформаційно наповнений відомостями про електронні адреси: Адміністрації ДПСУ [474], регіональних управлінь [475], органів охорони державного кордону [471], Контактний центр ДПСУ [111], на які можна направляти електронні листи, а також передбачена електронна форма запиту на інформацію [476] і такі звернення надходять та розглядаються.

Відповідно до ч. 6 ст. 5 Закону України «Про звернення громадян» електронне звернення, яке може бути надіслано з використанням мережі Інтернет або засобів електронного зв'язку, є різновидом (формою) письмового звернення. Наказ Адміністрації ДПСУ «Про забезпечення доступу до публічної інформації у ДПСУ» уточнює, що такі звернення можна подавати електронною поштою [113]. Обов'язковим елементом письмового запиту є підпис особи, що його подає [113, п. 2.4; 347, ч. 7 ст. 5; 97, ч. 5 ст. 19], при цьому застосування електронного цифрового підпису при надсиланні запитів на публік-ну інформацію, виконаних в електронній формі, не вимагається [347, ч. 7 ст. 5]. Не передбачено цього і Законом України «Про доступ до публічної інформації». Однак у випадку коли особа вимагає надання від ДПСУ персональних даних про себе шляхом подання запиту, виконаного в електронній формі, виникає потреба у її ідентифікації, щоб запобігти доступу до конфіденційної інформації у формі персональних даних сторонніх осіб. Тому, керуючись вимогами законів України «Про доступ до публічної інформації» та «Про захист персональних даних», які визначили, що при опрацюванні запитів на персональні дані володілець цих даних повинен упевнитися в тому, що суб'єкт персональних даних надав свою згоду на їх поширення, ДПСУ відмовляла у наданні конфіденційної інформації про осіб, якщо ця інформація запитувалася у спосіб подання запиту, виконаного в електронній формі, що не дозволяла ідентифікувати особу запитувача.

На офіційному сайті ДПСУ у розділі «Електронне звернення» міститься інформація про обмеження надання інформації шляхом подання електронного звернення (запиту). Виключно у письмовій формі (поштовим зв'язком по системі

Укрпошта або особисто до громадської приймальні Адміністрації ДПСУ) опрацьовуються звернення (запити) з питань:

перетинання державного кордону України громадянами;

можливого існування стосовно громадянина тимчасового обмеження у праві виїзду за кордон;

можливого існування стосовно іноземця та особи без громадянства рішення про заборону в'їзду [477].

Однак способом ідентифікації особи, яка направила електронне звернення (запит), є накладення на документ електронного цифрового підпису. Така вимога обґрунтована забезпеченням виконання положень Закону України «Про захист персональних даних». Для забезпечення захисту персональних даних та ідентифікації особи, яка направила електронне звернення (запит), доцільно застосовувати електронний цифровий підпис, але сьогодні існують перепони у його використанні [478, с. 99].

Концепцією електронного урядування передбачено розвиток інфраструктури електронної ідентифікації, що дасть змогу забезпечити зручний і безпечний доступ громадян до визначених даних з інформаційних систем органів влади, різноманітних електронних послуг та інтерактивних інструментів без необхідності використання декількох облікових записів у різних інформаційних системах, сприятиме розвитку електронних форм взаємодії громадян і держави. Одним із напрямків цього є реалізація принципу "single-sign-on" шляхом упровадження інтегрованої системи електронної ідентифікації та автентифікації і повторного використання в інформаційно-телекомунікаційних системах органів влади [469]. При цьому на ДПСУ, як і інші органи влади, покладається обов'язок щодо створення, розвитку й експлуатації інформаційно-телекомунікаційних систем, що здійснюються з урахуванням необхідності їх сумісності з базовою інформаційно-телекомунікаційною інфраструктурою електронного урядування та вимог законодавства у сфері захисту інформації [469].

Так, відповідно до ст. 4 Закону України «Про електронні документи та електронний документообіг» КМУ та інші органи виконавчої влади в межах

повноважень, визначених законом, реалізують державну політику електронного документообігу, спрямовану:

на реалізацію єдиної державної політики електронного документообігу;

забезпечення прав і законних інтересів суб'єктів електронного документообігу;

нормативно-правове забезпечення технології оброблення, створення, передавання, одержання, зберігання, використання та знищення електронних документів [479, ст. 4].

Крім того, Типовою інструкцію з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну, затвердженою постановою КМУ від 17 січня 2018 р. № 55 [480], передбачено здійснюється документування управлінської інформації в установах в електронній формі із застосуванням каліфі-кованого електронного підпису, кваліфікованої електронної печатки та кваліфікованої електронної позначки часу, крім випадків наявності обґрунтованих підстав для документування управлінської інформації у паперовій формі. І хоча відповідно до пункту 1 цієї Інструкції особливості організації діловодства з документами, що містять інформацію з обмеженим доступом, діловодства за зверненнями громадян, запитами на публічну інформацію визначаються окремими норматив-но-правовими актами та не можуть регулюватися цією Інструкцією, це не повинно обмежувати право направити свій запит про доступ до публічної інформації в електронній формі із застосуванням кваліфікованого електронного підпису. Тому постає необхідність подальшого удосконалення нормативно-правових актів, що регулюють діяльність ДПСУ у сфері доступу до публічної інформації та персональних даних у частині роботи з запитами, що виконані в електронній формі із застосуванням кваліфікованого електронного підпису [478, с. 100].

Державна прикордонна служба України завдяки підтриманню постійного міжнародного діалогу з країнами-партнерами втілює у своїй діяльності прогресивний практичний досвід цих країн у сфері охорони державного кордону

(аналіз ризиків, кримінальний аналіз, інтегроване управління кордонами тощо), вважаємо, що на короткочасну перспективу необхідно запланувати впровадження у ДПСУ використання системи та порядку електронної ідентифікації особи під час подання заяви (запиту) з урахуванням міжнародного досвіду [478, с. 100].

Так, наприклад, громадянин ЄС, а також інша фізична чи юридична особа, яка проживає або має зареєстрований офіс в ЄС, має право на доступ до документів, що зберігаються FRONTEX, за умови, установленої в Регламенті (ЄС) № 1049/2001 [481]. Запит, що подається в електронній формі й надсилається електронною поштою, підписується з використанням кваліфікованого підпису відповідно до Регламенту eDIAS (Регламент (ЄС) № 910/2014) [482].

Створення сучасної інфраструктури електронної ідентифікації та забезпечення її розвитку сьогодні є актуальним і перспективним питанням. Це повинно бути організаційно та технічно впроваджено у практичній діяльності ДПСУ відповідно до вимог Закону України «Про затвердження Положення про інтегровану систему електронної ідентифікації» від 19 червня 2019 р. № 546 [483].

Отже, окреслені нами проблемні питання у сфері електронного урядування ДПСУ потребують системного вдосконалення та перспективного розвитку з урахуванням детального нормативного й організаційного урегулювання. Їх вирішення сприятиме удосконаленню діяльності ДПСУ, розширенню можливостей доступу громадян до інформації у сфері охорони державного кордону, громадського контролю, популяризації ДПСУ та наближенню її до громадян, а також відповідності європейським вимогам [478, с. 101].

У межах розвитку електронного урядування важливим є питання покращання консультаційної роботи у діяльності Контактного центру щодо узгодження та вироблення чіткого механізму надання інформації, а також формування і дотримання єдиної позиції у роботі зі зверненнями громадян усіх посадових осіб ДПСУ. Досягнення реалізації цього положення можливе через узгодження норм чинного законодавства, що врегульовують порядок і підстави звернень; затвердження Положення про Контактний центр ДПСУ, Методичних рекомендацій у роботі зі зверненнями громадян у Державній прикордонній службі

України **(Додаток Р)**. Принциповими у таких Методичних рекомендаціях повинні стати: основні принципи у роботі зі зверненнями громадян, обов'язки посадових осіб ДПСУ щодо розгляду заяв і скарг, особливості роботи зі зверненнями громадян у ДПСУ, порядок та підстави відмови у прийнятті та розгляді звернення, терміни розгляду звернень громадян, відповідальність за порушення законодавства про звернення громадян [352].

На початку 2020 року започатковано впровадження державного онлайн-сервісу «Дія» як складової «цифрової держави». Але сьогодні такий сервіс тільки починає розвиватись, «щоб перетворити Україну на справжню цифрову державу», для цього ще «потрібно оцифрувати багато послуг, оновити законодавчу базу, упорядкувати роботу держреєстрів, забезпечити технічні можливості й захист даних» [484]. У контексті нашого дослідження можемо запропонувати створення у межах цього онлайн-сервісу послуги попередньої реєстрації громадян України, що планують перетнути державний кордон. У його межах особа, що бажає виїхати за кордон, може внести свої відцифровані персональні дані та пункт пропуску, де буде перетинати кордон. Така особа може отримати середній показник пасажиропотоку в конкретному пункті пропуску відповідно до часу доби, а також чи є щодо неї заборона виїзду, зокрема йдеться мова про найпоширеніші випадки несплачених аліментних зобов'язань, або коли особа їх сплатила, але залишається у базі даних таких боржників. Це дасть змогу завчасно узгодити ці питання. Тим більше, що подібна практика вже запроваджена в Естонії, а саме електронне бронювання черг в пунктах пропуску [485, с. 387].

Розвиток та безпека інформаційних систем у діяльності ДПСУ

Насичене використання інформаційних систем у діяльності ДПСУ сприяє прискоренню не тільки інформаційних процесів, але й виконанню усіх завдань, які стоять перед прикордонним відомством. Разом з тим обробка інформації у таких системах може створювати додаткові загрози для порушення її цілісності й безпеки. Тому одночасно з веденням, обробкою, передачею даних в інформаційних системах, забезпеченням їх функціонування необхідно постійно вживати заходів щодо убезпечення змісту інформації та дотримання режиму

доступу до такої інформації. Такі заходи повинні мати комплексний збалансований характер (правові, організаційні, технічні, здійснення контролю, притягнення винних до відповідальності тощо) та реалізовуватись усіма посадовими особами ДПСУ, які мають доступ до функціонування інформаційних систем. Системна робота структурних підрозділів, що забезпечують функціонування ІТС, захист інформації у межах діяльності Головного центру зв'язку, автоматизації та захисту інформації, діяльність кращих фахівців у сфері захисту інформації, а також постійне підвищення їх професійного зростання та обізнаність з вимогами законодавства щодо захисту інформації, новинами інформаційних технологій і програмних продуктів, заходами юридичної відповідальності за порушення інформаційного законодавства підвищить ефективність протистояння інформаційним загрозам у досліджуваній сфері [439, с. 83].

Формування знань і свідомості персоналу ДПСУ про основні засади та принципи інформаційного законодавства (інформаційна культура)

Не зважаючи на те, що сьогодні значна частка інформації у сфері діяльності ДПСУ накопичується, обробляється та зберігається із застосуванням інформаційних технологій, основним у системі обігу інформації залишається людський фактор. «Інформаційна безпека передбачає процес, розуміння, як захистити певні дані, які з цим пов'язані ризики, і що робити, коли оборона виявилася неефективною. Жодні програмні, апаратні або законодавчі способи без такого розуміння не працюють і стають марною втратою часу та зусиль» [486, с. 29].

Вимогою, яка ставиться на сучасному етапі розвитку інформаційного суспільства, є постійний розвиток та удосконалення інформаційних відносин, що не може відбуватись без базових знань, умінь і навичок застосування інформаційного законодавства у ході повсякденної діяльності військовослужбовцями органів і підрозділів охорони державного кордону й відповідно до цього сформованого світогляду. Важливе також розуміння кожним військовослужбовцем і працівник-ком ДПСУ цінності інформації в охороні

державного кордону, зокрема в умовах виникнення нових видів військових загроз, у тому числі інформаційного характеру, військової агресії РФ до України. Мова йде не лише про збереження таємної інформації, але й інформації про повсякденну службову діяльність. Жодна належним чином захищена ІТС за умови розповсюдження інформації персоналом, що допущений до роботи з нею, не є надійною. Про що свідчать життєві приклади.

У травні 2019 року з'явилась інформація про виявлені чисельні факти отримання та збут невизначеному колу осіб інформації, що міститься в ІТС прикордонного контролю. Метою такої діяльності, за даними суду, було сприяння в діяльності бойовикам «Донецької народної республіки», що здійснювалось військовослужбовцями ДПСУ, а також працівниками інших правоохоронних органів. Інформація передавалась через осіб, що мають доступ до ІТС прикордонного контролю «Гарт-1» [487]. У червні 2020 року кіберфахівці СБУ викрили в Івано-Франківській області діючого і колишнього прикордонників на продажі інформації з обмеженим доступом з бази даних ДПСУ. За попередніми даними слідства, зловмисники продавали дані про перетин держкордону громадянами України та іноземцями, термін їх перебування в країні і наявність заборон на в'їзд чи виїзд [488].

Ми вже згадували про інший нещодавній факт несанкціонованого копіювання та збут службової інформації [489], такі непоодинокі події вказують на важливість підвищення людського потенціалу у збереженні інформації розпорядником якої є ДПСУ.

Г. Г. Воробйов, у своїй праці зазначив, що стрімке накопичення знань у суспільстві неможливе без специфічних правил взаємодії з інформацією [490, с. 39], яка відбувається у межах інформаційної культури.

Отже, одним із ключових елементів держави стала інформаційна культура, яка наблизила частину державних процесів у цифровий віртуальний вимір та зумовила тих суб'єктів державних відносин, які вступають у взаємодію з нею, оволодівати інформаційними компетентностями. Базовими засадами «інформаційної культури особи є знання про інформаційне середовище, закони

його функціонування та розвитку, а головне – досконале вміння орієнтуватися в безмежному сучасному світі інформації» [491, с. 28].

Інформаційну культуру державного службовця П. С. Клімушин та І. Д. Іванова характеризують як важливий фактор успішної діяльності державних службовців, які є організаторами інформаційної взаємодії в суспільстві та складовою загальної культури людини як сукупності інформаційного світогляду, системи знань і вмінь, що забезпечують цілеспрямовану діяльність задоволення інформаційних потреб громадян з використанням системи уряд [492, с. 2]. Також науковці справедливо зазначають про існування прямого зв'язку між формуванням інформаційної культури державного службовця та вирішенням проблем інформаційного суспільства [492, с. 1], що безперечно стосується й кожного з персоналу ДПСУ як представника прикордонного органу та підрозділу у комунікації з інформаційним суспільством.

Під «інформаційною культурою» пропонуємо розуміти поняття, запропоноване К. І. Бєляковим, С. Г. Онопрієнком, І. М. Шопіною у монографії «Інформаційна культура в Україні: правовий вимір» а саме як, інтегральну цілісність, що включає світоглядні ціннісні, когнітивні, комунікативні та інструментальні компоненти життєдіяльності людини, соціальних груп та держави, які у сукупності спрямовані на формування інформаційного суспільства, виступають орієнтиром розвитку інформаційного законодавства і находять свій вияв в інформаційній діяльності та забезпеченні інформаційної безпеки [493, с. 31].

«Інформаційно-правова культура особистості виявляється в усвідомленні й особливій повазі до інформаційних прав і свобод людини, навичках використання сучасних інформаційних технологій для пошуку правової інформації й отримання правових знань, здійсненні інформаційної діяльності на фундаментальних засадах права, навіть за відсутності відповідних правових норм» [13, с. 263].

Отже, інформаційна культура персоналу ДПСУ є системним явищем, яке забезпечує зв'язок з інформаційним суспільством (його частиною, окремими особами), що реалізує свої потреби, інтереси та права, пов'язані із

функціонуванням органів і підрозділів охорони державного кордону, вдивляється у сформованих стійких знаннях військовослужбовцями ДПСУ інформаційного законодавства, розумінні важливості інформації у виконанні завдань усієї служби, навичках його реалізації (інформаційного законодавства) у конкретних прикордонних відносинах. Інформаційна культура включає, у зв'язку із тим, що ми визначили її як системне явище, сукупність складових частин, елементів.

В. В. Кириченко виділяє такі елементи інформаційної культури: уміння використовувати ІКТ, уміння працювати з інформацією, критичність мислення, уміння вчитися та освоювати нові знання та досвід, уміння здійснювати комунікацію та налагоджувати взаємодію, які у свою чергу, пише науковець, формують два принципові відмінні рівні інформаційної культури: технологічний рівень інформаційної культури (здатність суб'єкта соціальних відносин взаємодіяти із цифровими інформаційними технологіями, користуватися ІКТ та його функціоналом) та соціально-психологічний рівень, пов'язаний зі здатністю суб'єкта соціальних відносин здійснювати аналіз і перероблення інформації та використовувати її для здійснення соціальної активності» [494, с. 115]. Такий підхід відображає конкретні елементи-дії, процеси, які наповнюють інформаційну культуру, основу якої складають відповідні уміння, необхідні для роботи з інформацією в усіх її формах та виявах.

П. С. Клімушин та І. Д. Іванова розглядають формування інформаційної культури державних службовців з урахуванням окремих механізмів: правових, організаційних, технологічних, освітніх, соціальних [492, с. 2]. Науковці пропонують ураховувати загальні фактори (механізми), які пов'язані з обігом інформації та утворюють інформаційну культуру.

Важливою складовою інформаційної культури стало розуміння необхідності та дотримання заходів безпечного використання комп'ютерів і гаджетів, зокрема й в мережі Інтернет. «Люди, які служать державі і не до кінця розуміють важливість елементарної безпеки навіть власного комп'ютера, згодом можуть спровокувати своєю безвідповідальністю серйозні проблеми для елементів критичної інфраструктури», у зв'язку із цим начальник відомчого

Центру кібербезпеки застосовує термін «комп'ютерна гігієна» та наголошує на необхідності проведення просвітницької роботи для підвищення обізнаності небезпеки у зв'язку із зневажливим ставленням до комп'ютерної безпеки [442, с. 29].

Ускладнення ситуації у сучасних умовах, обмежувальними карантинними заходами пов'язаними із COVID-19 та зростання ролі інформаційних потоків, у результаті ізоляції від соціального спілкування, мотивувало К. І. Бєлякова та І. М. Шопіну до впровадження нового напрямку наукового дослідження , – «інформаційна гігієна» [495, с. 99]. Науковці пропонують розглядати інформаційну гігієну у межах «як проблемний напрямок інформаційної безпеки та культури людини в межах доктрини інформаційно-правових досліджень» [495, с. 118].

У зв'язку зі зростанням значимості інформації в інформаційному суспільстві та діяльності ДПСУ важливим у контексті нашого дослідження є **освітньо-правовий вплив**, який сприяє розвитку інформаційної культури представників ДПСУ, підвищує обізнаність з теоретичних засад у сфері формування та обігу інформації з урахуванням особливостей завдань, що виконує ДПСУ, з подальшим екстраполюванням у практичну діяльність.

На підтвердження даної тези маємо результат опитування. На запитання «Чи потрібно сьогодні офіцеру ДПСУ володіти знаннями щодо: правого регулювання обігу інформації, її видів; поняття та обсягу персональних даних; правового регулювання конфіденційної інформації; інформаційної безпеки та захисту інформації; правового режиму службової інформації та державної таємниці; настання юридичної відповідальності за порушення норм інформаційного законодавства?, 91,8 % респондентів відповіли «так», і лише 8,2 % – «ні», 75,8 % висловили необхідність вивчати основи інформаційного законодавства, правові основи інформаційної безпеки та кібербезпеки у НАДПСУ і лише 24,2 % – «ні» **(додаток В)**.

Тому нами запропоновано ввести в навчальну програму підготовки НАДПСУ навчальні дисципліни «Інформаційне право» за освітньо-кваліфікаційним рівнем «Бакалавр» та «Інформаційна діяльність Державної прикордонної служби України» за освітньо-кваліфікаційним рівнем «Магістр права», «Правові основи інформаційної безпеки» для усіх інших не правових спеціальностей.

Завдяки таким навчальним дисциплінам курсанти та слухачі можуть оволодівати та вдосконалювати такі компетентності:

знати:

підстави виникнення, зміни і припинення інформаційних правовідносин;

чинне національне інформаційне законодавство та особливості аналогічного законодавства країн ЄС;

правові засади організації інформаційної діяльності;

види інформації та їх правові режими інформації;

особливості конфіденційної, службової інформації та державної таємниці;

правовий режим використання інформації з вільним та обмеженим доступом;

порядок та підстави реалізації інформаційних прав людини і громадянина в ДПСУ;

поняття та захист персональних даних;

засоби захисту інформації та інформаційних прав; правові засади забезпечення інформаційної безпеки;

вміти:

використовувати загальнотеоретичні поняття та категорії при вивченні галузевих і спеціальних навчальних дисциплін для аналізу складних правових проблем, оперувати основними категоріями в практичній діяльності;

давати правову оцінку діям та обставинам, інформаційним відносинам у сфері охорони державного кордону;

в умовах діяльності оперативно-розшукових підрозділів застосовувати на практиці права та обов’язки учасників інформаційних відносин;

тлумачити інформаційне законодавство та правильно його застосовувати в інтересах охорони державного кордону;

складати правові документи;

ознайомитись:

з основними напрямками формування інформаційного суспільства в сучасних умовах та правового регулювання відносин з приводу обігу інформації в сфері діяльності ДПСУ.

Підвищення рівня інформаційної культури дозволить перешкоджанню деструктивному інформаційному впливу на свідомість прикордонників, який активно застосовується РФ не тільки в Україні, але й по всьому світу.

На нашу думку, основами інформаційного законодавства повинні володіти весь персонал прикордонного відомства, у першу чергу офіцерський склад, діяльність якого пов’язана з управлінням інформацією, обігом і захистом персональних даних осіб, що перетинають державний кордон, і підлеглих військовослужбовців, зі службовою та таємною інформацією. Тому кожен військовослужбовець, зокрема офіцер ДПСУ повинен оперувати категоріями інформаційного законодавства, забезпечувати режим і безпеку різних видів інформації, розпорядником якої є ДПСУ.

Отже, на підставі системного аналізу розуміння сутності інформаційної культури та її складових елементів нами сформований **Алгоритм формування інформаційної культури у ДПСУ** (далі – Алгоритм) **(додаток С)**.

На наш погляд, необхідність такого Алгоритму зумовлено прогресуючим розвитком інформаційних відносин, зростанням цінності інформації у забезпечені прикордонної безпеки держави, необхідністю посилення захисту інформації та приватності усіх суб’єктів цих відносин, а також складне та динамічне безпекове середовище довкола України, запровадження європейських стандартів інтегрованого управління кордонами обумовлюють необхідність формування нового типу свідомості прикордонника у межах модернізації інформаційної складової системи охорони державного кордону.

Формуючи такий Алгоритм, ми виходили з отриманих знань про особливості інформаційних відносин у сфері функціонування ДПСУ та необхідності вироблення такого типу поведінки у персоналу прикордонних підрозділів, який би відповідав вимогам інформаційного суспільства щодо обробки й захисту інформації, розпорядником якої є ДПСУ, а також унеможливлення деструктивного впливу, недопущення маніпулювання свідомістю військовослужбовців. Такий Алгоритм базується на системі загальноправових цінностей (правова аксіологія) щодо забезпечення справедливості, рівності відповідно до законодавства свободи доступу до відкритої публічної інформації, суворе дотримання та обґрунтований баланс між приватністю і захистом інформації (службової, таємної) у сфері інтересів прикордонної безпеки **(додаток С)**.

Змістовними компонентами **Алгоритму** повинні стати такі якісні навички:

володіння базовими (для усіх) або поглибленими (для осіб, що здійснюють інформаційну діяльність) знаннями інформаційного законодавства;

знання принципових вимог інформаційної діяльності, зокрема створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації, та їх особливостей у діяльності ДПСУ;

балансування принципу транспарентності інформаційних відносин із захистом персональних даних і прикордонною безпекою;

розуміння основних понять та їх змісту («інформація», «персональні дані», «володілець інформації», «розпорядник інформації» тощо);

розмежовування категорії «відкрита інформація», «інформація з обмеженим доступом» тощо;

володіння обсягом правових режимів «конфіденційна інформація», «службова інформація», «таємна інформація»;

нерозповсюдження особистої приватної інформації (зображення) у мережі Інтернет;

уміння використовувати комп’ютерну техніку із врахуванням «комп’ютерної гігієни»;

знання інформаційних правопорушень, за які застосовується кримінальна, адміністративна, дисциплінарна та цивільно-правова відповідальність.

Основою гарантування інформаційних відносин у діяльності ДПСУ повинно стати утвердження таких характерних для цієї сфери принципів, як:

забезпечення реалізації державної політики інформаційної безпеки;

прийняття управлінських рішень лише на підставі об'єктивної та достовірної інформації;

транспарентність;

реалізація інформаційних прав усіх суб'єктів прикордонних відносин;

достовірність і повнота публічної інформації про діяльність ДПСУ;

вираження особистих поглядів, переконань, персональних даних (у тому числі у мережі Інтернет) персоналу ДПСУ з урахуванням засад прикордонної безпеки;

обмін інформацією з іншими органами публічної адміністрації відповідно до вимог чинного законодавства та виключно в інтересах охорони державного кордону;

сприяння розвитку інформаційної складової охорони державного кордону;

посилений захист інформації з обмеженим доступом;

системність вжиття своєчасних та адекватних заходів захисту інформації у сфері службової діяльності ДПСУ **(додаток У)**.

Отже, проведений системний аналіз існуючих проблем в інформаційній сфері ДПСУ дозволив установити, що підвищення ефективності інформаційних відносин в діяльності ДПСУ зумовлено такими факторами:

відповідністю вимогам розвитку інформаційного суспільства;

впровадженням європейських стандартів у модернізації інформаційної складової системи охорони державного кордону;

виконанням норм, правил, вимог інформаційного законодавства;

виявленням та своєчасним реагуванням на інформаційні загрози;

оптимізацією механізмів у сфері обігу інформації;

впровадженням електронного урядування;

підвищенням довіри громадян до ДПСУ;

безпечним інформаційним обміном, у тому числі у відомчих та міжвідомчих інформаційних системах.

Таким чином, основними напрямками підвищення ефективності інформаційних відносин у діяльності ДПСУ є:

розвиток відкритості та доступності в діяльності ДПСУ на веб-сайті ДПСУ: висвітлювати розширений звіт по роботі зі зверненнями громадян, запитами на публічну інформацію, а також узагальнені дані з обробки персональних даних; кожного року видавати Стратегічний бюлетень прикордонної безпеки «Біла книга»; надати офіційну інформацію про відповідальну особу, яка організовує роботу, пов'язану із захистом персональних даних при їх обробці у ДПСУ, створити окремі відділи з роботи у цьому напрямку; закріпити у статті 3 Закону України «Про Державну прикордонну службу України» окремий принцип діяльності ДПСУ «*транспарентність*») **(додаток Т)**;

розвиток електронного урядування та електронної ідентифікації, впровадження та постійне удосконалення онлайн-сервісу «Дія» в інтересах та з метою оптимізації прикордонного контролю й охорони державного кордону;

розвиток та безпека інформаційних систем у діяльності ДПСУ: постійно та безперервно вживати заходів із забезпечення та розвитку системи заходів збереження та захисту інформації; створення сучасної інфраструктури електронної ідентифікації та забезпечення її розвитку;

формування знань та свідомості персоналу ДПСУ про основні засади та принципи інформаційного законодавства (інформаційна культура): формування та удосконалення знань, умінь персоналу в роботі з інформацією, підвищення інформаційної культури, формування інформаційної концепції у поведінці персоналу.

Отже, підвищення ефективності інформаційних відносин у діяльності ДПСУ перебуває у площині науково обґрунтованих організаційно-методологічних конкретних рекомендацій. Ґрунтується на системному охопленні розвитку всіх інформаційних складових у діяльності ДПСУ, досягненні нового

якісного стану відносин відповідно до існуючого, значна роль у якому відводиться професійності персоналу ДПСУ й відповідності їх знань потребам інформаційного суспільства у кореляції із прикордонною безпекою, що дозволить суттєво покращити впровадження державної інформаційної політики, буде сприяти ефективності отримання, обробки та захисту інформації, розпорядником якої є прикордонне відомство, надасть управлінській діяльності більшої цілеспрямованості, обґрунтованості, оперативності й результативності та загалом буде сприяти підвищенню прикордонної безпеки.

5.2 Напрямки удосконалення нормативно-правового регулювання інформаційних відносин у діяльності Державної прикордонної служби України

Постійна зміна характеру загроз на державному кордоні України потребує адекватного реагування, адже наслідком діяльності ДПСУ є дотримання загальнодержавного рівня безпеки (безпеки нації, суспільства та окремого громадянина) в частині недоторканності державного кордону України, недопущення зміни лінії державного кордону, збереження територіальної цілісності держави та реалізації права безперешкодного перетинання державного кордону України [455, с. 158]. Прикордонна безпека є складовою національної безпеки, що забезпечується комплексом різноманітних заходів спрямованих на забезпечення захисту інтересів особи, суспільства та держави у цій сфері. Елементом сучасної прикордонної безпеки є її інформаційна складова, одним із вимірів якої є інформаційні відносини.

Інтенсивний розвиток інформаційного суспільства, тотальна інформатизація публічної та приватної сфери, упровадження електронних засобів ідентифікації особи, що відбувається з урахуванням європейської інтеграції, вимагає від ДПСУ постійного удосконалення у сфері інформації та інформаційної діяльності. З урахуванням цього варто навести міркування Ю. Є. Максименко, яка констатує,

що інформаційна галузь законодавства є найбільш динамічною щодо інших галузей законодавства, а інтенсивність змін в інформаційній сфері сприяє необхідності особливої уваги наукової спільноти дослідженню чинного інформаційного законодавства стану інформаційних відносин в України [496, с. 142].

Інформаційні відносини, які зумовлені як внутрішньо-організаційними аспектами інформаційної діяльності ДПСУ, так і зовнішніми, потребують своєчасного охоплення та врегулювання нормативно-правовими актами, створення та удосконалення чітких організаційних механізмів у сфері інформації, інформаційного забезпечення та підтримання належного стану інформаційної безпеки. Питання удосконалення інформаційних відносин у сфері діяльності ДПСУ перебуває у тісному взаємозв'язку із очікуваним результатом, кінцевим наслідком та їх впливом на стан прикордонної безпеки.

Необхідність постійного удосконалення прикордонної безпеки, запровадження європейських стандартів інтегрованого управління кордонами, підвищення рівня довіри до ДПСУ [348], інтенсивний розвиток інформаційного суспільства (виникнення нових форматів інформаційної комунікації), а також необхідність протистояння гібридній (інформаційній) війні визначають актуальність розроблення напрямків удосконалення нормативно-правового регулювання інформаційних відносин у діяльності ДПСУ.

Розвиток нормативно-правового регулювання інформаційних відносин у ДПСУ повинен ґрунтуватись на урахуванні таких інформаційних інтересів, як:

державної політики інформаційної безпеки;

забезпечення надійної охорони державного кордону;

задоволення інформаційних прав громадян та суспільства у сфері охорони державного кордону;

функціонування, розвитку та захищеності інформаційно-телекомунікаційних систем внутрішньовідомчого та міжвідомчого (у межах інтегрованого управління кордонами) значення **(додаток У)**.

Актуальні засади удосконалення інформаційних відносин у діяльності ДПСУ сформульовані в нормативних вимогах розвитку інформаційного суспільства на державному та відомчому рівні, обґрунтовані у програмах, планах, стратегіях, концепціях, зорієнтованих на розвиток системи національної та державної безпеки, дотримання прав громадян, відповідності вимогам українського й міжнародного інформаційного суспільства.

Збільшення ролі інформації, удосконалення її форм відображення та застосування (електронна комунікація, удосконалення використання ІТС, використання електронних кваліфікованих підписів, електронної ідентифікації) в діяльності ДПСУ дозволяє підкреслити актуальність і необхідність якісного нормативно-правового забезпечення інформаційних відносин у прикордонній сфері, яке має будуватися на системній основі, що дозволить досягти бажаної мети – стабільного стану безпеки державних кордонів України [497, с. 91].

Основні координати розвитку інформаційних відносин закладені у плануючих документах, розрахованих на певний період, з урахуванням європейських орієнтирів. Так, у Плані заходів з реалізації стратегічного курсу держави на набуття повноправного членства України в ЄС та в Організації Північноатлантичного договору, затвердженому Указом Президента України від 20 квітня 2019 р. № 155/2019, передбачено забезпечити впровадження ефективної інформаційної політики у сферах європейської та євроатлантичної інтеграції України та поглиблення співробітництва з ЄС у питаннях інформаційної безпеки та кібербезпеки, забезпечення стійкості критичної інфраструктури, протидії транснаціональній злочинності, посилення охорони кордонів, мінімізації ризиків у сфері міграції [498, п. 15, 17].

У напрямку забезпечення інформаційної безпеки держави в умовах сьогодення у Доктрині інформаційної безпеки сформульовані пріоритети державної політики в інформаційній сфері, зокрема актуальними для прикордонної сфери є:

створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них [148, п. 5], розвиток системи аналізу ризиків у ДПСУ було розпочато ще в 2006 році [10], сьогодні продовжується покращання;

удосконалення повноважень ДПСУ з метою досягнення адекватного рівня спроможності відповідати реальним і потенційним загрозам національним інтересам України у прикордонній інформаційній сфері;

законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави інформації, яка пропагує війну або порушення територіальної цілісності України, загрожує державному суверенітету;

розвиток і захист технологічної інфраструктури забезпечення прикордонної інформаційної безпеки України;

забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах, а також тимчасово окупованих територій;

посилення протидії спеціальним інформаційним операціям, спрямованим на порушення суверенітету і територіальної цілісності, підрив обороноздатності України, деморалізацію особового складу ДПСУ, загострення суспільно-політичної ситуації, зокрема у прикордонних районах;

унеможливлення вільного обігу інформаційної продукції (друкованої та електронної), насамперед походженням з території держави-агресора, що містить пропаганду війни, національної і релігійної ворожнечі, зміни конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України, провокує масові заворушення. Контроль за ввезенням в Україну такої друкованої продукції здійснюється у пунктах пропуску через державний кордон [154] або в контрольних пунктах в’їзду на тимчасово окуповану територію та виїзду з неї відповідними підрозділами ДПСУ [155];

проведення розвідувальними органами України акцій сприяння реалізації та захисту національних інтересів України в інформаційній сфері, протидії зовнішнім загрозам інформаційній безпеці держави за межами України [148, п. 5]. У ДПСУ здійснюється оперативно-розшукова діяльність в інтересах безпеки державного кордону самостійно, яка у процесі здійснення розвідувальної

діяльності має сприяти реалізації та захисту національних інтересів України в інформаційній сфері, протидіяти зовнішнім загрозам інформаційній безпеці держави [148, п. 6];

створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави передбачено Стратегією кібербезпеки України [498].

Суттєвим недоліком на сучасному етапі розвитку інформаційних відносин є відсутність системного планування у розвитку інформаційного суспільства та інформаційної безпеки. Ще у 2014 році ВРУ було прийнято постанову «Про Рекомендації парламентських слухань на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні»», у якій КМУ зобов'язано розробити програму розвитку інформаційного суспільства в Україні на 2016-2020 роки. У зв'язку із цим Департаментом інформаційної політики було розроблено Стратегію розвитку інформаційного простору України на період до 2020 року, основною метою якої мало стати створення політико-правових, економічних, організаційних та матеріально-технічних умов для розвитку національного інформаційного простору України, а також формування сучасної моделі державної інформаційної політики, забезпечення розвитку та захисту національного інформаційного простору [286]. Але даний проект не було підписано й відповідно втілено у суспільні відносини, тому на державному рівні відбувається фрагментарне урегулювання окремих питань інформаційних відносин в аспекті інформаційної та кібербезпеки.

У межах специфіки діяльності ДПСУ та забезпечення охорони державного кордону України визначальними також є нормативні акти, які спрямовують розвиток прикордонного відомства з урахуванням існуючих загроз і потреб прикордонної сфери, а також формулюються конкретні завдання за окремими напрямками інформаційних відносин. Серед таких варто згадати розпорядження КМУ Стратегія розвитку Державної прикордонної служби України, Стратегія інтегрованого управління кордонами на період до 2025 року, рішення Колегій ДПСУ (у яких конкретизуються окремі завдання щодо розвитку інформаційної

складової на певний період). Норми цих документів визначають та конкретизують напрямки інформаційно-правової діяльності ДПСУ у межах, визначених законодавством, з урахуванням загроз у сфері охорони державного кордону, інтеграційних процесів та удосконалення її інформаційної складової. Такі норми можна називати програмними документами у сфері інформаційних відносин ДПСУ [223, с. 168].

З урахування цього варто зазначити, що у ДПСУ внутрішньовідомче забезпечення інформаційних відносин ґрунтується на основних вимогах законодавчих актів, передбачає впровадження та використання сучасних засобів і методів обробки, передачі, аналізу, збереження інформації, усебічного інформаційного обміну, які зорієнтовані на покращання інформаційного забезпечення внутрішньовідомчої діяльності ДПСУ як розпорядника інформації у сфері охорони державного кордону. Але такі заходи носять переважно технічний та організаційний характер, здебільшого перебувають на етапі становлення та розвитку. Крім того, на загальнодержавному рівні існує низка негативних аспектів, які зумовлені недостатньою системністю нормативно-правового урегулювання інформаційних відносин, що певним чином позначається на інформаційних відносин у діяльності ДПСУ і відповідно потребують удосконалення [496, с. 94]. У ході проведеного опитування 52,8 % респондентів оцінили «задовільно» стан нормативно-правового регулювання відносин, пов’язаних зі створенням, збиранням, одержанням, зберіганням, використанням, поширенням, охороною та захистом інформації в діяльності ДПСУ, 39,4 % «позитивно» і 7,8 % «незадовільно» **(додаток В)**.

Нормативно-правові підстави удосконалення інформаційних відносин у діяльності ДПСУ

Основним наріжним каменем проблеми нормативно-правового регулювання інформаційних відносин, зокрема і в діяльності ДПСУ є невпорядкованість норм інформаційного законодавства. Така позиція відслідковується практично в усіх наукових дослідженнях з проблем інформаційного права, інформаційних відносин, окремих аспектів суб’єктно-об’єктного складу цих відносин.

Необхідність удосконалення інформаційного законодавства зумовлена реальними потребами, а саме: прийняттям останнім часом великого обсягу норм інформаційного законодавства, які деколи є неузгодженими або навіть суперечливими; стрімким розвитком інформаційного суспільства, інформаційних технологій, механізми забезпечення яких не встигають за умовами часу; перебуванням інформаційного права (як комплексної, міжгалузевої галузі права, як науки) на етапі формування та розвитку [496, с. 95].

В. О. Шепета наголошує, що українське інформаційне законодавство важко визнати ефективним, незважаючи на доволі значну кількість нормативно-правових документів, що регулюють інформаційні відносини в інформаційній сфері [500, с. 183].

Основною вимогою інформаційно-правової доктрини є здійснення систематизації інформаційного законодавства. У науці інформаційного права ці вимоги обґрунтовані наступними підставами:

невиправдане дублювання; виявлення та ліквідація прогалин у законодавстві; скорочення термінів створення актів; підвищення їх якості й ефективності, включених до них норм [70, с. 174–179];

наявність численних нормативно-правових актів з регулювання інформаційних правовідносин різної юридичної сили; динамічність інформаційних відносин; неузгодженість зі стандартами ЄС; декларативність окремих норм через брак механізму правореалізації; необхідність системного розв’язання проблеми нормативно-правового регулювання суспільних відносин у сфері забезпечення інформаційної безпеки [436, с.146];

наявність колізій і конкуренції нормативно-правових актів, що регулюють правові відносини в інформаційній сфері; фрагментарність і ситуативність правового регулювання; неузгодженість понятійно-категоріального апарату (інформаційної термінології), що закріплено в нормативно-правових актах; численність і розгалуженість нормативно-правових актів, що ускладнюють їх право на реалізацію та контроль за виконанням; домінування підзаконних нормативно-правових актів над законами [400, с. 183; 436, с. 164–165];

неузгодженість деяких норм інформаційного законодавства що прийняті у різний час; перевага підзаконних нормативно-правових актів над законами [231, с. 164–165];

декларативність норм інформаційного законодавства без механізму та порядку їх реалізації, що спричиняє значну кількість правопорушень; чисельна кількість банкетних норм, абстрактних, суб'єктивних, технічних понять, що потребують додаткового офіційного роз'яснення або чіткого закріплення дефініцій; відсутність закріплення базових понять [496, с. 144–145];

відставання інформаційного законодавство від практики [24, с. 181].

Зазначені підстави достатньо обґрунтовано доводять необхідність удосконалення законодавства, що врегульовує інформаційні відносини та відповідає основним принциповим положенням теорії права, законотворчого процесу, де процес систематизації нормативно-правових актів за своєю суттю передбачає їх упорядкування, приведення у певну узгоджену систему [53, с. 384].

Наукові обґрунтування удосконалення інформаційного законодавства

Ряд науковців Р. А. Калюжний, О. В. Копан, О. Г. Марценюк слушно стверджують, що основою систематизації норм інформаційного права повинні стати відпрацьовані юридичною наукою і перевірені практикою основоположні принципи: поєднання традицій і новацій; інкорпорування норм чинного інформаційного законодавства України в нову систему через агрегацію інститутів права; формування міжгалузевих інститутів права на основі зв'язків з галузевими інститутами [24, с. 182], де інформаційним законодавством є система законів України, чинних міжнародних договорів України, згода на обов'язковість яких надана ВРУ, а також підзаконних нормативно-правових актів України, прийнятих відповідно до Конституції України, що регулюють суспільні відносини у сфері інформації [49, с. 134].

З урахуванням змістовних елементів (нормативно-правових актів) під час систематизації необхідно враховувати ратифіковані Україною нормативні акти (угоди, конвенції) міжнародного права; легалізувати позитивні звичаї у сфері інформаційних відносин і норми суспільної моралі, загальнолюдські цінності,

визначені Організацією Об’єднаних Націй в її Статуті, Декларації прав людини, рішеннях ЄС та інших загальноприйнятих міждержавних нормативних актів, що сьогодні виступають у ролі стандартів, за якими визначається цивілізованість не тільки окремої країни, а й світового співтовариства загалом [24, с. 183].

Систематизація інформаційного законодавства (систематизація законодавства про інформацію) містить цілеспрямовану діяльність компетентних органів чи окремих осіб зі структуризації, моніторингу, дослідження, упорядкування законів з метою підвищення ефективності правотворчості, правореалізації (правозастосування) та правової освіти щодо інформаційної сфери суспільства [49, с. 140].

На першому етапі удосконалення інформаційного законодавства, як зауважує І. В. Арістова, необхідно не починати одразу з його реформування, а розробити стратегію формування інформаційного законодавства [70, с. 174].

Щодо предмету регулювання нових галузей (який достатньо не конкретизований), найбільш оптимальному напрямку удосконалення є здійснення систематизації норм, шляхом інкорпорації та консолідації. Інкорпорація буде відігравати функцію обліку нормативно-правового матеріалу, а консолідація має започаткувати процес подальшої кодифікації [375, с. 178].

В. А. Ліпкан та К. П. Череповський вважають, що інкорпорацію можна здійснювати за інституційними ознаками, відображеними у нормах Конституції України: де застосовується термін «інформація» та подібні до нього терміни («відомості», «повідомлення», «дані»), або інформація є складовою категорій (наприклад, інформаційна безпека, екологічна інформація тощо), але за таким підходом упускаються інші законодавчі акти, де інформація є об’єктом правовідносин [49, с. 169]. Існує позиція щодо застосування структурованих інститутів інформаційного права як критеріїв для інкорпорації [501, с. 46].

На відміну від інкорпорації, консолідація передбачає переробку правового масиву, його уніфікацію, усуває чисельні нормативно-правові акти, позбавляє надмірного подрібнення, допомагає їх об’єднанню та подальшому здійсненню кодифікації.

Науковцями розроблено та представлено громадськості значна кількість кодексів (К. І. Бєлякова [4], М. Я. Швеця та В. М. Брижка [377, с. 7], Г. М. Красноступа [502, с. 122], Л. П. Коваленка [503], В. А. Липкана і В. А. Залізняка [375, с. 205–209], В. С. Цимбалюка [504, с. 21–22] та інших) проектів кодексів з урегулювання інформаційних відносин. Також існує проект Інформаційного кодексу, розроблений Державним комітетом інформаційної політики, телебачення та радіомовлення України. Підкреслюючи актуальність інформаційних відносин у сучасному світі та в Україні, з урахуванням низки проблемних питань, у структурі проектів таких Інформаційних кодексів, ураховані вимоги і стандарти міжнародного права, зобов'язання України стосовно процесу її інтеграції у світове співтовариство, а також сфери правового регулювання [4, с.10].

Проведення систематизації інформаційного законодавства буде сприяти узгодженню його норм, удосконаленню понятійно-категоріального апарату, унормуванню правозастосовної діяльності у реалізації інформаційних прав, інформаційної діяльності та загалом встановленню рівня відносин відповідно до вимог сучасного інформаційного суспільства. Ми не ставили собі за мету розроблення проекту Кодексу та вважаємо, що така робота має об'єднати велику кількість теоретиків, практиків, представників громадськості. Але дозволимо собі, висвітлити власне бачення проекту загальної структури Інформаційного кодексу України **(додаток Ф)**.

Також удосконалення у контексті дослідження інформаційних відносин потребують КК України, КУпАП, зокрема підтримуємо позицію багатьох науковців, щодо доцільності згрупування та виділення тих протиправних діянь які посягають на встановлений порядок у сфері інформації, які набули значного поширення.

На нашу думку, внесення змін потребує і стаття 15 КУпАП «*Відповідальність військовослужбовців та інших осіб, на яких поширюється дія дисциплінарних статутів, за вчинення адміністративних правопорушень*», у якій необхідно передбачити, що військовослужбовці за вчинення інформаційних

адміністративних правопорушень несуть відповідальність згідно з КУпАП на загальних підставах, що дозволить чітко розмежувати два види відповідальності: за порушення законів, постанов, розпоряджень – адміністративна; за порушення внутрішньовідомчих організаційних нормативно-правових актів – дисциплінарна.

Удосконалення нормативно-правового регулювання інформаційних відносин у нормах прикордонного законодавства

Формування законодавства у сфері охорони державного кордону розпочалось на початку створення нової української держави, зокрема згадаємо про ключові закони «Про державний кордон» (1991 р.), «Про Державну прикордонну службу України» (2003 р.), «Про прикордонний контроль» (2009 р.). Базові закони у сфері інформаційних відносин, зокрема «Про захист персональних даних» (2010 р.), «Про доступ до публічної інформації» (2011 р.), були прийняті значно пізніше, та й Закон Україну «Про інформацію», що був прийнятий у 1992 році постійно зазнає змін, останні від 3 грудня 2019 року (всього було внесено 18 змін). У зв’язку із цим виникла необхідність приведення законодавства у сфері охорони державного кордону відповідно до вимог інформаційного законодавства, що було упущено законодавцем під час розробки та прийняття законів, що врегульовують інформаційні відносини.

Кожного дня державний кордон перетинає велика кількість осіб, тим більше, що тенденція до збільшення пасажиропотоку зростає з кожним роком. За повідомленням ДПСУ за 2018 рік український кордон перетнули 100,5 мільйонів осіб та більш як 20 мільйонів транспортних засобів, ще понад 41 тисячі людей відмовили у в’їзді в країну: більш як тисяча людей намагались перетнути кордон за підробленими документами, ще 100 – за чужими і майже 6 тисяч – за недійсними [505]. Для порівняння у 2019 році державний кодон перетнуло більше як 102 мільйони осіб [506], а у 2017 році кількість таких осіб склала 97,3 мільйони осіб **(додаток Х.1).** Ураховуючи кількість затриманих на державному кордоні нелегальних мігрантів (у 2017 році – 931, у 2018 році – 1 205, за 9 місяців 2019 року – 850) **(додаток Х.2)**, оформлення яких потребує додаткових часових і ресурсних затрат у повсякденній діяльності прикордонників у пунктах пропуску

через державний кордон [507]. Такий пасажиропотік та тенденція до його зростання не дає можливості прикордонникам у кожного, хто перетинає державний кордон, отримувати згоду на обробку персональних їх даних у письмовій формі, а у прикордонному законодавстві норми, що встановлює, якою має бути форма згоди у такому випадку, не має. Тому пропонуємо у Законі України «Про прикордонний контроль» визначити норму про те, що особа яка прибула в пункт пропуску через державний кордон України та надає паспортний документ й інші необхідні для перетинання державного кордону відомості, тим самим надає добровільну згоду на обробку її персональних даних **(додаток Т)**.

Загальною вимогою законодавства у сфері захисту персональних даних є доведення до суб'єктів персональних даних, що обробляються органами влади, – **мети** обробки персональних даних. Така мета має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних [335, ч. 1 ст. 6]. Аналіз норм прикордонного законодавства дозволив установити відсутність визначення (формулювання) такої мети. Тому пропонуємо у Законі України «Про прикордонний контроль» передбачити, що обробка персональних даних уповноваженою службовою особою ДПСУ під час прикордонного контролю здійснюється з метою ідентифікації особи, установлення законних підстав для надання дозволу на перетинання державного кордону України, виявлення відсутності або наявності заборони для в'їзду (виїзду) на територію України, фіксації факту перетинання державного кордону, забезпечення безпеки державного кордону.

Установлення такої норми (статті 3-1 *«Обробка персональних даних осіб, що перетинають державний кордон»* у Законі України «Про прикордонний контроль») відповідатиме механізму оброки персональних даних відповідно до вимог Закону України «Про захист персональних даних», у якій буде сформульована мета та обсяг обробки персональних даних, а також те, що особа, яка надає паспортні документи під час здійснення паспортного контролю, разом з

тим засвідчує добровільну згоду на обробку персональних даних, що враховує інтенсивний пасажиропотік та унеможливлює отримання письмової згоди **(додаток Т)**.

Уточнення потребує наказ Адміністрації ДПСУ від 25 травня 2007 р. № 472, яким затверджено Положення про базу даних «Відомості про осіб, які перетнули державний кордон України». Досить сумнівним, на нашу думку, є положення п. 19 Бази даних осіб, у якому зазначено, що інформація, яка зберігається в Базі даних осіб, є сукупністю відкритої адміністративної інформації та інформації про осіб і є власністю ДПСУ та не належить до інформації з обмеженим доступом [92, п. 19].

По-перше, категорія «адміністративна інформація» у чинному Законі України «Про інформацію» як вид інформації відсутня, існувала у редакції цього Закону до 13.01.2011 р. Положення про базу даних «Відомості про осіб, які перетнули державний кордон України» затверджено у 2007 році та не зазнало відповідних змін у зв'язку із внесенням змін до Закону України «Про інформацію».

По-друге, чи може бути інформація у Базі даних осіб відкритою? Адже у ній містяться персональні дані осіб, які підлягають захисту відповідно до Закону України «Про захист персональних даних» і які є конфіденційною інформацією, що належить до інформації з обмеженим доступом.

Тому вважаємо, що в п. 19 Бази даних осіб необхідно внести відповідні зміни і речення «*Інформація, що зберігається в Базі даних осіб, є сукупністю відкритої адміністративної інформації та інформації про осіб і є власністю Державної прикордонної служби України та не належить до інформації з обмеженим доступом*» викласти у такій редакції «*Інформація, що зберігається у Базі даних осіб, є сукупністю персональних даних осіб, що перетинають державний кордон України, і є власністю Державної прикордонної служби України*» **(додаток Т)**.

Пропонується внести зміни до статті 3 Закону України «Про Державну прикордонну службу України» у вигляді окремої частини і принципу діяльності

ДПСУ «*транспарентність*» відповідно до вимог розвитку інформаційного суспільства та положення Закону України «Про доступ до публічної інформації» (ст. 4) **(додаток Т).**

Крім цього, така позиція підкріплена проаналізованими нормами законодавства, якими закріплена інформаційна відкритість у функціонуванні інших правоохоронних органів.

Стаття 3 Закону України «Про Національну гвардію України» 13 березня 2014 року серед інших закріплює такі принципи діяльності «відкритості для демократичного цивільного контролю, прозорості» [508].

У Законі України «Про Національну поліцію», який був прийнятий 2 липня 2015 р., окрема стаття 9 присвячена принципу «відкритості та прозорості» [509, ст. 9]: *«Поліція здійснює свою діяльність на засадах відкритості та прозорості в межах, визначених Конституцію та законами України.*

Поліція забезпечує постійне інформування органів державної влади та органів місцевого самоврядування, а також громадськості про свою діяльність у сфері охорони та захисту прав і свобод людини, протидії злочинності, забезпечення публічної безпеки і порядку.

Поліція забезпечує доступ до публічної інформації, володільцем якої вона є, у порядку та відповідно до вимог, визначених законом.

Поліція може оприлюднювати (поширювати) інформацію з обмеженим доступом лише у випадках та в порядку, визначених законом.

Нормативно-правові акти, що регламентують діяльність поліції, обов'язково оприлюднюються на веб-порталі центрального органу управління поліції. Нормативно-правові акти з обмеженим доступом оприлюднюються у випадках та в порядку, визначених законом.

Проекти нормативно-правових актів, що стосуються прав та свобод людини, обов'язково проходять громадське обговорення в порядку, визначеному Міністром внутрішніх справ України» [509, ст. 9].

Ця стаття загалом розкриває зміст інформаційної відкритості Національної поліції. Закони, що прийняті останні роки, з питань закріплення відкритості

відображають розвиток інформаційного суспільства та більш точно передають інформаційні потреби всіх суб'єктів інформаційних відносин.

У п. 9 ст. 4 Закону України «Про державну службу» серед принципів державної служби закріплено принцип прозорості як «відкритість інформації про діяльність державного службовця, крім випадків, визначених Конституцією та законами України» [510].

Засади інформаційної відкритості закріплені у Законі України «Про прокуратуру» в ст. 6 «*Інформування про діяльність прокуратури*», частина норм якої отримала зміни у 2016 та 2019 роках. Положення даної статті визначають обов'язок посадових осіб прокуратури з відповідною періодичність (двічі на рік, один раз на рік) та порядок (надання узагальнених статистичних та аналітичних даних; оприлюднюється в загальнодержавних і місцевих друкованих засобах масової інформації і на офіційних веб-сайтах органів прокуратури) інформувати суспільство про свою діяльність [105, ст. 6]. Тому, крім закріплення принципу «транспарентності», виникає потреба закріплення порядку інформування громадськості про діяльність ДПСУ, яка на практиці і так набула широкого розповсюдження, з тенденцією розширення джерел інформування від друкованих у ЗМІ до цифрових сучасних трансформацій (діджиталізації).

Окремі моменти інформування ДПСУ зазначені у Законі України «Про Державну прикордонну службу України» та стосуються лише окремих органів влади й підстав: «*Голова Державної прикордонної служби України систематично інформує Верховну Раду України про виконання Державною прикордонною службою України покладених на неї завдань, додержання законодавства, забезпечення прав і свобод людини та з інших питань.*

Голова Державної прикордонної служби України щороку подає Верховній Раді України письмовий звіт про діяльність Державної прикордонної служби України» [79, ст. 29];

- «*інформування органів доходів і зборів про факт наміру перетинання державного кордону України особами, стосовно яких органами доходів і зборів було виявлено порушення митних правил*» [79, п. 8 ст. 19];

- «*інформування відповідних державних органів та громадян про аварії, пожежі, катастрофи, стихійне лихо та інші надзвичайні події на державному кордоні України, у прикордонній смузі та в контрольованих прикордонних районах*» [79, п. 23 ст. 19].

Але сьогодні коло питань, з яких ДПСУ забезпечує інформування, виходять за межі цих пунктів. Так, згідно з п. 5 Р. 1 (індекс «І») «Порядку дій уповноважених службових осіб Державної прикордонної служби України в разі виявлення в пунктах пропуску через державний кордон України та контрольних пунктах в'їзду на тимчасово окуповану територію України та виїзду з неї осіб, стосовно яких надано доручення, та порядок взаємодії органів охорони державного кордону з уповноваженими державними органами, які надали доручення», затверджених наказом МВС України від 23 червня 2017 р. № 535, посадові особи ДПСУ (п. 4 Р. 2) інформують уповноважені державні орган, які надали доручення про виконання доручень (Р. 3) щодо установлення факту перетинання державного кордону особами або про факт їх в'їзду на тимчасово окуповану територію України чи виїзду з неї, стосовно яких уповноваженими державними органами проводяться оперативно-розшукові, контррозвідувальні або розвідувальні заходи [511].

Забезпечення права кожного на доступ до інформації, що знаходиться у володінні ДПСУ як розпорядника публічної інформації у сфері охорони державного кордону, урегульовано Законом України «Про доступ до публічної інформації» [97]. Отже, інформування не обмежено лише наданням інформації державним органам влади, але й громадськості.

Позитивним прикладом для нашого дослідження є стаття 11 Митного кодексу України, яка закріплює основні положення щодо «Додержання вимог щодо конфіденційності інформації»: про мету отримання, обробки та використання інформації, умови відповідальності посадових осіб митних органів за порушення інформаційного законодавства [254, ст. 11, 22].

З урахуванням зазначеного, пропонуємо у Закон України «Про Державну прикордонну службу України» додати статтю 5-1 «*Інформування про діяльність Державної прикордонної служби України*».

«Голова Державної прикордонної служби України систематично інформує Верховну Раду України про виконання Державною прикордонною службою України покладених на неї завдань, додержання законодавства, забезпечення прав і свобод людини та з інших питань. Голова Державної прикордонної служби України щороку подає Верховній Раді України письмовий звіт про діяльність Державної прикордонної служби України.

Державна прикордонна служба України інформує:

органи доходів і зборів про факт наміру перетинання державного кордону України особами, стосовно яких органами доходів і зборів було виявлено порушення митних правил;

відповідні державні органи та громадян про події на державному кордоні України, у прикордонній смузі та в контрольованих прикордонних районах;

уповноважені державні органи, які надали доручення про факт перетинання державного кордону особами або про факт їх в'їзду на тимчасово окуповану територію України чи виїзду з неї, стосовно яких уповноваженими державними органами проводяться оперативно-розшукові, контррозвідувальні або розвідувальні заходи.

Державна прикордонна служба України повідомляє Департамент у сфері захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини про обробку персональних даних відповідно до умов та порядку, визначеного у статті 9. Закону України «Про захист персональних даних».

Державна прикордонна служба України здійснює систематичне та оперативне висвітлення офіційної інформації: в офіційних друкованих виданнях; на офіційних веб-сайтах у мережі Інтернет; на єдиному державному веб-порталі відкритих даних; на інформаційних стендах; будь-яким іншим способом.

Державна прикордонна служба України надає інформацію за запитами на інформацію» **(додаток Т)**.

Також пропонуємо у Закон України «Про Державну прикордонну службу України» додати статтю 5-3 «*Захист приватності у діяльності Державної прикордонної служби України*».

Державна прикордонна служба України обробляє персональні дані у межах виконання своїх повноважень в інтересах охорони державного кордону України.

Державна прикордонна служба України повідомляє суб'єкта персональних даних про дії з його персональними даними на умовах, визначених статтею 21 Закону України «Про захист персональних даних».

Військовослужбовці та працівники Державної прикордонної служби України, які мають доступ до персональних даних, дають письмове зобов'язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням службових обов'язків **(додаток Т)**.

У статті 33 Закону України «Про Державну прикордонну службу України» додати частину 4 щодо *відповідальності за порушення норм інформаційного законодавства*»:

«*Військовослужбовці та працівники Державної прикордонної служби України несуть відповідальність, передбачену законом за надання недостовірної інформації, а також за неправомірну відмову у наданні відповідної інформації, несвоєчасне надання інформації, порушення порядку збереження та розповсюдження персональних даних та інші правопорушення у сфері інформаційних відносин*» **(додаток Т)**.

Відповідно виключити ст. 29, п. 8 ст. 19 та п. 23 ст. 19 Закону України «Про Державну прикордонну службу України».

Невід'ємним елементом діяльності ДПСУ є інформаційна складова. Сьогодні інформація та діяльність пов'язана із нею, охоплює та пронизує усі ланки та напрямки оперативно-службової діяльності органів та підрозділів охорони державного кордону України. Повсякдення діяльність Державної прикордонної служби України пов'язана із реалізацією інформації,

інформаційними потребами та правами, інформаційними процесами (створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації) в інтересах прикордонної безпеки та реалізацією прав осіб у сфері державного кордону України.

Саме тому, розвиток і інтенсивне збільшення обсягів діяльності, пов'язаної з інформацією у сфері охорони державного кордону потребує закріплення у ч. 3 ст. 2 Закону України «Про Державну прикордонну службу України» окремої функції: *«Здійснення інформаційної функції»* **(додаток Т)**.

З урахуванням особливості сфери діяльності ДПСУ необхідно прийняти Концепцію інформаційного забезпечення ДПСУ з метою інтеграції та розвитку інформаційних відносин у сфері діяльності ДПСУ **(додаток У)**. Така Концепція може сприяти створенню передумов розвитку інформаційної сфери в діяльності ДПСУ, у поєднанні з вимогами сучасного інформаційного суспільства та розвитку системи інформаційної безпеки в охороні державних кордонів. Також сприятиме забезпеченню ефективної реалізації інформаційних відносин та інформаційної безпеки у сфері діяльності ДПСУ.

Крім цього, доцільно вести систематизований облік загальних для усієї ДПСУ відомчих нормативно-правових актів з питань урегулювання інформаційного простору ДПСУ (таку думку підтримують 98,1 % опитаних респондентів **(додаток В)**, що підвищить поінформованість персоналу про особливості забезпечення інформаційних відносин, інформаційної безпеки у сфері діяльності відомства.

Удосконалення термінології

Ще одним напрямком удосконалення інформаційних відносин є необхідність уточнення термінології та змісту окремих категорій у нормах інформаційного законодавства. Тільки точність і однозначність термінів і понять дозволять найбільш коректно сформулювати зміст того чи іншого правового інституту і забезпечити культуру правового регулювання у певній галузі правових відносин, тому що вироблення уніфікованих дефініцій у праві взагалі є однією із важливих завдань законодавчої нормотворчої практики [19, с. 385]. В Україні

вважають, що вирішення проблем нормативно-правового забезпечення інформаційних відносин можливе на основі ситуативного реагування. Певні проблеми правового врегулювання суспільних відносин у цій сфері вирішуються в окремих законах і підзаконних нормативних актах досить фрагментарно, низка юридичних норм, які прямо або опосередковано регулюють суспільні відносини у сфері інформаційно-комунікаційних відносин, концептуально не узгоджені між собою [512, с. 203]. У зв'язку з цим О. А. Баранов констатує, що робота з розвитку інформаційного права та вдосконалення інформаційного законодавства має значну перспективу з огляду на коло та важливість проблем, які мають місце в інформаційній сфері [513, с.15].

Відсутність сформованої термінології в інформаційному законодавстві може стати причиною відмови органами публічної адміністрації у задоволенні інформаційних прав громадян, плутанини у правозастосовній діяльності, а також суб'єктивізму при вирішення питань, що виникають в інформаційній сфері.

Досить часто у власних інтересах або в інтересах третіх осіб посадові особи відмовляють у наданні публічної інформації громадянам, безпідставно підміняючи категорії, які не знайшли чіткого закріплення у чинних нормах інформаційного законодавства, зокрема прикриваючись такими, як «службова інформація» або «відсутність суспільного інтересу». Прикладом цього є рішення у справі 335/13988/17 Орджонікідзевського районного суду, позивача до Запорізької міської ради щодо ненадання позивачу як запитувачу публічної інформації копій договорів з переможцями конкурсу на управителів будинків. Позивачу, який звернувся до Запорізької міської ради у наданні публічної інформації, було відмовлено на підставі того, що ця послуга потребує відшкодування фактичних витрат, а позивач їх не сплатив. Разом з тим запитувана інформація становила суспільний інтерес, а при наданні особі інформації про себе та інформації, що становить суспільний інтерес, плата за копіювання та друк не стягується. Тому суд задовольнив вимоги позивача [514].

Інтенсивний процес створення сучасного інформаційного законодавства зумовив появу нових правових категорій і термінів. Але непоодинокі випадки

появи одних і тих самих термінів у різних нормативно-правових актах, що мають різне або неоднозначне трактування [513, с. 29].

У зв'язку з тим, що різні закони та підзаконні акти, які регулюють суспільні відносини, об'єктом яких є інформація, приймались у різні часи без узгодження понятійного апарату, вони мають низку термінів, які недостатньо коректні, не викликають відповідну інформаційну рефлексію або взагалі не мають чіткого визначення змісту. Термінологічні неточності, різне тлумачення однакових за назвою та формою понять і категорій призводить до їх неоднозначного розуміння і застосування на практиці. Наприклад, щодо інформаційних відносин зазначимо такі, як «таємна інформація», «таємниця», «документ», «документована інформація», «володіння», «інтелектуальна власність», «автоматизована система», «суб'єкт суспільних відносин», «учасники суспільних відносин», «система інформаційних відносин» тощо [11, с. 110].

Уточнення потребує поняття «інформація про фізичну особу», яка у ст. 11 Закону України «Про інформацію» ототожнюється із «персональними даними». Ураховуючи положення законодавства ЄС та відповідно до Регламенту (ЄС) 2016/679 від 04.05.2016 р. «General Data Protection Regulation», термін «персональні дані» означає *будь-яку інформацію*, що стосується ідентифікованої фізичної особи («суб'єкт даних»). Варто наголосити, що у Регламенті ЄС використовується однозначний термін «персональні дані», на відміну від згаданої ст. 11 Закону України «Про інформацію», що спричиняє плутанину у правозастосовній діяльності. Ці дві категорії потребують диференціації та уточнення змісту, а інформація про особу має ширше значення ніж персональні дані.

Крім зазначеного, існує низка проблемних термінологій і категорій, які потребують окремого наукового розроблення та не вичерпуються у межах даного дослідження.

Таких прикладів можна навести багато. Так, Законом України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо відповідальності за незаконне перетинання державного кордону

України» від 18 жовтня 2018 року було введено кримінальну відповідальність за незаконне перетинання державного кордону України [253, ст. 332-2]. Відповідальність за цією статтею може настати за перетинання державного кордону України з метою заподіяння шкоди інтересам держави або особою, якій заборонено в'їзд на територію України, або представниками підрозділів збройних сил чи інших силових відомств держави-агресора. Одним зі способів вчинення такого злочину є перетинання державного кордону в пунктах пропуску через державний кордон України без відповідних документів, або за документами, що містять недостовірні відомості [253, ч. 1 ст. 332-2].

Якщо відсутність відповідних документів є очевидним, то документи, що містять недостовірні відомості потребують наукового обміркування. Термін «недостовірні» у словниках української мови тлумачиться як такий, що викликає сумнів щодо правдивості, правильності [42 с. 758]. Тобто застосування поняття «недостовірні відомості» можуть мати місце у разі виникнення сумнівів під час прикордонного контролю, щодо їх правдивості.

Зі свого боку Закон України «Про прикордонний контроль» установлює, що паспортні та інші документи громадян України, іноземців та осіб без громадянства, які перетинають державний кордон, перевіряються уповноваженими службовими особами ДПСУ з метою встановлення їх дійсності та належності відповідній особі. При цьому з'ясовується наявність або відсутність підстав для тимчасової відмови особі у перетинанні державного кордону [154, ч. 1 ст. 7].

Під час прикордонного контролю перевіряється дійсність документів. Поняття «дійсний», «дійсність» уживається для: підтвердження висловлення; те, що насправді існує або існувало; реальний [43, с. 304]. Така реальність під час перевірки документів ґрунтується на конкретних діях прикордонників, які дозволяють встановити, чи спростувати правдивість інформації про особу, що перетинає державний кордон, а не на міркуваннях. Для цього у ході перевірки документів уповноважені службові особи ДПСУ використовують технічні засоби контролю для пошуку ознак підробки у документах, здійснюють пошук

необхідної інформації у базах даних ДПСУ, а також за результатами оцінки ризиків проводять опитування осіб, які прямують через державний кордон [154, ч. 1 ст. 7].

Крім цього, дозвіл на перетинання державного кордону іноземцю, особі без громадянства у разі в'їзду в Україну надається за відповідності таким умовам: наявності дійсного паспортного документа; відсутності щодо нього рішення уповноваженого державного органу України про заборону в'їзду в Україну; наявності в нього в'їзної візи, якщо інше не передбачено законодавством України; підтвердження мети запланованого перебування; наявності достатнього фінансового забезпечення [154, ч. 1 ст. 8].

Отже, законодавством про прикордонний контроль визначені та чітко встановлені підстави й інформація про особу, які необхідно установити та підтвердити конкретними способами і засобами. Тому посадові особи ДПСУ, що здійснюють перевірку документів, керуються перевіреними даними про осіб, що перетинають державний кордон України, а не підозрами. У зв'язку із цим, доречно замість словосполучення «що містять недостовірні відомості» у контексті ч. 1 ст. 332-2 КК України, уживати «що містять відомості, які не відповідають дійсності» [515, с. 244].

Чіткого розмежування потребує службова інформація та інформації, яка становить державну таємницю [516, с. 71], що є важливим у реалізації оперативно-службової діяльності ДПСУ, зокрема під час здійснення оперативно-розшукової діяльності в інтересах забезпечення захисту державного кордону України [517, с. 100].

Зазначені аспекти обумовлюють теоретичну необхідність та практичну доцільність на сучасному етапі розвитку інформаційного суспільства, своєчасного (відповідно умовам часу та реальним потребам), обґрунтованого науковою доктриною інформаційного права закріплення актуальних категорій і термінів інформаційного законодавства [518, с. 130]. Удосконалення термінології повинно відбуватись комплексно і систематично, синхронно із систематизацією

інформаційного законодавства, із залученням фахівців практичної, теоретичної, аналітичної сфери.

Безпека державного кордону України складна та динамічна сфера державної діяльності. Систему прикордонної безпеки формують різні завдання та напрямки у функціонуванні ДПСУ, які безпосередньо залежать від прикордонного відомства та загальнодержавної тенденції розвитку. Однією з інтегрованих, залежних від державного регулювання та відомчого забезпечення, є інформаційна складова діяльності ДПСУ, яка знаходить вияв в інформаційних відносинах.

Найбільш урегульованою відповідно до чинного законодавства та специфіки внутрішньої діяльності є технічне та організаційне інформаційне забезпечення ДПСУ. Але інформаційні відносини передбачають ще й комунікацію із громадськістю щодо реалізації їх інформаційних прав у прикордонній сфері. Так, значна кількість виявів інформаційних відносин у діяльності прикордонного відомства є достатньо урегульованою та переважно задовольняє інформаційні потреби всіх суб'єктів цих відносин, але є й такі сторони, що потребують удосконалення.

Основний важіль проблемності обумовлений відсутністю загально державної стратегії розвитку інформаційного суспільства (лише є за окремими напрямками: інформаційна безпека, кібербезпека тощо) та систематизованості інформаційного законодавства. З урахуванням цього та специфіки завдань, що виконує ДПСУ визначені напрямки, які сприятимуть удосконаленню нормативно-правовому регулюванню інформаційних відносин у діяльності ДПСУ, а саме, систематизація інформаційного законодавства (прийняття Інформаційного кодексу України, згрупувати склади злочинів (у КК України) та адміністративних проступків (у КУпАП), які передбачають відповідальність за порушення норм інформаційного законодавства); удосконалення термінології інформаційного законодавства; удосконалення нормативно-правового регулювання інформаційних відносин у нормах прикордонного законодавства (прийняття Концепцію інформаційного забезпечення ДПСУ, створення відомчої нормативно-

правової бази, доступної до персоналу ДПСУ, внесення змін у норми окремих нормативно-правових актів).

Висновки до розділу 5

Аналіз теорії та практика інформаційних відносин у діяльності ДПСУ дозволив констатувати про існування низки питань, які потребують підвищення ефективності. Тому нами розроблені напрямки (розвиток відкритості та доступності у діяльності ДПСУ, розвиток електронного урядування та електронної ідентифікації, розвиток та безпека інформаційних систем у діяльності ДПСУ, формування знань та свідомості персоналу ДПСУ про основні засади та принципи інформаційного законодавства (інформаційна культура) та конкретні заходи, які будуть сприяти удосконаленню інформаційних відносин.

Важливим питанням є виправдання та підтримання отриманого високого рівня довіри громадян до ДПСУ усіма військовослужбовцями та працівниками. Адже загальновідомо, що довіру важко отримати, але легко втратити. Тому будь-які дії з боку представників ДПСУ можуть вплинути (позитивно чи негативно, залежно від характеру дій) на досягнутий рівень довіри, що необхідно враховувати у повсякденній діяльності, у спілкуванні з громадськістю, із ЗМІ, взаємодіючими суб'єктами. За будь-яких умов залишатись зваженими, спокійними, об'єктивними, розсудливими та показувати свій професіоналізм.

Підвищення ефективності на веб-сайті ДПСУ повинно відбуватися завдяки: висвітленню розширеного звіту по роботі зі зверненнями громадян, запитами на публічну інформацію, а також узагальненню даних з обробки персональних даних; видаванню кожного року Стратегічного бюлетеня прикордонної безпеки «Біла книга»; наданню інформації про відповідальну особу, яка організовує роботу, пов'язану із захистом персональних даних під час їх обробки у ДПСУ, а у перспективі розвиток структурних підрозділів по роботі у цьому напрямку;

закріпленню у частині 1 статті 3 Закону України «Про Державну прикордонну службу України» окремого принципу діяльності ДПСУ «*транспарентність*»).

У межах розвитку та безпеки інформаційних систем у діяльності ДПСУ необхідно постійно та безперервно вживати заходів із забезпечення та розвитку системи збереження та захисту інформації; створення сучасної інфраструктури електронної ідентифікації та забезпечення її розвитку. Удосконалювати надання цифрових послуг у межах онлайн-сервісу «Дія» для осіб, що планують виїхати за кордон.

Формування знань та свідомості персоналу ДПСУ про основні засади та принципи інформаційного законодавства (інформаційна культура) можливий через формування та удосконалення знань, умінь персоналу у роботі з інформацією, підвищення інформаційної культури, формування інформаційної концепції у поведінці персоналу.

Потребують удосконалення й нормативно-правові акти, що врегульовують інформаційні відносини, зокрема здійснення систематизації норм інформаційного законодавства шляхом кодифікації, прийняття Інформаційного кодексу України, згрупування статей КК України та КУпАП, які передбачають відповідальність за порушення норм інформаційного законодавства. Удосконалення також потребує термінологія інформаційного законодавства; нормативно-правове регулювання інформаційних відносин у нормах прикордонного законодавства (прийняття Інформаційної концепції ДПСУ, створення відомчої нормативно-правової бази доступної до персоналу ДПСУ, внесення змін у норми окремих нормативно-правових актів).

ВИСНОВКИ

У дисертації надано теоретичне узагальнення та нове розв’язання наукової проблеми, що полягає у з’ясуванні особливостей нормативно-правового регулювання інформаційних відносин у діяльності ДПСУ, формулюванні обґрунтованих рекомендацій щодо підвищення ефективності інформаційних відносин і напрямків удосконалення їх нормативно-правового регулювання. За результатами проведеного дослідження сформульовано такі узагальнені науково-теоретичні і практичні висновки.

Стан наукової розробленості інформаційних відносин у сучасній правовій доктрині характеризується збільшенням наукового інтересу через зростання кількості та якості теоретико-правових праць, присвячених загальним чи окремим аспектам інформаційних відносин, які підкреслюють вагомість і актуальність дослідження інформаційних відносин у діяльності ДПСУ. Відсутність системної роботи юридичного спрямування зумовила потребу ґрунтовного та системного дослідження проблематики, поставленої в дисертації.

Результатом аналізу рівня наукової розробленості досліджуваної тематики стала концептуальна побудова структури та змістовної складової дисертації за зовнішнім і внутрішнім спрямуванням. Зовнішній напрямок передбачає реалізацію інформаційних прав осіб, що перетинають державний кордон України, задоволення інформаційних потреб, захист приватності у зв’язку із функціонуванням органів і підрозділів ДПСУ. Внутрішній напрямок генерує забезпечення інформаційної діяльності у ДПСУ, усебічний розвиток інформаційної складової в управлінні оперативно-службовою діяльністю ДПСУ, забезпечення інформаційної відкритості та збільшення довіри громадян до ДПСУ, створення умов для протидії та недопущення інформаційних загроз прикордонній безпеці, досягнення розуміння кожним військовослужбовцем і працівником ДПСУ цінності інформації в охороні державного кордону України, особливо в умовах реальної зовнішньої агресії.

Методологічна основа дослідження розглядається через систему взаємопов’язаних методів онтологічного, гносеологічного, аксіологічного та праксеологічного сприйняття дійсності. Методологія інформаційних відносин у діяльності ДПСУ є доволі складним і несформованим донині в межах науки інформаційного права явищем, яке можна пізнати через систему методів, на підставі яких здійснюється розкриття теоретико-правових засад інформаційних відносин у функціонуванні ДПСУ. Методологічний інструментарій створює умови для пізнання та відображення об’єктивної дійсності цих відносин, дозволяє розкрити їх нове бачення, а також є теоретичним підґрунтям для вирішення практичних завдань у діяльності ДПСУ.

Методологічне підґрунтя пізнання інформаційних відносин у діяльності ДПСУ має вагоме значення: для створення теоретичної основи при формуванні нових, змістовно якісних знань відповідно до сучасних умов розвитку інформаційних відносин у прикордонній сфері; для формування логічних засад процесу опрацювання великого обсягу інформації теоретичного та практичного значення, пов’язаної з інформаційною діяльністю ДПСУ; для формулювання чітких теоретичних і практичних цілей дослідження; для обрання оптимального методологічного інструментарію дослідження, що залежить від світогляду науковця, специфіки прикордонної сфери та очікуваного результату дослідження і впливає на кінцевий результат; при створенні фундаменту для вироблення та уніфікації понятійного апарату інформаційних відносин; для забезпечення отримання всебічних відомостей про інформаційні відносини у сфері діяльності ДПСУ; для формування та зміцнення теоретико-методологічної майстерності конкретного науковця.

Обґрунтовано правову природу інформаційних відносин у діяльності ДПСУ. Надано авторське бачення поняття «інформаційні відносини у діяльності ДПСУ» та сформульовано особливості, які розкривають правову природу досліджуваних відносин. Інформаційні відносини у діяльності ДПСУ – це різновид суспільних відносин у сфері охорони державного кордону, які урегульовані нормами законодавства (інформаційного, адміністративного та

інших галузей, а також нормами законодавства у прикордонній сфері) та обумовлені реалізацією прав, потреб і процесів щодо інформації, яка пов’язана з діяльністю або створюється в процесі виконання завдань Державної прикордонної служби України.

Зміст інформаційних відносин визначають специфічні, особливі для діяльності ДПСУ (у забезпеченні охорони державного кордону України) елементи, такі як суб’єкт інформаційних відносин, зміст (інформаційно-правовий статус суб’єкта), об’єкт інформаційних правовідносин.

Суб’єкт відносин у цій сфері може бути загальним (фізичні та юридичні особи, громадські організації тощо, які мають інтерес чи право, пов’язане з інформацією у сфері діяльності ДПСУ), особливим або центральним (усі структурні підрозділи та посадові особи ДПСУ). У межах ДПСУ функціонують спеціальні суб’єкти, правовий статус яких обумовлюється призначенням – безпосереднє здійснення інформаційної діяльності за окремими напрямками: оприлюднення публічної інформації; надання консультування та прийняття заяв, звернень; забезпечення обігу оперативно-службової інформації; документування, робота з управлінськими, внутрішньоорганізаційними та індивідуальними документами; опрацювання електронної інформації; забезпечення захисту інформації.

Інформаційні права й обов’язки як системоутворюючі складові змісту (інформаційно-правового статусу ДПСУ) інформаційних відносин визначають межі інформаційної діяльності у вигляді правових можливостей і дотримання, виконання та здійснення необхідних дій відповідно до законодавства, а чітко врегульований механізм втілення в реальні інформаційно-правові відносини у сфері охорони державного кордону відповідних прав і обов’язків дозволяє ДПСУ вчиняти дії, пов’язані з інформацією, що мають правові наслідки. Обґрунтовано, що зміст інформаційно-правового статусу ДПСУ тісно пов’язаний з інформаційною правосуб’єктністю.

Інформаційно-правовий статус ДПСУ розкривають такі елементи: правові підстави участі у правовідносинах з приводу інформації; завдання інформаційної

діяльності; система спеціальних підрозділів, діяльність яких спрямована на забезпечення та реалізацію інформаційних потреб ДПСУ; інформаційна правосуб'єктність (права й обов'язки) посадових осіб ДПСУ щодо інформаційної діяльності.

Об'єктом інформаційних відносин у діяльності ДПСУ є відомості, пов'язані з функціонуванням органів (підрозділів) охорони державного кордону та порядком перетинання державного кордону. Запропоновано класифікацію інформації у сфері охорони державного кордону за такими критеріями: за характером, напрямком діяльності, порядком доступу, сутністю, результатами службової діяльності, очікуваним результатом, способом доведення, формою вираження, формою візуалізації, територіальним спрямуванням, державно-правовим і суспільним схваленням.

Визначено, що інформація всіх видів має самостійну цінність, створює основу для правових актів як на міжнародному та державному, так і на регіональному рівнях. Вона здатна до випереджального впливу на державну прикордонну безпеку, визначає вибір того чи іншого варіанта управлінського рішення посадовими особами ДПСУ, а також дій прикордонних органів і підрозділів.

Прикордонна інформаційна безпека ґрунтується на врахуванні актуальних загроз національній безпеці України, забезпеченні інформаційних прав і визначенні пріоритетів державної політики в інформаційній сфері, залежить від чіткого нормативного регулювання та злагодженої роботи всіх структурних елементів ДПСУ у напрямку її забезпечення. Визначено, що державна політика у сфері прикордонної інформаційної безпеки – це діяльність компетентних органів держави щодо формування правових засад і напрямків інформаційної безпеки та їх реалізація, що ґрунтується на урахуванні загроз територіальній цілісності держави та прикордонній безпеці в інформаційній сфері, спрямована на забезпечення інформаційних потреб сучасного суспільства з оволодіння даними про особливості перетинання державного кордону України, про стан охорони державного кордону та про діяльність прикордонного відомства тощо.

З’ясовано, що інформаційна безпека є складним систематизованим поняттям, забезпечення якої є підґрунтям (окрім власне інформаційної) національної та прикордонної безпеки. Захист інформації передбачає здійснення конкретних заходів, спрямованих на забезпечення збереження вмісту даних, що містяться на матеріальних носіях, забезпечення права на інформацію та дотримання режимних правил доступу до інформації, розпорядником якої є ДПСУ. Доведено, що інформаційна безпека є напрямком діяльності ДПСУ, захист інформації є її складовою, а їх співвідношення відображається як частина цілого.

Інформаційна складова діяльності ДПСУ урегульована системою нормативно-правових актів різного рівня ієрархії, а саме: Конституцією України; загальними або базовими нормативно-правовими актами; спеціальними нормативно-правовими актами; програмними документами. Установлено, що ці нормативно-правові акти визначають основні засади, принципи, механізми забезпечення обігу інформації, зокрема і з використанням інформаційно-телекомунікаційних систем у сфері охорони державного кордону, що здійснюється в процесі виконання завдань ДПСУ.

Правовий режим інформації з обмеженим доступом у діяльності ДПСУ – це установлені законодавством процедури та порядок надання дозволу, доступу, охорони, захисту, а також здійснення діяльності з інформацією, яка становить велику цінність для прикордонної безпеки держави. Доведено, що правовий режим інформації з обмеженим доступом є одним із визначальних чинників прикордонної безпеки, тобто важливим засобом захисту та збереження цілісності інформації, розпорядником якої є ДПСУ.

Основними елементами правового режиму інформації з обмеженим доступом у діяльності ДПСУ є: порядок і підстави здійснення інформаційної діяльності з відповідним видом інформації, що обмежена в доступі (створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації, а також порядок віднесення та скасування інформації, обмеженої у доступі); права посадових осіб ДПСУ щодо здійснення окремих процедур із

такою інформацією; процедура отримання допуску до цієї інформації; відповідальність за порушення встановленого режиму інформації.

Організаційні засади інформаційних відносин в управлінні оперативно-службовою діяльністю ДПСУ сконцентровано на процесі прийняття рішень начальниками органів і підрозділів охорони державного кордону. В процесі прийняття управлінського рішення у сфері охорони державного кордону інформація здійснює кругообіг, змінюється лише її зміст, кількість і якість. Достовірна та актуальна інформація є основою правильного та своєчасного рішення у сфері охорони державного кордону України і впливає на прикордонну безпеку держави.

Багатокомпонентний зміст інформаційних відносин в управлінні оперативно-службовою діяльністю ДПСУ передбачає: інформаційну діяльність, інформаційно-аналітичну діяльність, завдання, інформаційні потреби людини й держави у прикордонній сфері, актуальні бази даних, зовнішні та внутрішні інформаційні фактори начальника прикордонного підрозділу тощо. Розвиток інформаційних відносин обумовлює застосування в управлінській діяльності нових інформаційних технологій та інформаційно-аналітичного забезпечення як одних із найважливіших засобів удосконалення управління у сфері охорони державних кордонів. Такі заходи дають змогу втілювати положення Стратегії розвитку ДПСУ в частині здійснення модернізації системи управління шляхом упровадження сучасних інформаційних технологій у систему управління.

На підставі здійсненого узагальнення досвіду інформаційної взаємодії в діяльності ДПСУ зроблено висновок, що інформаційна взаємодія закладає основи для спільної діяльності та покращання ефективності в охороні державного кордону України, має цілеспрямований характер, орієнтована на обмін інформацією щодо своєчасного виявлення, попередження та недопущення порушення прикордонного законодавства, забезпечення недоторканності державного кордону. Напрямками інформаційної взаємодії в діяльності ДПСУ є: функціонування віртуального контактного аналітичного центру; розширення мереж і функцій контактних пунктів; удосконалення механізму обміну

інформацією; проведення спільних аналітичних досліджень з оцінки загроз і ризиків у сфері безпеки державного кордону й ефективності інтегрованого управління кордонами, надання взаємного доступу до інформаційних систем компетентними державними органами тощо.

У предметному контексті проведеного дослідження запропоновано під «інформаційною сферою суспільства» розглядати урегульовані національним законодавством інформаційні відносини, інформаційні повноваження, сукупність інформаційних ресурсів ДПСУ, які дають змогу реалізувати інформаційні права, інтереси та потреби громадян, суспільства, органів і підрозділів ДПСУ у сфері охорони державного кордону.

Показником комунікації ДПСУ з інформаційною сферою суспільства слугує реалізація принципу відкритості перед громадянами, що є пріоритетом державної політики в інформаційній сфері, закріпленої Доктриною інформаційної безпеки України, та становить вимогу керівництва ДПСУ. Практичну дієвість інформаційна відкритість у діяльності ДПСУ набуває через такі складові елементи: нормативно врегульований механізм забезпечення отримання інформації про діяльність прикордонного відомства та його структурні підрозділи; стан забезпечення реалізації прав громадян на інформацію у прикордонній сфері; оприлюднення інформації у прикордонній сфері через доступні процедури; простота й доступність електронного урядування у ДПСУ; визначення змісту інформації, яка підлягає оприлюдненню, а отже її чітке розмежування на інформацію, що може бути доведена до всіх (публічна відкрита), стосується окремої особи (конфіденційна) чи групи осіб або безпеки держави (службова чи таємна), тобто які результати діяльності та дії посадових осіб ДПСУ підлягають оприлюдненню; рівень інформаційної культури персоналу ДПСУ.

Найбільш широке коло питань, пов’язаних із забезпеченням приватності в діяльності ДПСУ, стосується здійснення прикордонних процедур і встановлення особи запитувача інформації. Зокрема інформаційна приватність стосується ідентифікації осіб, що вступають у відносини з органами та підрозділами ДПСУ під час проходження прикордонного контролю у пунктах пропуску через

державний кордон України, доступу до інформації та забезпечення захисту такої інформації. Актуальною є ідентифікація за допомогою персональних даних, яка по суті є засобом установлення відповідності, ототожнення, розпізнання ідентичних ознак, належності даних між різними об'єктами, відомого з невідомим, у тому числі особи самій собі (наприклад, пред'явника паспортного або іншого документа із зображенням особи в ньому).

Важливе значення у захисті приватності відіграє надання згоди на опрацювання персональних даних від суб'єкта персональних даних. З'ясовано, що щоденний пасажиропотік не дає можливості під час здійснення прикордонних процедур запитувати письмову згоду на опрацювання персональних даних. Разом з тим аналіз норм прикордонного законодавства дозволив констатувати відсутність сформульованої мети та форми отримання згоди на опрацювання персональних даних осіб, які перетинають державний кордон України.

Відносини ДПСУ з інформаційною сферою суспільства набувають реальних форм через інститути звернення та запиту на публічну інформацію, які належать до одного з основних напрямків діяльності – формування ефективного механізму комунікації з громадськістю для реалізації державної політики у сфері охорони державного кордону. Розширення безвізових можливостей перетинання державного кордону для громадян України, установлення адміністративної межі на тимчасово окупованій території та інші обставини зумовлюють постійне збільшення у суспільства потреб в інформації, пов'язаній з діяльністю ДПСУ. Якість такої діяльності переважно відповідає запитам інформаційного суспільства, водночас потребують удосконалення питання сучасної електронної ідентифікації запитувачів інформації за електронним кваліфікаційним підписом.

Визначено поняття «інформаційні загрози у діяльності ДПСУ» та здійснено їх аналіз. Інформаційні загрози в діяльності ДПСУ – це фактори, які утворюють небезпеку чи заподіюють шкоду інформаційним відносинам, інформаційним правам та інформаційним ресурсам ДПСУ, посягають на прикордонну безпеку. Означено, що інформаційні загрози в сучасному суспільстві можуть іноді завдати більшої шкоди, ніж будь-які протиправні фізичні дії.

Аналіз сучасних інформаційних загроз дозволив диференціювати їх за такими критеріями:

– за локалізацією: зовнішні (інформаційна війна РФ проти України); внутрішньодержавні (надання представникам ДПСУ неправдивої, недостовірної інформації); внутрішньовідомчі (витікання інформації через персонал ДПСУ або суб'єктів інтегрованого управління кордонами);

– 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;

– за характером вияву: відомчі (посягають на прикордонну безпеку держави), корпоративні (стосуються безпеки окремого підрозділу), особисті (щодо окремих військовослужбовців чи посадових осіб ДПСУ);

– за способом впливу: інтелектуальні (дезінформація); програмні (хакерські атаки); організаційні (порушення режиму інформації); організаційно-технічні (використання ПК для роботи з обмеженою інформацією, що заборонено);

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

Будь-які сучасні інформаційні технології опрацювання та захисту інформації не виключають шкідливого чинника на інформацію та інформаційні відносини. Гарантією їх захисту є правові засоби охорони (юридична відповідальність), які сьогодні потребують комплексного підходу до вдосконалення норм, що визначають підстави, порядок і міри застосування негативних правових засобів до порушників, незалежно від їх правого становища. Для цього першочергово мають бути згруповані у межах окремих підрозділів

КК України, КУпАП, ЦК України. За вчинення правопорушень, зазначених у КУпАП, де передбачена відповідальність за адміністративні інформаційні правопорушення, військовослужбовці повинні нести адміністративну, а не дисциплінарну відповідальність, що сприятиме розмежуванню останніх (за порушення законів, постанов, розпоряджень – адміністративна, за порушення внутрішньовідомчих організаційних нормативно-правових актів – дисциплінарна).

Розвиток інформаційних відносин у діяльності ДПСУ супроводжується популяризованим використанням і застосуванням глобальних, локальних і відомчих мереж. Розповсюдження в них інформації службового або приватного характеру може як прискорити інформаційні процеси (своєчасне оприлюднення особливостей і умов перетинання державного кордону на окремих ділянках), так і спричинити негативні наслідки для прикордонної безпеки та безпеки військовослужбовців ДПСУ. Аргументовано, що безпечне використання інтернету, інформаційно-телекомунікаційних систем має бути пріоритетом для кожного військовослужбовця та працівника ДПСУ, ґрунтуватись на чіткому виконанні службових обов’язків, дотриманні норм законодавства (режиму інформації з обмеженим доступом), усвідомленні значення збереження інформації (правової культури, інформаційної культури) та рекомендацій щодо обмеження розповсюдження приватної інформації (про себе) та користування електронними пристроями (ґаджетами тощо).

Одночасно з веденням, опрацюванням, переданням даних в інформаційних системах, забезпеченням їх функціонування необхідно постійно вживати заходів з убезпечення змісту інформації. Такі заходи повинні мати комплексний характер (правові, організаційні, технічні, здійснення контролю, притягнення винних до відповідальності тощо) та реалізовуватись усіма посадовими особами ДПСУ, які мають доступ до функціонування інформаційних систем. Налагоджена робота спеціальних структурних підрозділів, призначених для захисту інформації у межах діяльності Головного центру зв’язку, автоматизації та захисту інформації Адміністрації ДПСУ, залучення кращих фахівців у сфері захисту інформації до їх

складу, а також надання можливості їх професійного зростання підвищить ефективність протистояння інформаційним загрозам у досліджуваній сфері.

Аналіз теорії та практики інформаційних відносин у діяльності ДПСУ став підставою для розроблення рекомендацій (розвиток відкритості та доступності у діяльності ДПСУ, розвиток і безпека інформаційних систем у діяльності ДПСУ, розвиток електронного урядування та електронної ідентифікації, формування знань і свідомості персоналу ДПСУ про основні засади та принципи інформаційного законодавства (інформаційна культура) та конкретних заходів, які будуть сприяти удосконаленню інформаційних відносин. Підвищення ефективності вебсайту ДПСУ повинно відбуватися через висвітлення розширеного звіту щодо роботи за зверненнями громадян і запитами на публічну інформацію, а також через узагальнення даних (запровадження реєстру) з опрацювання персональних даних; через публікацію кожного року Стратегічного бюлетеня прикордонної безпеки «Біла книга», надання інформації про відповідальну особу, яка організовує роботу, пов’язану із захистом персональних даних при їх обробці у ДПСУ, розвиток і розширення структурних підрозділів, які працюють у цьому напрямку.

У межах розвитку та безпеки інформаційних систем у діяльності ДПСУ необхідно постійно та безперервно вживати заходів із забезпечення та розвитку системи збереження та захисту інформації, створення сучасної інфраструктури електронної ідентифікації та забезпечення її розвитку. Удосконалювати надання цифрових послуг у межах онлайн-сервісу «Дія» для осіб, що планують виїхати за кордон.

Важливим є формування освіченості та свідомості у персоналу ДПСУ щодо основних засад і принципів інформаційного законодавства (інформаційна культура) через формування та удосконалення знань, умінь персоналу в роботі з інформацією, підвищення інформаційної культури, формування інформаційної концепції в поведінці.

Пропонуються напрямки удосконалення нормативно-правового регулювання інформаційних відносин у діяльності ДПСУ, серед яких:

необхідність здійснення систематизації норм інформаційного законодавства шляхом кодифікації, ухвалення Інформаційного кодексу України, згрупування статей КК України та КУпАП, які передбачають відповідальність за порушення норм інформаційного законодавства; удосконалення термінології інформаційного законодавства; покращання нормативно-правового регулювання інформаційних відносин у нормах прикордонного законодавства (прийняття Концепції інформаційного забезпечення ДПСУ, створення відомчої нормативно-правої бази, доступної до персоналу ДПСУ, внесення змін у норми окремих нормативно-правових актів).

Запропоновано внести низку змін і доповнень до законів України «Про Державну прикордонну службу України» та «Про прикордонний контроль», до наказу Адміністрації Державної прикордонної служби України від 25.06.2007 № 472 «Відомості про осіб, які перетнули державний кордон України».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Арістова І. В. Наука «інформаційне право» на новому етапі розвитку інформаційного суспільства. *Правова інформатика*. 2011. № 1(29). С. 3–11.

2. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади : автореф. дис... д-ра юрид. наук : 12.00.07. Харків, 2002. 39 с.

3. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади : дис. … д-ра юрид. наук: 12.00.07. Харків, 2002. 476 с.

4. Бєляков К. І. Організаційно-правове та наукове забезпечення інформатизації в Україні: проблеми теорії та практики : автореф. дис... д-ра юрид. наук : 12.00.07. Київ, 2002. 39 с.

5. Сопілко І. М. Правові засади державної інформаційної політики України : автореф. дис. ... д-ра юрид. наук : 12.00.07. Київ, 2014. 38 с.

6. Ліпкан В. А., Сопілко І. М., Кір'ян В. О. Правові засади розвитку інформаційного суспільства в Україні : монографія / за заг. ред. В. А. Ліпкана. Київ. : ФОП О. С. Ліпкан, 2015. 664 с.

7. Негодченко В. О. Адміністративно-правове забезпечення державної інформаційної політики органами Національної поліції України : автореф… д-ра юрид. наук : 12.00.07. Харків. 2017. 40 с.

8. Почепцов Г. Г., Чукут С. А. Інформаційна політика : навч. посіб. 2-ге вид., Київ : Знання, 2008. 663 с.

9. Інформаційна політика. URL: https://pidruchniki.com/18211001/politologiya/informatsiyna_politika_problemni_pitannya#19 (дата звернення: 20.07.2019).

10. Розвиток системи аналізу ризиків в Держприкордонслужбі. URL: https://dpsu.gov.ua/ua/rozvitok-sistemi-analizu-rizikiv-derzhprikordonsluzhbi-/ (дата звернення: 07.05.2019).

11. Основи інформаційного права України : навчальний посібник / В. С. Цимбалюк та ін. ; за ред. М. Я. Швеця, Р. А. Калюжного, П. В. Мельника. Київ : Знання, 2004. 274 с.

12. Марущак А. І. Інформаційне право: Доступ до інформації : навчальний посібник. Київ : КНТ, 2007. 532 с.

13. Теорія держави і права : навчальний посібник / О. О. Тихомиров та ін. ; за заг. ред. Л. М. Стрельбицької. Київ : Кондор, 2016. 332 с.

14. Селезньова О. М. Теоретико-методологічні основи інформаційного права України : монографія. Чернівці : Місто, 2014. 408 с.

15. Селезньова О. М. Теоретико-методологічні засади інформаційного права України як інтегрованої категорії : дис. д-р. юрид. наук : 12.00.07. Київ, 2015. 420 с.

16. Маріц Д. О. Інформаційні правовідносини в України: теоретичні та практичні аспекти : монографія. Вінниця: Тов «ТОВТРИ», 2018. 472 с.

17. Маріц Д. О. Теоретичні проблеми правового регулювання інформаційних відносин в України : дис. … д-ра юрид. наук : 12.00.07. Київ, 2019. 462 с.

18. Маріц Д. О. Теоретичні проблеми правового регулювання інформаційних відносин в України : автореф. дис... д-ра юрид. наук : 12.00.07. Київ, 2019. 38 с.

19. Литвин Н. А. Адміністративно-правове забезпечення інформаційної діяльності органів Державної фіскальної служби України : дис… д-ра юрид. наук : 12.00.07. Ірпінь, 2018. 517 с.

20. Сопілко І. М. Інформаційні правовідносини за участю органів державної влади України : монографія. Київ : МП «Леся», 2013. 220 с.

21. Мороз Д. О. Адміністративно-правові засади діяльності податкової міліції як суб’єкта інформаційних відносин в Україні : автореф. дис… канд. юрид. наук : 12.00.07. Ірпінь, 2016. 20 с.

22. Бурило Ю. П. Організаційно-правові питання державного управління в інформаційній сфері : автореф. канд. юрид. наук : 12.00.07. Київ, 2008. 20 с.

23. Кохановська О. В. Цивільно-правові проблеми інформаційних відносин в Україні : автореф. дис. д-ра юрид. наук : 12.00.03. Київ, 2006. 34 с.

24. Калюжний Р. А., Копан О. В., Марценюк О. Г. Теоретико-методологічні засади інформаційного права України: реалізація права на інформацію : монографія. Київ : «МП Леся», 2013. 236 с.

25. Кормич Б. А. Інформаційне право : підручник для вузів. Харків : Бурун і К, 2011. 334 с.

26. Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України : автореф. дис. … д-ра юрид. наук : 23.00.02. Одеса, 2005. 36 с.

27. Петров Д. О. Інформаційні правовідносини в Україні : автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2014. 18 с.

28. Кузнецова М. Ю. Органи виконавчої влади України як суб'єкт інформаційних правовідносин : автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2015. 23 с.

29. Кушнір І. П. Теоретичні засади дослідження інформаційних відносин у діяльності Державної прикордонної служби України. *Держава та регіони. Право.* 2019. № 4. С. 86–91.

30. Зьолка В. Л. Охорона національних інтересів України у прикордонній сфері (адміністративно-правовий аспект) : монографія. Хмельницький : Вид-во НАДПСУ, 2015. 672 с.

31. Ляшук Р. М. Діяльність відділів прикордонної служби Державної прикордонної служби України (адміністративно-правовий аспект) : монографія / за заг. ред. В. Л. Грохольського. Хмельницький : Вид-во НАДПСУ, 2015. 386 с.

32. Словник української мови. В 11 томах. Том 1. 1970 с. 547. URL: http://sum.in.ua/s/vyjavljaty (дата звернення: 21.05.2018).

33. Фаріон О. Б. Інформаційне забезпечення стратегічного кримінального аналізу в оперативно-розшукових підрозділах Державної прикордонної служби України. *Збірник наукових праць Національної академії Державної прикордонної служби України. Військові науки*. 2017. № 3. С. 154–166.

34. Фаріон О. Б. Алгоритм опрацювання оперативно-розшукової інформації для забезпечення потреб кримінального аналізу злочинної діяльності. *Збірник наукових праць Національно академії Державної прикордонної служби України. Військові науки.* 2013. № 1. С. 194–203.

35. Фаріон О. Б. Інструментарій визначення типу загроз прикордонній безпеці в процесі проведення стратегічного кримінального аналізу оперативно-розшуковим підрозділом регіонального управління Державної прикордонної служби України. *Збірник наукових праць Національної академії Державної прикордонної служби України. Військові науки*. 2013. № 2. С. 212–218.

36. Кушнір І. П. Методологічні засади теорії інформаційних відносин у прикордонній сфері. National law journal: theory and practice. 2019. № 2 (36). С. 17–20.

37. Філософський енциклопедичний словник / В. І. Шинкарук та інші. Київ : Абрис, 2002. 751 с.

38. Юридична енциклопедія : в 6 т. / редкол. Ю. С. Шемшученко (голова редкол.) та ін. Київ : Укр. енцикл., 2002. Т. 4 : Н–П. 720 с.

39. Зайчук О. В., Оніщенко Н. М. Теорія держави і права: академічний курс: підручник. 2-ге вид., перероб. і допов. Київ : Юрінком Інтер, 2008. 688 с.

40. Пилипчук В. Г., Брижко В. М. Наукова інформація: питання теорії, викладення та редагування. *Інформація і право.* 2015. № 3. С. 135–149.

41. Теорія держави і права : підручник / М. В. Цвік та ін. ; за ред. М. В. Цвік, О. В. Петришина. Харків : Право, 2010. 584 с.

42. Андрушко О. В. Методологічні підходи до наукового дослідження юридичної відповідальності за правопорушення у кримінальному процесі. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки.* 2017. Вип. 4. URL: http://nbuv.gov.ua/UJRN/vnadpcurn_2017_4_3 (дата звернення: 07.01.2019).

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

44. Шевчук Р. М. Методологія наукового пізнання: від явища до сутності. *Філософські та методологічні проблеми права*. 2016. № 1 (11). С. 31–44.

45. Сопілко І. М. Засади інформаційної гносеології. *Право і суспільств*. 2014. № 3. С. 228–234.

46. Рабінович П. М. Методологія юридичної науки. Юридична енциклопедія : в 6 т. / [голова редкол. Ю. С. Шемшученко]. Київ : Вид-во «Українська енциклопедія» імені М. П. Бажана, 1998–2004. Т. 3 : К–М. 2001. 789 с.

47. Селезньова О. М. Методи науки інформаційного права. *Право і суспільство.* 2015. № 2. С. 184–189.

48. Ліпкан В. А., Дімчогло М. І. Консолідація інформаційного законодавства України : монографія / за заг. ред. В. А. Ліпкана. Київ : ФОП О. С. Ліпкан, 2014. 416 с.

49. Ліпкан В. А., Череповський К. П. Інкорпорація інформаційного законодавства України : монографія / за заг. ред. В. А. Ліпкана. Київ : ФОП О. С. Ліпкан, 2014. 408 с.

50. Притула А. М. Теоретико-правові засади оперативно-службової діяльності Державної прикордонної служби України : монографія. Одеса : Фенікс, 2019. 332 с.

51. Жаровська І. М. Щодо проблем методології теорії держави і права. *Вісник Національного університету «Львівська політехніка». Юридичні науки*. 2015. № 827. С. 138–141.

52. Цимбалюк В. С. Методологія інформаційного права як комплексної галузі юридичної науки (засадничі, принципові положення). *Правова інформатика.* 2007. № 3(15). С. 40–51.

53. Крестовська Н. М., Матвєєва Л. Г. Теорія держави і права. Підручник. Практикум. Тести : підручник. Київ : Юрінком Інтер, 2015. 584 с.

54. Колпаков В. К. Адміністративно-деліктний правовий феномен : монографія. Київ : Юрінком Інтер, 2004. 528 с.

55. Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право. Санкт-Петербург : Юридический центр «Пресс», 2001. 789 с.

56. Історія розвитку та виникнення інформаційного права. URL: http://studopedia.su/10_64702_Istoriya-rozvitku-ta-viniknennya-informatsiynogo-prava.html4 (дата звернення: 08.05.2017).

57. Про інформацію : Закон України від 02.10.1992 р. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650. Зі змінами.

58. Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року : розпорядження КМУ від 24.07.2019 р. № 687-р. *Урядовий кур'єр*. 2019. № 170.

59. Про схвалення Стратегії розвитку Державної прикордонної служби України : розпорядження КМУ від 23.11.2015 р. № 1189-р. *Урядовий кур'єр*. 2015. № 220.

60. Угода між Урядом України і Урядом Республіки Польща про пункти пропуску через державний кордон, затверджена постановою КМУ від 25.03.93 № 223. *Офіційний вісник України*. 2005. № 24. Ст. 1375.

61. Кушнір І. П. Інформаційні відносини у прикордонній сфері. *Науковий вісник Ужгородського національного університету.* 2016. № 36. Т. 2. С. 36–38.

62. Копылов В. А. Информационное право. 2-е изд. перераб. и доп. Москва : Юрист, 2002. 512 с.

63. Лисенков С. Л. Загальна теорія держави і права : навчальний посібник. Київ : Юрисконсульт, 2006. 355 с.

64. Скакун О. Ф. Теорія держави і права : підручник. 3-те видання. Київ : Алерта ; ЦУЛ, 2011. 524 с.

65. Кушнір І. П. Доктринальні підходи до різноманітності інформаційних правовідносин. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки.* 2017. Вип. 4. URL: http://nbuv.gov.ua/UJRN/vnadpcurn_2017_4_8 (дата звернення: 10.11.2019).

66. Коваленко Л. Проблеми правового регулювання інформаційних відносин. *Вісник Академії правових наук України*. 2012. № 4. С. 272–277.

67. Кульчій О. О. Інформаційне право : навчально-методичний посібник. Полтава. 2015. 193 с.

68. Гаврилов О. А. Курс правовой информатики : учебник для вузов. Москва : Норма-инфра, 2002. 432 с.

69. Чубукова С. Г., Элькин В. Д. Основы правовой информатики (юридические и математические вопросы информатики) : учебное пособие / под ред. М. М. Рассолова, В. Д. Элькина. Москва : Контракт, 2007. 287 с.

70. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти : монографія / за заг. ред. О. М. Бандурки. Харків : Вид-во Ун-ту внутр. справ, 2000. 368 с.

71. Безверхня І. В., Перевалова Л. В. Поняття інформаційних правовідносин: тези доповідей XIX міжнародної науково-практичної конференції у чотирьох частинах Ч. IV. Харків. 2011. URL: http://compi.com.ua/naukove-vidannya-tezi-dopovidej-hix-mijnarodnoyi-naukovo-prakt.html?page=21 (дата звернення: 04.10.2017).

72. Огородов Д. В. Правовые отношения в информационной сфере : дис. ... канд. юрид. наук : 12.00.14. Москва, 2002. 243 с.

73. Боер В. М., Павельева О. Г. Информационное право : учеб. пособие. Ч. 1. Санкт-Петербург, 2006. 116 с.

74. Ковалева Н. Н. Информационное право России : учебное пособие. Москва: Издательско-торговая корпорация «Дашков и К», 2007. 360 с.

75. Маріц Д. Поняття та зміст інформаційних правовідносин. *Национальный юридический журнал: теория и практика.* Молдова, 2016. № 5 (21). С. 64–68.

76. Коваленко Л. П. Інформаційні відносини. 2012. URL: tlaw. nlu.edu.ua/article/download/62395/57938.

77. Тихомиров Ю. А. Публичное право. Москва, 1995. С. 339.

78. Басараб О. Т. Поняття системи прикордонного законодавства. *Університетські наукові записки*. 2013. № 3. С. 366–372.

79. Про Державну прикордонну службу України : Закон України від 03.04.2003 р. *Відомості Верховної Ради України*. 2003. № 27. Ст. 208.

80. Інформаційне право та правова інформатика : курс лекцій / В. Г. Хахановський та ін. ; за заг. ред. проф. Є. М. Моісеєва. Київ : Київський національний університет внутрішніх справ, 2007. 253 с.

81. Хоменко І. В. Логіка для юристів : підручник. Київ. Юрінком Інтер. 2004. 224 с.

82. Маріц Д. О. Критерії класифікації інформаційних правових відносин в Україні. *Прикарпатський юридичний вісник*. 2018. № 1 (22). С. 127–132.

83. Лапина М. А., Ревин А. Г., Лапин В. І. Информационное право. Москва : Юнити-дана ; Закон и право, 2004. 335 с.

84. Информационные правоотношения: теоретические аспекты : монография / И. М. Рассолов и др. Москва : ООО Проспект, 2016. 263 с.

85. Курс адміністративного права України : підручник / В. К. Колпаков та ін. 2-ге вид., перероб. і допов. Київ : Юрінком Інтер, 2013. 872 с.

86. Яременко О. І. Інформаційні відносини як предмет правового регулювання : теоретичний аспект. *Вісник Хмельницького інституту регіонального управління та права*. Хмельницький, 2004. №. 1–2. С. 156–161.

87. Кушнір І. П. Нормативно-правове регулювання інформаційних відносин у діяльності Державної прикордонної служби України: теоретичні та організаційні аспекти : монографія / за заг. ред. д-ра юрид наук Р. М. Ляшука, Хмельницький. Вид-во: ПП «Монускрипт», 2020. 528 с.

88. Кузнецова М. Ю. Критерії класифікації інформаційних правовідносин за участю органів виконавчої влади України в умовах розвитку інформаційного суспільства. *Порівняльно-аналітичне право*. 2015. № 6. С. 200–203.

89. Попов Л. Л., Мигачев Ю. И., Тихомиров С. В. Информационное право : учебник. Москва : Норма ; Инфра-М, 2010. 495 с.

90. Перов Д. О., Климентьєв О. П. Зміст та структура інформаційних правовідносин. *Науковий вісник Міжнародного гуманітарного університету*. *Юриспруденція.* 2013. № 6–3. Том 1. С. 81–84.

91. Кушнір І. П. Класифікація інформаційно-правових відносин у прикордонній сфері. *Вісник Запорізького національного університету. Юридичні науки*. 2017. № 4. С. 56–62.

92. Про затвердження Положення про базу даних «Відомості про осіб, які перетнули державний кордон України» : наказ Адміністрації Державної прикордонної служби України від 25.06.2007 р. № 472. *Офіційний вісник України*. 2007. № 50. Ст. 2047.

93. Карташов В. Н. Теория правовой системи общества : учебное пособие: в 2 т. Т. І. Ярославль : ЯрГУ, 2005. 547 с.

94. Селезньова О. М. Структура інформаційних правовідносин. *Науковий вісник Ужгородського національного університету. Право*. 2014. №. 27(2). С. 183–186.

95. Коваленко Л. П. Суб'єкти інформаційних правовідносин. *Ученые записки Таврического национального университета им. В. И. Вернадского*. *Юридические науки*. 2012. № 2. Т. 25(64). С. 376–379.

96. Про захист прав споживачів : Закон України від 12.05.1991 р. № 1023-XII URL: https://zakon.rada.gov.ua/laws/ show/1023-12 (дата звернення: 03.06.2019).

97. Про доступ до публічної інформації : Закон України від 13.01.2011 р. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.

98. Кушнір І. П. Види інформації, розпорядником якої є Державна прикордонна служба України, їх сутнісна характеристика. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2018. Вип. 1. URL: http://nbuv.gov.ua/UJRN/vnadpcurn_2018_1_6 (дата звернення: 17.06.2018).

99. Розпорядники інформації. Методичні рекомендації Головного територіального управління юстиції у Донецькій області м. Краматорськ, 2016. URL: http://justice-dn.gov.ua/index.php/19-publichna-informatsiya/1077-rozporyadniki-informatsiji (дата звернення: 18.12.2018).

100. Положення про орган охорони державного кордону Державної прикордонної служби України : наказ Міністрества внутрішніх справ України від

30.11.2018 р. № 971. URL: https:// zakon.rada.gov.ua/laws/show/z1468-18 (дата звернення: 01.02.2020).

101. Банчук О. А. Науково-практичний коментар до Кодексу адміністративного судочинства України. Київ. 2011. 753 с.

102. Білокур Є. І. Функції державного управління: поняття, особливості, правове регулювання : дис. ... канд. юрид. наук : 12.00.07. Одеса, 2015. 195 с.

103. Адміністративне право України : підручник / Ю. П. Битяк та ін. ; за ред. Ю. П. Битяка. Київ : Юрінком Інтер, 2007. 544 с.

104. Денисова А. Співвідношення контролю та нагляду. *Адміністративне право і процес*. 2013. № 2(4). С. 30–37.

105. Про прокуратуру : Закон України від 14.10.2014 р. № 1697/VII. *Офіційний вісник України*. 2014. № 87. Ст. 9.

106. Кушнір І. П. Органи охорони державного кордону як суб'єкти інформаційних правовідносин. *Правові новели*. 2018. № 5. С. 71–77.

107. Цивільний кодекс України : Закон України від 16.01.2003 р. № 435-IV. *Відомості Верховної Ради України,* 2003, № 40–44. Ст. 356.

108. Про внесення змін у розпорядження Адміністрації Державної прикордонної служби України від 11.07.2006 р. № 412 : розпорядження Адміністрації Державної прикордонної служби України від 14.11.2006 р. № 680. Окреме видання.

109. Департамент інформаційно-аналітичного та доку-ментального забезпечення. URL: https://dpsu.gov.ua/ua/ Departamentu-informaciino-analitycnogo-ta-dokumentalnogo-zabezpech ennya/ (дата звернення: 20.042.2018).

110. Частини центрального підпорядкування. Головний центр зв'язку, автоматизації та захисту інформації URL: https://dpsu.gov.ua/ua/structure/chastini-centralnogo-pidporyadkuva nnya/golovniy-centr-zvyazku-avtomatizacii-ta-zahistu-informacii/ (дата звернення: 20.04.2018).

111. Служба «Довіра». URL: https://dpsu.gov.ua/ua/sluzhba-dovira/ (дата звернення: 27.04.2018).

112. Про затвердження Інструкції з діловодства в Державній прикордонній службі України : наказ АДПСУ від 17.05.2004 р. № 400. Окреме видання.

113. Інструкція про порядок забезпечення доступу до публічної інформації у Державній прикордонній службі України : наказ Адміністрації Державної прикордонної служби України від 03.04.2012. № 222. *Офіційний вісник України*. 2012. № 37. Ст. 1404.

114. Баранов О. А. Інститути інформаційного права. *Правова інформатика*. 2006. № 3. С. 40–46.

115. Шпенов Д. Суб'єкти правовідносин в інформаційній сфері. *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки.* 2011. Вип. 89. С. 92–95.

116. Резченко Є. О. Необхідність розробки та прийняття Закону України «Про інформаційне забезпечення органів державної влади» (робоча назва). *Державне будівництво*. 2007. № 1(2). С. 1–14.

117. Гіда Є. О., Білозьоров Є. В., Завальний А. М. Теорія держави і права : підручник ; за заг. ред. Є. О. Гіди. Київ : ФОП, 2011. 576 с.

118. Адміністративне право України : підручник. вид 2-ге, змін. і доп. / за заг. ред. Т. О. Коломоєць. Київ : Істина, 2012. 528 с. URL: https://pidruchniki.com/1183121955843/pravo/administrativno-pravoviy_status_tsentralnih_organiv_vikona vchoyi_vladi (дата звернення: 17.01.2018).

119. Адміністративне право України : підручник / за заг. ред. Т. О. Коломоєць. Київ : Істина, 2008. 457 с.

120. Ковалів М. В., Стахура І. Б. Особливості адміністративно-правового статусу органів виконавчої влади. *Вісник Національного університету «Львівська політехніка». Юридичні науки*. 2014. № 807. С. 22–26.

121. Саблук С. А. Правосуб'єктність як елемент правового статусу дитини. *Університетські наукові записки*. 2008. № 2. С. 101–105.

122. Нечипорук Ю. Суб'єктний та об'єктний склад інформаційних правовідносин. *Юридична Україна*. 2012. № 6. С. 39–44.

123. Кузнецова М. Ю. Реалізація інформаційно-правового статусу органів виконавчої влади України під час захисту персональних даних. *Право і суспільство.* 2014. № 6. Ч. 1. С. 131–139.

124. Качур В. О. До визначення поняття «правосуб'єктність» у теорії права. *Науковий вісник Національного університету біоресурсів і природокористування України*. 2014. Вип. 197. Ч. 3. С. 24–29.

125. Кушнір І. П. Інформаційно-правовий статус Державної прикордонної служби України. *Приватне та публічне право*. 2018. № 4. С. 50–53.

126. Конституція України : Закон України від 28.06.1996. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: http://zakon0.rada.gov.ua/laws/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 05.02.2020).

127. Гелич Ю. О. Види інформації за законодавством України. *Правничий вісник Університету «КРОК»*. 2011. Вип. 10. С. 84–88.

128. Про інформацію : Закон України від 2 жовтня 1992 року. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650. В редакції від 06.01.2011, підстава 2724-17.

129. Гаман Т. В. До питання забезпечення інформацією органів державного управління. *Вісник Хмельницького інституту регіонального управління та права*. 2004. № 4. С. 307–312.

130. Яременко О. І. Офіційна правова інформація в Україні: поняття, класифікація, джерела. *Підприємництво, господарство і право*. 2005. № 10. С. 101–102.

131. Офіційний словник іншомовних слів. URL: www.jnsm. com.ua/cgi-bin/u/book/sis.pl?Qry=Офіційний&found=8& action (дата звернення: 13.11.2017).

132. Палеха Ю. Загальне діловодство : теорія та практика керування документацією із загальних питань. Видавництво «Ліра-К», 2014. 624 с. URL:

http://pidruchniki.com/1228112860534/dokumen toznavstvo/ofitsiyni_dokumenti (дата звернення: 27.12.2017).

133. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації : Закон України від 23.09.1997 р. *Відомості Верховної Ради України*. 1997. № 49. Ст. 299.

134. Словник української мови : в 11 томах. Том 8, 1977. С. 383. URL: http://sum.in.ua/s/publichnyj (дата звернення: 11.12.2017).

135. Види інформації. URL: https://dpsu.gov.ua/ua/vidi-informacii/ (дата звернення: 11.12.2017).

136. Цехмістрова Г. С. Основи наукових досліджень : навчальний посібник. Київ : Видавничий Дім «Слово», 2003. 240 с. URL: http://www.info-library.com.ua/books-text-3032.html (дата звернення: 16.11.2017).

137. Тихомиров О. О. Правова інформація: теоретико-правовий аспект. *Інформаційна безпека людини, суспільства, держави*. 2012. № 1 (8). С. 29–35.

138. Правова інформація та комп'ютерні технології в юридичній діяльності : навч. посіб. / за заг. ред. В. Г. Іванова. Харків : Право, 2010. 240 с.

139. Подання запиту на інформацію (довідково-енциклопе-дична, науково-технічна, правова, статистична, соціологічна тощо). URL: https://dpsu.gov.ua/ua/podannya-zapitu-na-informaciyu-dovidkovo-enciklopedichna-naukovo-tehnichna-pravova-statistichna-sociologichna-toshcho/ (дата звернення: 10.12.2017).

140. Про державну статистику : Закон України від 17.09.1992 р. *Відомості Верховної Ради України*. 1992. № 43. Ст. 608.

141. Кормич Б. А. Трансформація поняття та типології інформації в новому інформаційному законодавстві. *Актуальні проблеми політики : Зб. наук. праць.* Одеса, 2012. Вип. 44. С. 296–305.

142. Погорілецька А. В. Офіційна інформація: теоретико-правовий аспект. *Питання юридичної теорії і практики* : *Вісник Вищої ради юстиції.* 2012. № 1 (9). С. 131–140.

143. Плішкін В. М. Теорія управління органами внутрішніх справ : підручник / за ред. канд. юрид. наук Ю.Ф. Кравченка. Київ : Національна академія внутрішніх справ України, 1999. 702 с.

144. Перелік пунктів пропуску. URL: http://dpsu.gov.ua/ua/ Perelik-punktiv-propusku (дата звернення: 07.09.2018).

145. Про затвердження Порядку подання авіаперевізникам або уповноваженим ними особами попередньої інформації про пасажирів, імпортні та транзитні вантажі, які перевозяться повітряними суднами, органам охорони державного кордону та митним органам : наказ Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства інфраструктури України від 27.04.2012 № 291/506/228. URL: https://dpsu.gov.ua/ua/Zvit-pro-periodichne-vidstezhennya-rezultativnosti-regulyatornogo-akta-nakazu-Administracii-Derzhavnoi-prikordonnoi-sluzhbi-Ukraini-Ministerstva-finansiv-Ukraini-Ministerstva-infrastrukturi-Ukraini-vid-27042012-291506228-zarestrovanogo-v-Ministerstvi-yust/ (дата звернення: 22.12.2019).

146. Трофименко О. Г., Дубовий Я. В. Еволюція поглядів на інформаційні війни в епоху інформаційного суспільства. *Порівняльно-аналітичне право*. 2017. № 1. С. 189–192.

147. Безвершенко О. О. Інформаційна безпека України в системі забезпечення національної безпеки. URL: http://www.rusnauka.com/13_NPN_2010/Pravo/66151.doc.htm (дата звернення: 18.12.2017).

148. Про рішення Ради національної безпеки і оборони України від 29.12.2016. «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017. *Офіційний вісник Президента України*. 2017. № 5. Ст. 102.

149. Кушнір І. П. Прикордонна інформаційна безпека як складова національної безпеки України. *Освітньо-наукове забезпечення складових сектору безпеки і оборони України* : тези XI Всеукраїнської науково-практичної

конференції (Хмельницький, 15 листопада 2018 року). Хмельницький : Вид-во НАДПСУ, 2018. С. 247–248.

150. Словник української мови : в 11 томах. Том 7, 1976. С. 80. URL: http://sum.in.ua/s/polityka (дата звернення: 08.11.2017).

151. Горлач М. І., Кремень В. Г. Політологія: наука про політику : підручник. Київ : Центр навчальної літератури, 2009. 840 с.

152. Політичні аспекти формування та охорони державного кордону : навчальний посібник / М. І. Кабачинський, Т. В. Бунєєв, І. Г. Блощинський, С. В. Сінкевич. Хмельницький : Вид-во НАДПСУ, 2015. 400 с.

153. Плахотний М. Загрози національній безпеці України на державному кордоні. *Ефективність державного управління* : Збірник наукових праць. 2013. Вип. 36. С. 105–111.

154. Про прикордонний контроль : Закон України від 05.11.2009 р. *Відомості Верховної Ради України.* 2010. № 6. Ст. 46.

155. Про затвердження Порядку в'їзду на тимчасово окуповану територію України та виїзду з неї (із змінами) : постанова Кабінету Міністрів України від 04.06.2015 р. № 367. URL: http://zakon5.rada.gov.ua/laws/show/367-2015-%D0%BF. (дата звернення: 14.07.2019).

156. Про затвердження Положення про Департамент оперативної діяльності Адміністрації Державної прикордонної служби України та його структурні підрозділи : наказ Адміністрації Державної прикордонної служби України від 11.12.2014 р. № 196. Окреме видання.

157. Литвин М. М. Інтегроване управління кордонами : підручник. Хмельницький : Вид-во НАДПСУ, 2012. 416 с.

158. Про національну безпеку України : Закон України від 21.06.2018. *Голос України*. 2018. № 22.

159. Про затвердження Положення про Адміністрацію Державної прикордонної служби України : постанова Кабінету Міністрів України від 16.10.2014 р. № 533. *Урядовий кур'єр*. 2014. № 195.

160. Труш О. О. Механізми реалізації державної політики у сфері цивільного захисту в Україні. *Теорія та практика державного управління*. 2010. Вип. 4. С. 420–426.

161. Про деякі заходи з оптимізації системи центральних органів виконавчої влади : Указ Президента України від 24.12.2012 р. № 726/2012. URL: https://zakon.rada.gov.ua/laws/ show/726/2012#n22 (дата звернення: 19.12.2019).

162. Про деякі заходи з оптимізації системи центральних органів виконавчої влади : Указ Президента України від 09.12.2010 р. № 1085/2010. *Офіційний вісник України.* 2010. № 32. Ст. 1026.

163. Корж І. Ф. Державна прикордонна служба України: правовий статус та місце в системі сектору безпеки і оборони. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2017. Вип. 2. URL: http://nbuv.gov.ua/ UJRN/vnadpcurn_2017_2_3 (дата звернення: 04.01.2020).

164. Про основи національної безпеки України: Закон України від 19.06.2003 р. Відомості Верховної Ради України. 2003. № 39. Ст. 351.

165. Литвин М. М. Основи інтегрованого управління кордонами : курс лекцій. Хмельницький : Вид-во НАДПСУ, 2011. 386 с.

166. Охорона державного кордону України в сучасних геополітичних умовах : організаційні та правові проблеми : монографія / О. В. Андрушко та ін. Хмельницький : Вид-во НАДПСУ, 2017. 296 с.

167. Про схвалення Концепції інтегрованого управління кордонами : розпорядження Кабінету Міністрів України від 28.10.2015 р. № 1149-р. *Урядовий кур'єр*. 2015. № 210.

168. Кушнір І. П. Аналіз змісту поняття «безпека державного кордону». *Вісник Південного регіонального центру Національної академії правових наук України*. 2018. № 16. С. 75–81.

169. Цевельов О. Є. Державне реагування на загрози національній безпеці у сфері безпеки державного кордону України : дис.. канд..наук з держ. управл. : 25.00.05. Хмельницький, 2017. 313 с.

170. Корж І. Ф. Адміністративно-правове регулювання відносин у сфері державної безпеки України : монографія. Вінниця : ТОВ «Нілан-ЛТД», 2013. 384 с.

171. Данільян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України. Сутність, структура та напрямки реалізації: навчальний посібник. Харків : ФОЛІО, 2002. 285 с.

172. Горбулін В. П., Качинський А. Б. Засади національної безпеки України: підручник. Київ : Інтертехнологія, 2009. 272 с.

173. Ліпкан В. А. Національна безпека України : навчальний посібник. 2-ге вид. Київ : КНТ, 2009. 576 с.

174. Марченко Б. М. Адміністративна діяльність Державної прикордонної служби України : автореф. дис. ... канд. юрид. наук : 12.00.07. Дніпропетровськ, 2009. 20 с.

175. Купрієнко Д., Білявець С. Прикордонна безпека України: національний та міжнародний аспекти. Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку : збірник матеріалів ІІІ міжнародної науково-практичної конференції (14 червня 2019 р.), Острог. НУОА, НДІІП НАПрН України. Київ : ТОВ «Видавничий дім «АртЕк», 2019. С. 161–164.

176. Курилюк Ю. Б. Державний кордон і правопорядок (законодавство, теорія, практика) : монографія. Київ : ВД «Дакор», 2020. 446 с.

177. Мельников О. Г. Інтегрований прикордонний менеджмент – європейська модель управління кордонами для України. *Вісник Державної прикордонної служби України.* 2008. № 3. С. 46–51.

178. Ананьїн О. В. Прикордонна безпека України в сучасних умовах. URL: http://scientistsua.at.ua/index/ananin_oleg_valer evich/0-24 (дата звернення: 16.10.2018).

179. Нікіфоренко В. С. Поняття та сутність державного управління у сфері забезпечення прикордонної безпеки України. *Державне управління: удосконалення та розвиток.* 2014. № 12. URL: http://www.dy.nayka.com.ua/?n=12&y=2014 (дата звернення: 14.07.2018).

180. Словник української мови: в 11 томах. Том 1, 1970. С. 137. URL: http://sum.in.ua/s/bezpeka (дата звернення: 18.07.2018).

181. Короткий словник політологічних термінів. Безпека. URL: http://politics.ellib.org.ua/encyclopedia-term-252.html (дата звернення: 18.07.2018).

182. Про державний кордон України : Закон України від 04.11.1991 р. *Відомості Верховної Ради України*. 1992. № 2. Ст. 5.

183. Словник української мови : в 11 томах / АН УРСР. Інститут мовознавства; за ред. І. К. Білодіда. Київ : Наукова думка, 1970–1980. Т. 8. С. 643. URL: http://ukrlit.org/slovnyk/%D0%BF%D1%80%D0%B8%D0%BA%D0%BE%D1%80%D0%B4%D0%BE%D0%BD%D0%BD%D1%8F (дата звернення: 26.06.2018).

184. Угода між Кабінетом Міністрів України та Урядом Російської Федерації про порядок перетинання українсько-російського державного кордону жителями прикордонних регіонів України та Російської Федерації від 18.10.2011 р. Дата ратифікації Україною: 22.02.2012 р. Дата набрання чинності для України 29.03.2012 р. *Офіційний вісник України*. 2012. № 21, 37. Ст. 788.

185. Мілашовська О. І. Прикордонний регіон як об'єкт дослідження регіональної економіки. *Ефективна економіка* 2010. № 3. URL: http://www.economy.nayka.com.ua/?op=1&z=173 (дата звернення: 04.09.2018).

186. Про прикордонний режим : постанова Кабінету Міністрів України від 27.07.1998 р. №1147. *Офіційний вісник України*. 1998. № 30. Ст. 33.

187. Фролов С. М., Скляр І. Д. Бюджетний менеджмент прикордонних територій (теорія і практика) URL: http://elkniga.info/book_21_glava_37_7.1._Viznachennja_statusu_%D1%96_k.html (дата звернення: 21.08.2018).

188. Царенко С. І. Адміністративно-правове регулювання та забезпечення прикордонного режиму Державною прикордонною службою України : дис. ... канд. юрид. наук : 12.00.07. Київ, 2014. 310 с.

189. Цимбалістий Т. О. Державний кордон України : конституційно-правовий статус : навч. посіб. Хмельницький : Вид-во НАПВУ, 2000. 204 с.

190. Braman S. *D*efining information policy. *Journal of Inform-ation Policy*. 2011. Vol. 1.

191. Ліпкан В. А., Максименко Ю. Є. , Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посібник. Київ : КНТ, 2006. 280 с. URL: http://pidruchniki.com/17190512/politologiya/ponyattya_osoblivosti_informatsiynoyi_politiki_derzhavi (дата звернення: 11.09.2017).

192. Почепцов Г. Г. Інформаційна політика: сучасні підходи. URL: http://osvita.mediasapiens.ua/ethics/manipulation/informatsiyna_politika_suchasni_pidkhodi/ (дата звернення: 16.06.2019).

193. Департамент організаційно-адміністративної роботи та аналітичного забезпечення. URL: https://dpsu.gov.ua/ua/ Departame ntu-organizaciyno-administrativnoi-roboti-ta-analitichno go-zabezpeche nnya/ (дата звернення: 04.10.2018).

194. Іванченко Ю. М. Сутність, головні напрями та способи державної інформаційної політики в Україні. *Державне управління теорія та практика*. 2005. № 2. URL: academy.gov.ua/ej/ej2/txts/ philo/05ijmipu.pdf (дата звернення: 07.04.2018).

195. Попова Т. Чому потрібне оперативне управління? URL: https://www.radiosvoboda.org/a/28387220.html (дата звернення: 07.04.2018).

196. Лісовська Ю. П. Адміністративно-правове забезпечення інформаційної безпеки в Україні : дис. ... канд. юрид. наук : 12.00.07. Київ, 2017. 204 с.

197. Fruhlinger J. What is information security? Definition, principles, and jobs. URL: https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html (дата звернення: 26.01.2020).

198. Про Концепцію Національної програми інформатизації : Закон України від 04.021998. *Відомості Верховної Ради України*. 1998. № 27. Ст. 182.

199. Проект Концепції інформаційної безпеки України. Міністерство інформаційної політики України. URL: http://mip.gov.ua/ru/documents/30.html (дата звернення: 16.11.2017).

200. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007. *Відомості Верховної Ради України.* 2007. № 12. Ст. 102.

201. Суббот А. Інформаційна безпека суспільства. *Віче*. 2015. № 8. С. 29–31.

202. Кириленко В. А. Методика інформаційно-аналітичного забезпечення вирішення спеціального комплексного завдання щодо оцінки бойової та мобілізаційної готовності підлеглих підрозділів. *Збірник наукових праць Національної академії Державної прикордонної служби України імені Б. Хмельницького*. *Військові та технічні науки.* 2014. № 1 (61). С. 79–90.

203. Громико І. О., Саханчук Т. І. Інформаційна безпека України. *Системи обробки інформації*. 2009. Вип. 7. С. 115–116.

204. Северина С. В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету*. *Економічні науки.* 2016. № 1. С. 155–161.

205. Муравська (Якубівська) Ю. Є. Інформаційна безпека суспільства: концептуальний аналіз. *Економіка та суспільство*. 2017. № 9. С. 289–294.

206. Кузьменко А. М. Особливості проблем законодавчого забезпечення інформаційної безпеки держави, суспільства і громадянина в умовах інформаційно-психологічного протиборства. *Часопис Київського університету права*. 2010. № 4. С. 317–321.

207. Інформаційна безпека особистості. URL: https://sites.google.com/site/infobezpekaosobu/informacijna-bezpeka (дата звернення: 29.07.2019).

208. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України. *Політичний менеджмент*. 2008. № 4. С. 135–141. URL: http://nbuv.gov.ua/UJRN/PoMe_2008_4_16 (дата звернення: 19.11.2017).

209. Субіна Т. В. Адміністративно-правове забезпечення інформаційної безпеки в органах Державної податкової служби України : автореф. дис. ... канд. юрид. наук : 12.00.07. Ірпінь, 2010. 19 с.

210. Информационные технологии в юридической деятельности : учебник для бакалавров. Уральская государственная юридическая академія ; под. ред. П. У. Кузнецова. Москва : Юрайт, 2012. URL: https://stud.com.ua/34557/informatika/stan_zahischenosti (дата звернення: 11.09.2018).

211. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах Євроінтеграції України: правовий вимір : монографія. Київ : ТОВ «Видавничий дім АртЕк», 2018. 422 с.

212. Логінов О. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : автореф. дис... канд. юрид. наук : 12.00.07. Київ, 2005. С. 20.

213. Кормич Б. А. Правові засади політики інформаційної безпеки України : монографія. Одеса : Юрид. літ., 2003. 472 с.

214. Бєляков К. І. Правове та організаційне забезпечення інформаційної безпеки у воєнний сфери / Військове право: підручник / за ред. І. М. Коропатніка, І. М. Шопіної. Київ: Алерта, 2019. 648 с. С. 453–491.

215. Кушнір І. П. Співвідношення понять «інформаційна безпека» та «захист інформації» в діяльності Державної прикордонної служби України. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція.* 2018. № 35. Т. 1. с. 81–84.

216. Юридична енциклопедія : в 6 т. / ред. кол. Ю. С. Шемшученко та ін. Київ : Українська енциклопедія, 1998. Т. 2 : Д–Й. 744 с. URL: http://leksika.com.ua/18590418/legal/zahist_informatsiyi (дата звернення: 10.05.2018).

217. Кушнір І. П. Основні засади інформаційної політики держави в прикордонній сфері. *Науковий вісник Херсонського державного університету. Юридичні науки*. 2017. Вип. 6. Т. 2. С. 81–84.

218. Кушнір І. П. Напрями прикордонної інформаційної безпеки як складова національної безпеки України. *Порівняльно-аналітичне право*. 2017. № 5. С. 230–233.

219. Коваленко Л. П. Інформаційна діяльність. *Правова інформатика*. 2012. № 4(36). С. 10–13.

220. Кормич Б. А. Конституційно-правове регулювання інформаційних відносин. *Юридичний вісник*. 2013. № 3. С. 46–51.

221. Дорогих С. О. Сутність та визначення понять «інформаційна діяльність» та «інформаційна діяльність органів влади». *Інформація і право.* 2013. № 3(9). С. 74–82.

222. Пилипчук В. Г., Брижко В. М. Проблеми становлення і розвитку інформаційного законодавства в контексті євроінтеграції України. *Інформація і право*. 2011. № 1(1). С. 11–19.

223. Кушнір І. П. Інформаційно-правова діяльність Державної прикордонної служби України: нормативно-правовий аспект. *Конституційно-правові академічні студії.* 2018. № 2. С. 165–170.

224. Буртник Х. Конфіденційна інформація, інформація про особу та персональні дані. URL: https://dostup.pravda.com.ua/news/publications/konfidentsiina-informatsiia-informatsiia-pro-osobu-ta-personalni-dani-spivvidnoshennia-i-rehuliuvannia (дата звернення: 20.02.2019).

225. Зьолка В. Л. Концепція охорони національних інтересів України у прикордонній сфері (адміністративно-правовий аспект) : автореф. дис. … д-ра. юрид. наук : 12.00.07. Київ, 2015. 40 с.

226. Коротушак А. І. Місце та значення правового механізму в структурі механізму державного управління публічною інформацією з обмеженим доступом у Державній прикордонній службі України. *Право та державне управління*. 2014. № 1–2. С. 155–159.

227. Коротушак А. І. Мотиваційний механізм в структурі державного управління публічною інформацією у Державній прикордонній службі України. *Університетські наукові записки*. 2014. № 3. С. 211–217.

228. Мандзюк О. А. Правовий режим податкової інформації в Україні : автореф. дис. … канд. юрид. наук : 12.00.07. Запоріжжя, 2014. 15 с.

229. Кушнір І. П., Царенко О. М. Правовий режим інформації з обмеженим доступом у діяльності Державної прикордонної служби України. *Право та державне управління.* 2019. № 3. С. 180–185.

230. Крестьянінов О. О. Правове регулювання митних режимів : автореф. дис... канд. юрид. наук : 12.00.07. Харків, 2002. 20 с.

231. Ліпкан В. А., Баскаков В. Ю. Адміністративно-правовий режим інформації з обмеженим доступом в Україні : монографія / за заг. ред. В. А. Ліпкана. Київ : ФОП О. С. Ліпкан, 2013. 344 с.

232. Логінова Н. І., Дробожур Р. Р. Правовий захист інформації : навчальний посібник. Одеса : Фенікс, 2015. 264 с.

233. Чернишова Т. В. Правові режими інформації за законодавством України. *Право і суспільство*. 2012. № 4. С. 97–101.

234. Гордієнко С. Г. Конфіденційна інформація та «таємниці»: їх співвідношення. *Часопис Київського університету права*. 2013. № 4. С. 233–238.

235. Словник української мови : в 11 томах. Том 4, 1973. С. 273 URL: http://sum.in.ua/s/konfidencijnyj (дата звернення: 16.09.2018).

236. Інструкції із захисту публічної інформації у Державній прикордонній службі України : наказ Адміністрації ДПСУ від 07.07.2011 р. № 501. Окреме видання.

237. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII. URL: https://zakon.rada.gov.ua/laws/ show/3855-12 (дата звернення: 19.09.2019).

238. Про затвердження Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на

підприємствах, в установах і організаціях : постанова Кабінету Міністрів України від 18.12.2013 р. № 939. ДСК.

239. Про затвердження Зводу відомостей, що становлять державну таємницю : наказ СБ України від 12.08.2005 р. № 440. URL: https://zakon.rada.gov.ua/laws/show/z0902-05#n14 (дата звернення: 19.11.2019).

240. Благодарний А. М. Адміністративна відповідальність за порушення законодавства про державну таємницю : дис… канд.. юрид. наук : 12.00.07. Київ. 2006. 200 с.

241. Мірошник Ю. П. Організаційно-правові засади охорони державної таємниці в Україні. *Науковий вісник НАВСУ*. Київ. 2004. № 4. С. 51–57.

242. Баскаков В. Ю. Інформація з обмеженим доступом: аналіз термінологічно-понятійного апарату. *Підприємництво, господарстов і право.* 2011. № 5. С. 124–127.

243. Сибіга О. М. Доступ до державної таємниці: місце в системі режимів доступу до інформації та розвиток національного законодавства. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція.* 2018. № 35. Т. 1. С. 77–80.

244. Дейнега Х. Інформаційно-аналітичне забезпечення діяльності органів виконавчої влади: *Актуальні проблеми державного управління : зб. наук. пр. ОРІДУ*. Вип. 1 (53). Одеса : ОРІДУ НАДУ, 2013. С. 64–67.

245. Грохольський В. Л. Управління діяльністю спеціальних підрозділів МВС України по боротьбі з організованою злочинністю : автореф. дис... д-ра юрид. наук : 12.00.07. Харків, 2004. 36 с.

246. Вдовиченко Л. Теоретичні підходи до визначення змісту державного регулювання інформаційних відносин у сфері регуляторної діяльності. *Актуальні проблеми державного управління : зб. наук. пр. ОРІДУ*. Вип. 1 (53). Одеса : ОРІДУ НАДУ, 2013. С. 9–12.

247. Єжунінов В. В. Інформаційна складова сучасних державно-суспільних відносин: проблема дефініцій. URL: https://www.

google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwimgfHp8sfnAhWMxosKHfyxBCIQFjAAegQIARAB&url=http%3A%2F%2Fwww.dridu.dp.ua%2Fzbirnik%2F2010-01%2F10evvvpd.pdf &usg=AOvVaw3DSkUC-lRQbTQGnI8Nd-fk (дата звернення: 17.07.2018).

248. Про Статут внутрішньої служби Збройних Сил України : Закон України від 24.03.1999 р. № 548-XIV. *Відомості Верховної Ради України*, 1999. № 22. Ст. 194.

249. Положення про орган охорони державного кордону Державної прикордонної служби України : наказ Адміністрації Державної прикордонної служби України від 15.02.2005 р. № 116. *Офіційний вісник України*. 2005. № 11. С. 27.

250. Основи інформаційно-аналітичної діяльності в Державній прикордонній службі України : підручник / Шинакрук О. М., Артюшин Л. М., Кириленко В. А., Стоянов І. І. Хмельницький : Вид-во НАДПСУ, 2017. 380 с.

251. Bohumil Pikna Evropská pohraniční a pobřežní stráž – „nová“ agentura FRONTEX Časopis Policajná teória a prax 4-2017. PP. 75–84.

252. Kushnir I. Information component in preparing and making management decisions in border protection bodies of the state border of Ukraine. *Legea si Viata*. 2019. № 5. С. 100–104.

253. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. *Відомості Верховної Ради України.* 2001. № 25–26. Ст. 131. URL: http://zakon3.rada.gov.ua/laws/ show/2341-14/page7 (дата звернення: 13.09.2018).

254. Митний кодекс України : Закон України від 13.03.2012 № 4495-VI. *Відомості Верховної Ради України*. 2012. № 44–45, № 46–47, № 48. Ст. 552.

255. Ананьєв О. М., Белей О. М. Інформаційна складова процесу прийняття управлінських рішень в торговельному підприємстві: теоретико-методичні аспекти. *Торгівля, комерція, підприємництво*. 2011. Вип. 12. С. 42–45. URL: http://nbuv.gov.ua/UJRN/Torg_ 2011_12_11 (дата звернення: 23.08.2018).

256. Олійниченко О. М. Інформаційне забезпечення як важлива складова процесу підготовки, реалізації та контролю реалізації управлінського рішення на підприємстві. *Економіка харчової промисловості.* Одеса. 2010. № 3. С. 38–42.

257. Комісаров О. Г. Етапи інформаційного супроводження службово-бойової діяльності. *Честь і закон*. 2014. № 4(51). С. 71–75.

258. Мельник А. Ф., Оболенський О. Ю., Васіна А. Ю. Державне управління : підручник. Київ : Знання, 2009. 582 с.

259. Король М. О. Питання покращення інформаційної складової діяльності Державної прикордонної служби України. *Вісник Львівського торгівельно-економічного університету*. *Юридичні науки.* 2017. Вип. 5. С. 81–87.

260. Комісаров О. Г., Хитра О. Л. Концептуальні підходи до використання категорії «кризової ситуації, що загрожують національній безпеці України». Науковий вісник ДДУВС. 2017. № 3. С. 104–111.

261. Кушнір І. П. Основні тенденції інформаційної взаємодії у діяльності Державної прикордонної служби України. *Visegrad Journal on Human Rights*. 2019. 4 (volume 2). С. 96–101.

262. Положення про функціонування фондових бірж : затверджене рішенням Національної комісії з цінних паперів та фондового ринку від 22.11.2012 р. № 1688. URL: https://zakon.rada.gov.ua/laws/show/z2082-12 (дата звернення: 20.07.2019).

263. Угода між Кабінетом Міністрів України та Урядом Республіки Молдова про організацію обміну інформацією про осіб, транспортні засоби, на яких особи перетинають українсько-молдовський державний кордон : затверджено постановою Кабінету Міністрів України від 08.08.2016 р. № 511. URL: https://zakon.rada.gov.ua/laws/ show/498_169/sp:max15 (дата звернення: 20.07.2019).

264. Про затвердження Вимог до організації роботи з оформлення віз для в'їзду в Україну і транзитного проїзду через її територію : наказ МЗС України,

МВС України, СБ України від 30.10.2017 № 469/897/605. *Офіційний вісник України*. 2017. № 98. Ст. 200.

265. Клементьєв О. П. Інформаційна взаємодія як прояв інформаційної функції. *Науковий вісник Ужгородського національного університету*. *Право.* 2014. № 25. С. 154–158.

266. Дубняк М. В. Правове регулювання інформаційної взаємодії суб'єктів громадської експертизи в місцевому самоврядуванні. *Порівняльно-аналітичне право*. 2016. № 6. С. 173–177.

267. Олійник І. Л. Організаційно-правові засади взаємодії міліції (поліції) країн – учасниць СНД у боротьбі з правопорушеннями : автореф. дис. канд. юрид. наук. Ірпінь, 2005. 26 с.

268. Кушнір І. П. Інформаційна взаємодія як основа забезпечення спільних дій правоохоронних органів та військових формувань в охороні державного кордону. П'ята Всеукраїнська науково-практична конференція *«Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи*. 2019. Одеса. С. 186–187.

269. Про затвердження Порядку обміну інформаційно-аналітичними матеріалами між суб'єктами інтегрованого управ-ліньня кордонами : наказ Адміністрації ДПСУ, МВС України, МЗС України, Мінінфраструктури, МФ України, СБ України від 01.09.2015 р. № 1050/254/341/749/562. *Офіційний вісник України*. 2015. № 77. Ст. 2560.

270. В Адміністрації відбулось чергове засідання Віртуального контактного аналітичного центру суб'єктів інтегрованого управління кордонами. URL: https://dpsu.gov.ua/ua/news/v-administracii-vidbulos-chergove-zasidannya-virtualnogo-kontaktnogo-analitichnogo-centru-subktiv-integrovanogo-upravlinnya-kordonami/ (дата звернення: 23.07.2019).

271. Про затвердження Методики аналізу ризиків з метою протидії нелегальній міграції : наказ МВС України, МЗС України, Мінсоцполітики,

МОН України, СЗР України, СБ України від 29.04.2015 р. № 494/132/467/497/141/281. *Офіційний вісник України*. 2015. № 40. Ст. 352.

272. Протокол між Адміністрацією Державної прикордонної служби України і Департаментом Прикордонної поліції Міністерства внутрішніх справ Республіки Молдова про обмін статистичною та аналітичною інформацією від 20.11.2014 р. URL: https://zakon. rada.gov.ua/laws/show/498_163 (дата звернення: 22.07.2019).

273. Протокол між Адміністрацією Державної прикордонної служби України і Державним прикордонним комітетом Республіки Білорусь про порядок обміну інформацією про обстановку на державних кордонах України і Республіки Білорусь від 18.06.2013 р. URL: https://zakon.rada.gov.ua/laws/show/112_183 (дата звернення: 22.07.2019).

274. Протокол між Адміністрацією Державної прикордонної служби України та Державним прикордонним комітетом Республіки Білорусь про пілотний контактний пункт «Житомир – Пінськ» від 14.12.2016 р. URL: https://zakon.rada.gov.ua/ laws/show/112_201 (дата звернення: 22.07.2019.).

275. Положення про консультаційний пункт Державної прикордонної служби України : наказ МВС України від 04.08.2016 р. № 752. *Офіційний вісник України*. 2016. № 78. Ст. 2624.

276. Калюжний Р. А., Кушнір І. П. Правове забезпечення взаємодії публічної адміністрації у прикордонній сфері : монографія. Київ : «МП Леся», 2015. 224 с.

277. Про затвердження Порядку здійснення координації діяльності органів виконавчої влади та органів місцевого самоврядування з питань додержання режимів на державному кордоні : постанова Кабінету Міністрів України від 18.01.1999 р. № 48. *Офіційний вісник України*. 1999. № 3. С. 14.

278. Про затвердження Порядку взаємодії інформаційних систем Державної фіскальної служби України та Державної прикордонної служби України щодо обміну інформацією, необхідною для забезпечення контролю при переміщенні осіб та транспортних засобів через державний (митний) кордон України та

адміністративний кордон вільної економічної зони «Крим» : наказ МФ України, МВС України від 07.09.2017 № 746/759. *Офіційний вісник України*. 2017. № 85. Ст. 2585.

279. Про затвердження Інструкції про порядок організації обміну інформацією між структурними підрозділами МВС, Служби безпеки України, Державної податкової адміністрації України, Державної прикордонної служби України, Держмитслужби в діяльності з виявлення та припинення корупційних діянь в правоохоронних органах : наказ МВС України, СБ України, ДПА України, Адміністрації ДПСУ, ДМСУ від 23.03.2009 р. № 124/936/139/ 199/250. URL: https://zakon.rada. gov.ua/laws/ show/ z0670-09 (дата звернення: 24.07.2019).

280. Рівень довіри до суспільних інститутів та електоральні орієнтації громадян України. URL: http://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/riven-doviry-do-suspilnykh-instytutiv-ta-elektoralni-oriientatsii-gromadian-ukrainy (дата звернення: 16.12.2019).

281. Оцінка громадянами ситуації в країні та діяльності влади. URL: http://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/otsinka-gromadianamy-sytuatsii-v-kraini-ta-diialnosti-vlady (дата звернення: 28.12.2019).

282. Прес-конференція «Стратегічні комунікації – складова ефективного реформування правоохоронної системи». URL: https://dpsu.gov.ua/ua/news/golova-derzhprikordonsluzhbi-mi-rozumimo-neobhidnist-donositi-do-suspilstva-pravdu/ (дата звернення: 28.12.2019).

283. Про вільний доступ і порядок обміну відкритою науково-технічною інформацією держав – учасниць СНД : Міжнародна угода від 11.09.1998 р. URL: https://zakon.rada.gov.ua/laws/show/ru/997_889/ed19990401/find?text=%F1%F4%E5%F0%E0+%28%F1%F0%E5%E4%E0%29+%97+%F1%F4%E5%F0%E0 (дата звернення: 05.11.2019).

284. Словник української мови : в 11 т. Т 9, 1978. С. 876. URL: http://sum.in.ua/s/sfera (дата звернення: 09.05.2019).

285. Концепція інформаційної безпеки. URL: http://mip.gov.ua/files/banners/Final%20%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%20

%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D1%96%D1%97%20(%D0%A2%D0%B5%D0%BA%D1%81%D1%82)%20-%2030.09.15.pdf (дата звернення: 09.05.2019).

286. Проект Указу Президента України «Про затвердження Стратегії розвитку інформаційного простору України на період до 2020 року». URL: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113102&cat_id=61025 (дата звернення: 11.06.2018).

287. Пазюк А. В. Інформаційна сфера як предмет міжнародного права: теоретичні підходи. URL: https://www.academia.edu/5313495/%D0%86%D0%9D%D0%A4%D0%9E%D0%A0%D0%9C%D0%90%D0%A6%D0%86%D0%99%D0%9D%D0%90_%D0%A1%D0%A4%D0%95%D0%A0%D0%90_%D0%AF%D0%9A_%D0%9F%D0%A0%D0%95%D0%94%D0%9C%D0%95%D0%A2_%D0%9C%D0%86%D0%96%D0%9D%D0%90%D0%A0%D0%9E%D0%94%D0%9D%D0%9E%D0%93%D0%9E_%D0%9F%D0%A0%D0%90%D0%92%D0%90_%D0%A2%D0%95%D0%9E%D0%A0%D0%95%D0%A2%D0%98%D0%A7%D0%9D%D0%86_%D0%9F%D0%86%D0%94%D0%A5%D0%9E%D0%94%D0%98 (дата звернення: 03.12.2019).

288. Бєляков К. І. Інформатизація в Україні: проблеми організаційно-правового та наукового забезпечення: монографія. Київ: КВІЦ, 2008. 576 с.

289. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика: монографія. Київ: Едельвейс, 2014. 434 с.

290. Заярний О. А. Інформаційна сфера як об’єкт адміністративно-правової охорони: деякі доктринальні та нормативні аспекти. *The Journal of Eastern European Law / Журнал східноєвропейського права*. 2016. № 23. С. 18–31.

291. Соснін О. Інформаційна сфера в реалізації інтересів інноваційного розвитку нації. *Віче*. 2011. № 15–16. С. 17–21.

292. Словник іншомовних слів Мельничука. URL: http://slovopedia.org.ua/42/53402/284274.html (дата звернення: 28.12.2019).

293. Онуфрієнко Г., Черневич А. Термін комунікація в понятєвому вимірі й лінгвістичному контексті. *Вісник Нац. ун-ту «Львівська політехніка». Проблеми*

української термінології. 2010. № 675. С. 154–160. URL: http://www.nbuv.gov.ua/portal/natural/Vnulp/ Ukr_term/ 2010_675/34.pdf. (дата звернення: 29.11.2019).

294. Інформаційна складова державної політики та управління : монографія / Соловйов С. Г, та ін. ; за заг. ред. Грицяк Н. В. ; Нац. акад. держ. упр. при Президентові України. Київ : К.І.С., 2015. 320 с.

295. Мельник Р. С., Бевзенко В. М. Загальне адміністративне право : навчальний посібник / за заг. ред. Р. С. Мельника. Київ : Ваіте, 2014. 376 с.

296. Кушнір І. П. Інформаційна відкритість у діяльності Державної прикордонної служби України. *Правова позиція*. 2019. № 1 (22). С. 30–36.

297. Recommendations for greater transparency of Frontex activities Arne Semsrott and Luisa Izuzquiza 26 November 2018. URL: https://ec.europa.eu/info/law/better-regulation/feedback/15674/attachment/090166e5bf82536a_en (дата звернення: 07.10.2019).

298. Гудима Н. В. Принципи відкритості та прозорості в діяльності органів державного управління України : дис... канд. наук з держ. упр. : 25.00.01. Київ, 2008. 204 с.

299. Крук Н. В. Інформаційна відкритість влади як принцип діяльності органів державної влади : автореф. дис. ... канд. політ. наук : 23.00.02. Одеса, 2014. 18 с.

300. Словник української мови : в 11 томах. Том 1, 1970. 597 с. URL: http://sum.in.ua/s/vidkrytyj (дата звернення: 08.10.2019).

301. Енциклопедичний словник з державного управління / Сурмін Ю. П., Бакуменко В. Д., Михненко А. М., Ковбасюк Ю. В. Київ : НАДУ, 2010. 820 с.

302. Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31.5.2001, p. 43–48 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV). URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32 001R1049 (дата звернення: 12.11.2019).

303. Recommendations for greater transparency of Frontex activities Arne Semsrott and Luisa Izuzquiza 26 November 2018. URL: https://ec. europa.eu/info/law/better-regulation/feedback/15674/attachment/090166e5bf82536a_en (дата звернення: 04.11.2019).

304. Словник бюджетної термінології. URL: http://slovopedia.org.ua/50/53410/362635.html (дата звернення: 12.11.2019).

305. Арбузов С. Г., Колобов Ю. В., Міщенко В. І., Науменкова С. В. Банківська енциклопедія. Київ : Центр наукових досліджень Національного банку України : Знання, 2011. 504 с.

306. Наливайко Л., Романов М. Поняття, ознаки та значення транспарентності в контексті євроінтеграції. *National law journal: theory and practice.* 2016. № 4/1 (36). С. 158–163.

307. Афонін Е. А., Суший О. В. Транспарентність влади в контексті європейської інтеграції України : консп. лекц. до короткотерм. семін. в системі підвищення кваліфікації кадрів. Київ : НАДУ, 2010. 48 с. URL: http://lib.rada.gov.ua/static/about/text/transparentnist.pdf (дата звернення: 16.11.2019).

308. Тихомирова Є. Б. Транспарентність і відкритість діяльності влади та шляхи їх забезпечення в Україні. *Наукові записки*. Т. 20. Політичні науки. 2002. С. 39–43.

309. Пашковська М. Поняття транспарентності в сучасній науці «державне управління». *Ефективність державного управління*. 2013. Вип. 34. С. 135–143.

310. Кудіна О. А. Транспарентність влади в Україні: проблеми становлення та чинники забезпечення. *Вісник Дніпропетровського університету*. *Філософія. Соціологія. Політологія*. 2013. Т. 21. Вип. 23(4). С. 33–38.

311. Public Access to Documents. URL: https://frontex.europa.eu/ contact/public-access-to-documents/ (дата звернення: 19.11.2019).

312. Інформаційна відкритість української влади. Аналітична доповідь / О. В. Литвиненко та ін. Київ : НІСД, 2002. 59 с. URL: http://old.niss.gov.ua/Table/opengov/a_dopovid.htm (дата звернення: 20.05.2019).

313. Мосора Л. Особливості забезпечення відкритості органів місцевого самоврядування об'єднаних територіальних громад. С. 263–266. URL: dspace.tneu.edu.ua/bitstream/316497/24840/1/263-266.PDF (дата звернення: 24.05.2019).

314. П'ятіна О. Інформаційна відкритість органів державної влади як складова формування їх корпоративного іміджу. URL: http://archive.nbuv.gov.ua/portal/soc_gum/Dums/2011_2/11pasfki.pdf (дата звернення: 20.05.2019).

315. Юридична енциклопедія : в 6 т. / за ред. Ю. С. Шемшученко та ін. Київ : Укр. енцикл., 1999. Т. 1. : А–Г. 672 с. URL: https://cyclop.com.ua/content/view/1019/58/1/2/#2623 (дата звернення: 20.05.2019).

316. Словник української мови : в 11 томах. Т 2, 1971. С. 80. URL: http://sum.in.ua/s/ghlasnyj (дата звернення: 18.05.2019).

317. Короткий словник політологічних термінів. Гласність. URL: http://politics.ellib.org.ua/encyclopedia-term-293.html (дата звернення: 18.05.2019).

318. Transparency in Three Dimensions Frederick Schauer / 2011 U. Ill. L. Rev. P 1339–1358. URL: https://illinoislawreview.org/wp-content/ilr-content/articles/2011/4/Schauer.pdf (дата звернення: 20.11.2019).

319. Ляшук Р. М. Адміністративно-правове забезпечення діяльності відділів прикордонної служби Державної прикордонної служби України : дис. … д-ра юрид. наук. 12.00.07. Київ, 2016. 541 с.

320. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 р. № 2135-XII. Відомості Верховної Ради України. 1992. № 22. Ст. 303.

321. Інформаційна відкритість органів державної влади України / за заг. ред. М. Лациби. Київ: Український незалежний центр політичних досліджень, 2005. 156 с.

322. Захарчук В. І., Свідерська І. О. Світова практика діяльності прес-служб органів охорони державного кордону. Міжнародний досвід навчального процесу у Сполучених Штатах Америки, країнах Європейського Союзу та Східного партнерства : правовий аспект : тези внутрішньовузівської методичної

конференції (14 червня 2017 р.). Хмельницький : Вид-во НАДПСУ, 2017. С. 41–42.

323. Методичні рекомендації щодо формування єдиних підходів до інформування громадськості у соціальних мережах про діяльність Державної прикордонної служби України : наказ Голови ДПСУ від 31.05.2017 р. Окреме видання.

324. Державна прикордонна служба України. URL: https:// www.facebook.com/DPSUkraine/ (дата звернення: 08.02.2020).

325. Radio.Kordon. URL: https://www.facebook.com/RadioKordon (дата звернення: 08.02.2020).

326. Пилипчук В. Г., Брижко В. М. Реформування і розвиток системи захисту персональних даних в Україні. *Інформація і право.* 2017. № 3(22). С. 5–21.

327. Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016. URL : https://gdpr-info.eu/art-4-gdpr/(дата звернення: 20.10.2019).

328. Брижко В. М. Сучасні основи захисту персональних даних в європейських правових актах. *Інформація і право*. 2016. № 3(18). С. 45–57.

329. Словник української мови : в 11 томах. Т.7. 1976. С. 568. URL: http://sum.in.ua/s/pryvatnyj (дата звернення: 30.10.2019).

330. Кардаш А. В. Конституційно-правовий захист інформації про особу (порівняльно-правовий аспект). : дис. канд.. юрид. наук : 12.00.02. Харків, 2019. 223 с.

331. Право на приватність. Українська Гельсінська спілка з прав людини. URL: https://helsinki.org.ua/articles/pravo-na-pryvatnist/ (дата звернення: 30.10.2019).

332. В. Я. Тацій та ін. Конституція України. Науково-практичний коментар / В. Я. Тацій та ін. Нац.акад.прав.наук України. 2-ге вид., переробл. і допов. Харків: Право, 2012. 1128 с.

333. Пилипчук В. Г. Проблеми захисту приватності, індивідуальних свобод та безпеки людини в інформаційному суспільстві. Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 18. Право. 2017. № 32. С. 106–118.

334. Типовий порядок обробки персональних даних : наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n11 (дата звернення: 19.10.2019).

335. Про захист персональних даних : Закону України від 01.06.2010 р. № 2297-VI. *Урядовий кур'єр*. 2010. № 122.

336. Data protection notice for Frontex application for return (FAR). URL: http://frontex.europa.eu/assets/Data_Protection/Data_Protection_Notice_Returns.pdf (дата звернення: 20.10.2019).

337. Про затвердження Інструкції про порядок фіксації біометричних даних (параметрів) іноземців та осіб без громадянства посадовими особами Державної міграційної служби України, її територіальних органів і територіальних підрозділів : наказ МВС України від 23.11.2018 р. № 944. *Офіційний вісник України*. 2018. № 3. Ст. 82.

338. Філіппов С. О. Інформаційне забезпечення протидії транскордонній злочинності. *Visegrad Journal on Human Rights.* 2018. № 4(2). С. 107–112.

339. Філіппов С. О. Біометричні технології: значення для протидії транскордонній злочинності. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2018. Випуск 2. URL: https://nadpsu.edu.ua/wp-content/uploads/2018/11/visnik_2_2018_ur.pdf (дата звернення: 04.12.2019).

340. Царенко О. М., Царенко С. І. Перетин державного кордону України із Російською Федерацією та Республікою Білорусь громадянами України. *Вісник Національної академії Державної прикордонної служби України*. *Юридичні науки*. 2018. Вип. 4. URL: http://nbuv.gov.ua/UJRN/vnadpcurn_2018_4_10 (дата звернення: 04.12.2019).

341. Data Protection. URL: https://frontex.europa.eu/about-frontex/data-protection/ (дата звернення: 19.10.2019).

342. Processing personal data for risk analysis (PeDRA) – Privacy statement URL: https://frontex.europa.eu/assets/Data_Protection/Privacy_Statement.pdf, (дата звернення: 13.10.2019).

343. Апетик А. Інформаційна безпека: історії успішних рішень Естонії. URL: https://ecpl.com.ua/news/pro-estoniiu-dydzhytalizatsiiu-ta-personal-ni-dani/ (дата звернення: 15.01.2020).

344. Interoperability services. URL: https://e-estonia.com/solutions/interoperability-services/x-road/ (дата звернення: 15.01.2020).

345. Кушнір І. П. Реалізація права на звернення громадян у Державній прикордонній службі України.. *Visegrad Journal on Human Rights*. 2018. 4 (volume 2). С. 56–60.

346. Соболь В. Актуальні проблеми забезпечення реалізації права громадян на звернення до органів влади. *Збірник наукових праць Національної академії державного управління при Президентові України*. 2013. Вип. 1. С. 184–195.

347. Про звернення громадян : Закон України від 02.10.1996 р. № 393/96-ВР. *Відомості Верховної Ради України*. 1996. № 47. Ст. 256.

348. Рішення Колегії ДПСУ № 7 від 19.12.2019 р. Окреме видання.

349. Графік особистого прийому громадян, осіб для надання безоплатної первинної правової допомоги та запитувачів на отримання публічної інформації керівництвом та керівниками структурних підрозділів Адміністрації Державної прикордонної служби України : наказ Адміністрації ДПСУ від 24.01.2018 р № 50 АГ. URL: https://dpsu.gov.ua/ua/gromadska-priymalnya/ (дата звернення: 26.04.2018).

350. Інструкція з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об’єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, в засобах

масової інформації : постанова Кабінету Міністрів України від 14.04.1997 р. № 348. *Офіційний вісник України*. 1997. № 16 (дата звернення: 09.10.2019).

351. Гонюкова Л. В. Основні напрями співпраці влади та громади і необхідні для цього умови. URL: http://www.dy.nayka.com.ua/?op=1&z=819 (дата звернення: 30.09.2019).

352. Кушнір І. П., Новодранов Р. С. Проблеми та перспективи розвитку консультаційної роботи Контактного центру Державної прикордонної служби України. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2019. Вип. 4. URL: http://periodica.nadpsu.edu.ua/index.php/legal/article/view/316/317 (дата звернення: 25.05.2020).

353. Про затвердження Положення про Національну систему опрацювання звернень до органів виконавчої влади та Типового положення про контактний центр Автономної Республіки Крим, області, міст Києва і Севастополя : постанова Кабінету Міністрів України від 18.01.2012 р. № 21. URL: https://zakon.rada.gov.ua/laws/show/21-2012-%D0%BF (дата звернення: 07.09.2019).

354. Про правовий статус іноземців та осіб без громадянства : Закон України від 22.09.2011. № 3773-VI. URL: https://zakon.rada.gov.ua/laws/show/3773-17 (дата звернення: 28.09.2019).

355. Деякі питання документування управлінської діяльності : постанова Кабінету Міністрів України від 17.01.2018 р. № 55. URL: https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF (дата звернення: 23.11.2018).

356. Про затвердження Інструкції з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, в засобах масової інформації : постанова Кабінету Міністрів України від 14.04.1997 р. № 348. URL: https://zakon.rada.gov.ua/laws/show/348-97-%D0%BF (дата звернення: 25.11.2018).

357. Про взаємодію органів виконавчої влади, Секретаріату Кабінету Міністрів України та державної установи «Урядовий контактний центр» :

постанова Кабінету Міністрів України від 12.08.2009 р. № 898. URL: https://zakon1.rada.gov.ua/laws/show/898-2009-%D0%BF (дата звернення: 17.09.2019).

358. Стан роботи зі зверненнями громадян у Державній прикордонній службі України у 2015 році. Окреме видання. URL: https://dpsu.gov.ua/ua/stan-roboti-zi-zvernennyami-gromadyan-u-2015-roci/ (дата звернення: 29.10.2017).

359. Стан роботи зі зверненнями громадян, що надійшли до органів управління Державної прикордонної служби України у першому півріччі 2020 році. URL: https://dpsu.gov.ua/ua/stan-roboti-zi-zvernennyami-gromadyan-u-2018-roci/ (дата звернення: 23.07.2020).

360. Державна прикордонна служба України. Публічна інформація. Звіти. URL: https://dpsu.gov.ua/ua/zviti/ (дата звернення: 23.02.2020).

361. Коновалов Л. В. Інформаційна потреба: сутність та дефініції. Місце і роль бібліотек у формуванні національного інформаційного простору : матеріали міжнародної наукової конференції (Київ, 21–23 жовтня 2014 р.). 2014. URL: http://confe rence.nbuv.gov.ua/report/view/id/350 (дата звернення: 04.05.2019).

362. Аблякімова Е. Е. Адміністративно-правове забезпечення доступу до публічної інформації : автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2014. 19 с.

363. Кушнір І. П. Особливості правових відносини щодо забезпечення запиту на публічну інформацію, розпорядником якої є Державна прикордонна служба України. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2018. Вип. 4. URL: https://nadpsu.edu.ua/wp-content/uploads/2019/02/visnuk_4_2019_ur.pdf.

364. Державна прикордонна служба України. Подання запиту на інформацію. URL: https://dpsu.gov.ua/ua/Podannya-zapitu-na-informaciyu/ (дата звернення: 09.12.2018).

365. Державна прикордонна служба України. Заява стосовно перетинання особою державного кордону. URL: http://dpsu.gov.ua/ua/Zayava-stosovno-peretinannya-osoboyu-derzhavnogo-kordonu/ (дата звернення: 10.12.2018).

366. Науково-практичний коментар до Закону України «Про доступ до публічної інформації» / Р. Головенко та ін. ; за ред. Д. Котляр. Київ. 2012. 335 с.

367. Кушнір І. П. Інформаційні загрози в діяльності Державної прикордонної служби України. *Підприємництво, господарство і право*. 2019. № 7. С. 147–150.

368. Про Концепцію розвитку Державної прикордонної служби України на період до 2015 року : Указ Президента України від 19.06.2006 р. № 546/2006. *Офіційний вісник України*. 2006. № 25. Ст. 1807.

369. Про затвердження Інструкції з проведення аналізу ризиків у Державній прикордонній службі України : наказ Міністерства внутрішніх справ України 11.12.2017 р. № 1007. URL: https://zakon.rada.gov.ua/laws/show/z0091-18 (дата звернення: 04.09.2018).

370. Про затвердження Порядку роботи органів управління Державної прикордонної служби України з підготовки до оперативно-службової діяльності в наступному календарному році або іншому періоді : наказ Міністерства внутрішніх справ України від 26.04.2018 р. № 350. *Офіційний вісник України*. 2018. № 49, Ст. 1726.

371. Золотар О. О., Трубін І. О. Класифікація загроз інформаційній безпеці. *Інформація і право*. 2013. № 3. С. 105–112.

372. Про основи національної безпеки України : Закон України від 19.06.2003 р. *Відомості Верховної Ради України*. 2003. № 39. Ст. 351.

373. Стратегія національної безпеки України : Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#n7 (дата звернення: 11.10.2020).

374. Рекомендації парламентських слухань на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні» : постанова Верховної Ради України від 03.07.2014 р. № 1565-VII. *Відомості Верховної Ради України.* 2014. № 33. Ст. 1163.

375. Ліпкан В. А., Залізняк В. А. Систематизація інформаційного законодавства України : монографія / за заг. ред. В. А. Ліпкана. Київ : ФОП О. С. Ліпкан, 2012. 332 с.

376. Сопілко І. М. Становлення інформаційного суспільства та інформаційні загрози в мережі Інтернет. *Юридичний вісник «Повітряне і космічне право»*. Київ : НАУ, 2017. № 3 (44) С. 61–69.

377. Швець М., Брижко В. До питання систематизації інформаційного законодавства України. *Правова інформатика.* 2007. № 4(16). С. 5–7.

378. Новицький А. М., Касянюк Т. С. Інформаційне законодавство України: окремі питання систематизації. *Правова інформатика*, 2009. № 2(22). С. 17–24.

379. Словник української мови : в 11 томах. Том 5, 1974. С. 246. URL: http://sum.in.ua/s/nebezpeka (дата звернення: 16.07.2018).

380. Ліпкан В. А. Національна безпека України. URL: //www.pidruchniki.ws/15341220/politologiya/ponyattya_vidi_zagroz_natsionalnim_interesam_natsionalniy_bezpetsi_informatsiyniy_sferi (дата звернення: 11.09.2017).

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

382. Золотар О. О. Правові основи інформаційної безпеки людини : дис. … д-ра. юрид. наук : 12.00.07. Київ, 2018. 479 с.

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

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

385. Савінова Н. А. Кримінально-правова політика забезпечення розвитку інформаційного суспільства в України : дис…д-ра юрид. наук. : 12.00.08. Львів. 2013. 510 с.

386. Литвиненко О. В. Проблема інформаційної безпеки в контексті міграційних процесів. URL: http://nbuv.gov.ua/UJRN/Ukralm_2012_7_35. (дата звернення: 09.05.2019).

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

388. Кузьменко Б. В., Чайковська О. А. Захист інформації : навч. посіб. Ч. 2. Київ : Видавничий відділ КНУКіМ, 2009. 69 с.

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

390. Євдоченко Л. О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації : автореф. дис. .. канд. наук з держ. упр. : 25.00.01. Львів, 2011. 24 с.

391. Погребняк А. В. Технології комп'ютерної безпеки : монографія. Рівне : МЕГУ, 2011. 17 с.

392. Цевельов О. Є. Реальні та потенційні загрози національній безпеці України у сфері безпеки державного кордону. *Публічне управління: ціннісні орієнтири, стандарти якості та оцінка ефективності* : матеріали щоріч. Всеукр наук.-практ. конф. за міжнар. участю. (Київ, 26 травня 2017 р.) : у 5 ч. / за заг. ред. В. С. Куйбіди, А. П. Савкова, С. В. Загороднюка. Київ : НАДУ, 2017. Ч. 1. : Оцінка якості державної політики. С. 161–163.

393. Розкрита провокація спецслужб РФ проти українських прикордонників – ІС. URL: https://sprotyv.info/news/raskryta-provokaciya-specsluzhb-rf-protiv-ukrainskih-pogranichnikov-is (Дата звернення: 29.07.2020).

394. Тихомиров О. О. Цивільно-правова відповідальність за інформаційні правопорушення: загальнотеоретичні аспекти. *Порівняльно-аналітичне право*. 2015. № 1. С. 37–40.

395. Кушнір І. П. Питання кримінально-правової охорони інформації у функціонуванні Державної прикордонної служби України. *Актуальні проблеми*

кримінального права, процесу, криміналістики та оперативно-розшукової діяльності : тези II Всеукраїнської науково-практичної конференції (Хмельницький, 2 березня 2018 р.). Хмельницький: Видавництво НАДПСУ, 2018. С. 169–172.

396. Вирок у справі № 127/19700/15-к провадження № 1-кп/127/1180/15 Вінницького міського суду Вінницької області від 18.09.2015. URL: http://www.reyestr.court.gov.ua/Review/50803207 (дата звернення: 12.01.2020).

397. Дадерко Л. Ф. Кримінальна відповідальність за розголошення державної таємниці. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція.* 2013. № 6–2. Т. 2. С. 82–85.

398. Вирок у справі № 760/8755/15-к провадження № 1-кп/760/655/15 Солом'янського районного суду м. Києва від 18.05.2015 р. URL: http://www.reyestr.court.gov.ua/Review/44222629. (дата звернення: 12.01.2020).

399. Кушнір І., Степанова Ю. Інформаційна безпека держави у прикордонній сфері як об'єкт державної зради. *National law journal: theory and practice.* 2018. № 4 (32). Т. 1. С. 123–126.

400. Семенюк О. О. Перспективи розвитку кримінального законодавства у сфері охорони інформації з обмеженим доступом. *Юридична Україна*. 2017. № 1. С. 44–56.

401. Правдюк С. А. Комп'ютерні правопорушення та інформаційні правопорушення: аспекти співвідношення. *Науковий вісник Національного університету біоресурсів і природокористування України*. 2013. Вип. 182. Ч. 3.

402. На Харківщині поліцейський продавав в РФ інформацію з обмеженим доступом. URL: https://www.unian.ua/society/10809143-na-harkivshchini-policeyskiy-prodavav-v-rf-informaciyu-z-obmezhenim-dostupom.html (дата звернення: 21.12.2019).

403. Тугарова О. К. Кримінально-правове забезпечення охорони інформаційних відносин. *Науковий вісник Херсонського державного університету. Юридичні науки*. 2015. Вип. 4. Т. 3. С. 61–66.

404. Савінова Н. А. Удосконалення кримінально-правового забезпечення розвитку інформаційного суспільства в Україні. Правова інформатика. 2012. № 2(34). с. 60–65.

405. Кушнір І. П. Кримінально-правове забезпечення охорони інформаційних відносин у прикордонній сфері. *Питання боротьби зі злочинністю.* 2018. Вип. 36. 186 с. С. 82–93.

406. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави : монографія / за заг. ред. Р. А. Калюжного. Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.

407. Максименко Ю. Є. Інформаційні правопорушення: поняття та ознаки. *Глобальна організація союзницького лідерства*. 2014. URL: http://goal-int.org/informacijni-pravoporushennya-ponyattya-ta-oznaki/ (дата звернення: 21.01.2019).

408. Коваленко Л. П. Деякі питання щодо правопорушень в інформаційній сфері. *Форум права*. 2013. № 4. С. 158–167.

409. Стоєцький О. В. Адміністративна відповідальність за порушення у сфері інформаційної безпеки України : автореф. дис. … канд. юрид. наук. : 12.00.07. Київ, 2013. 20 с.

410. Шапка А. В. Адміністративно-правові засади забезпечення інформаційної безпеки в діяльності органів Державної фіскальної служби України : дис. канд. юрид. наук : 12.00.07. Ірпінь, 2016. 205 с.

411. Кодекс України про адміністративні правопорушення : Закон України від 07.12.1984. № 8073-X. URL: https://zakon.rada.gov.ua/laws/show/80731-10 (дата звернення: 03.02.2019).

412. Благодарний А. М. Особливості адміністративної відповідальності за правопорушення в інформаційній сфері. *Підприємництво, господарство і право*. 2009. № 11. С. 123–126.

413. Мота А. Ф. Адміністративна відповідальність військовослужбовців за законодавством України : автореф. дис... канд. юрид. наук : 12.00.07. Київ, 2003. 18 с.

414. Баскаков В. Ю. , Стоєцький О. В. Тенденції адміністративної відповідальності у сфері інформаційної безпеки. URL: http://goal-int.org/tendencii-administrativnoi-vidpovidalnosti-u-sferi-informacijnoi-bezpeki/ (дата звернення: 01.02.2019).

415. Справа про адмінправопорушення № 297/1691/16-п. Незаконне використання інформації, що стала відома особі у зв’язку з виконанням службових повноважень. URL: http://www.reyestr.court.gov.ua/Review/62670316 (дата звернення: 16.03.2019).

416. Справа про адмінправопорушення №: 503/2299/15-п. Незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових повноважень. URL: http://www.reyestr.court.gov.ua/Review/57123283 (дата звернення: 16.03.2019).

417. Кушнір І. П. Адміністративна відповідальність за порушення законодавства про інформацію у прикордонній сфері. *Право і інформація.* 2019. № 1(28). С. 45–51.

418. Ліпкан В. А., Максименко Ю. Є. Засади розвитку інформаційної деліктології. *Право України*. 2013. № 10. С. 249–256. URL: http://goal-int.org/zasadi-rozvitku-informacijnoi-deliktologii/ (дата звернення: 15.03.2019).

419. Заярний О. А. Класифікація адміністративних інформаційних правопорушень як метод наукового дослідження адміністративної деліктності та інструмент удосконалення адміністративно-деліктного законодавства. *Науково-практичний журнал Київського національного університету імені Тараса Шевченка*. 2014. № 4 (10) URL: http://applaw.knu.ua/index.php/arkhiv-nomeriv/4-10-2015/item/ 354-klasyfikatsiya-administratyvnykh-infor matsiynykh-pravoporushen-yak-metod-naukovoho-doslidzhennya-administratyvnoyi-deliktnosti-ta-instrument-udoskonalennya-administratyvno-deliktnoho-zakonodavstva-zaiarnyi-o-a (дата звернення: 11.04.2019).

420. Писаренко Г. М. Підстави юридичної відповідальності в інформаційній сфері. *Держава та регіони*. *Право.* 2017. № 2 (56). С. 14–18.

421. Кодекс Республики Беларусь об административных правонарушениях : Закон Республики Белорусь від 21.04.2003 г. № 194-З. URL: http://pravo.by/document/?guid=3871&p0=hk030 0194 (дата звернення: 29.01.2019).

422. Кодекс Российской Федерации об административных правонарушениях : Закон Российской Федерации от 2012.2001 г. № 195-ФЗ. URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102074277 (дата звернення: 29.01.2019).

423. Кодекс о правонарушениях : Закон Республики Молдова от 24.10.2008 г. № 218-XVI. URL: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=369412&lang=2 (дата звернення: 29.01.2019).

424. Тихомиров О. О., Тугарова О. К. Юридична відповідальність за правопорушення в інформаційній сфері : навч. посіб. Київ : Нац. акад. СБУ, 2015. 172 с.

425. Передерій О. С. Дисциплінарна відповідальність як складова правового статусу поліції країн континентальної правової сім'ї (загальнотеоретична характеристика на прикладі Німеччини). *Вісник Харківського національного університету імені В. Н. Каразіна: Право.* 2008. № 1. С. 137–141.

426. Пахомова І. А. Юридична відповідальність державних службовців за правопорушення у сфері обігу інформації. *Вісник Харківського національного університету імені В. Н. Каразіна*. *Право*. 2016. Вип 21. С. 85–89.

427. Про Дисциплінарний статут Збройних Сил України : Закон України від 24.03.1999 р. № 551-XIV. URL: https://zakon.rada.gov.ua/laws/show/551-14 (дата звернення: 12.02.2019).

428. Кушнір І. П., Царенко С. І., Царенко О. М. Особливості застосування дисциплінарної відповідальності за порушення інформаційного законодавства у діяльності Державної прикордонної служби України. *Актуальні проблеми вітчизняної юриспруденції.* 2019. № 6. С. 80–84.

429. Положення про орган охорони державного кордону Державної прикордонної служби України : наказ Міністрества внутрішніх справ України від 30.11.2018 р. № 971. URL: https://zakon.rada.gov.ua/laws/show/z1468-18 (дата звернення: 01.02.2019).

430. Кохановська О. В. Інформація як нематеріальне благо та захист інформаційних прав згідно з Цивільним кодексом України. *Вісник Верховного Суду України*. 2005. № 11 (63). С. 37–44.

431. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобан та ін.; за заг. ред.. проф. К. І. Бєлякова. Київ: КВІЦ, 2019. 346 с.

432. Писаренко Г. М. Юридична відповідальність в інформаційній сфері: окремі аспекти становлення. *Науковий вісник Ужгородського національного університету*. *Право*. 2016. Вип. 36(2). С. 55–58.

433. Тихомиров О. О. Інформаційні правопорушення: теоретико-правова концепція. *Інформаційна безпека людини, суспільства, держави*. 2015. № 1 (17). С. 38–47. URL: http://tihoma-law.at.ua/publ/teorija_derzhavi_i_prava/informacijni_pravoporushennja_teoretiko_pravova_koncepcija/3-1-0-38 (дата звернення: 04.26.2019).

434. Селезньова О. М. Теоретико-методологічне трактування окремих засадничих категорій інформаційного права. *ІТ-право: проблеми і перспективи розвитку в Україні* : міжнародна наукова конференція (круглий стіл) (18 листопада 2016 р.). Львів. URL: http://aphd.ua/publication-164/ (дата звернення: 23.05.2018).

435. Пам’ятка щодо забезпечення інформаційної безпеки при роботі в мережі Інтернет : Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України. Київ. 2019. Окреме видання.

436. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : дис.. канд. юрид. наук. : 12.00.07. Київ, 2007. 188 с.

437. Кушнір І. П. Організаційно-правові питання забезпечення захисту інформації в інформаційних системах Державної прикордонної служби України. *Прикарпатський юридичний вісник*. 2018. № 3. С. 81–84.

438. Ящук Д. Ю., Савчук В. В. Криптографічний захист інформації на основі удосконаленого алгоритму clefia. *Проблеми кібербезпеки інформаційно-телекомунікаційних систем* : збірник матеріалів доповідей та тез науково-технічної конференції (м. Київ, 10–11 березня 2016 р.), Київський національний університет імені Тараса Шевченка. Київ. С. 96–98.

439. Боровик О. В., Боровик Л. В., Трасковецька Л. М. Дослідження характеристик ефективності функціонування інформаційно-телекомунікаційної системи «Гарт-1» на основі застосування методів імітаційного моделювання. *Збірник наукових праць Національної академії Державної прикордонної служби України*. *Військові та технічні науки*. 2015. № 1. С. 167–182.

440. Основні напрями діяльності та подальшого розвитку Державної прикордонної служби України у 2018 році. Прикордонник України. 2018. № 3–4 (5593-5594). С. 13–15.

441. Коваленко Н. В. Про правовий режим кібербезпеки в Україні. Актуальні проблеми вітчизняної юриспруденції. 2016. № 3. С. 96–100.

442. Кіберварта «невидимі будні». Кордон. 2018. № 7. С. 26–29.

443. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

444. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. Вип. 1. С. 312–320.

445. Основні напрями діяльності та подальшого розвитку Державної прикордонної служби України у 2019 році. Окреме видання. URL: dpsu.gov.ua/upload/Haprjami_ДПСУ_Optimi zed.pdf. (дата звернення: 04.03.2019).

446. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. Відомості Верховної Ради України. 1994. № 31.

Ст. 286. URL: http://zakon4.rada.gov.ua/laws/show/80/94-вр (дата звернення: 20.10.2019).

447. Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29.03.2006 р. № 373. Офіційний вісник України. 2006. № 13. Ст. 878.

448. Пашков П. В. Митні інформаційні технології. URL: http://pidruchniki.com/13670622/informatika/zahist_informatsiyi_informatsiynih_sistemah (дата звернення: 21.10.2019).

449. Про рішення Ради національної безпеки і оборони України від 27.01.2016 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 16.06.2015 р. № 341/2015. Урядовий кур'єр. 2015. № 10.

450. Сташевський З. П., Грицюк Ю. І. Обгрунтування показника якості функціонування комплексної системи захисту інформації. *Вісник Національного технічного університету України «КПІ» : Радіотехніка. Радіоапаратобудування*. 2014. № 56. С. 137–143.

451. Про затвердження Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон : наказ ДПСУ, ДМСУ, ДПА України, МВС України, МЗС України, Мінсоцполітики, СБ України, СЗР України від 03.04.2008 р. № 284/287/214/150/64/175/266/75. URL: http://zakon3.rada.gov.ua/laws/show/z0396-08 (дата звернення: 20.10.2019).

452. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право*. 2017. № 5. С. 174–180.

453. Климчук О. О., Ткачук Н. А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. *Інформаційна безпека людини, суспільства, держави*. 2015. № 3. С. 75–83.

454. Словник української мови в 11 томах. Т 7. 1976. С. 77. URL: http://sum.in.ua/s/polipshuvaty (дата звернення: 17.11.2019).

455. Кушнір І. П., Ляшук Р. М. Результативність та ефективність в діяльності органів охорони державного кордону України. *Право і суспільство*. 2017. № 5. С. 154–159.

456. Разумков центр. URL: http://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/pidsumky2019-gromadska-dumka (дата звернення: 28.01.2020 р.).

457. Аналітична довідка за результатами проведеного Держкомтелерадіо моніторингу інформаційного наповнення офіційних веб-сайтів органів виконавчої влади у другому півріччі 2019 року. Додаток 1. URL: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=162482&cat_id=112507 (дата звернення: 28.01.2020).

458. Кілька сотень рівненчан пікетували львівський аеропорт та управління ДПСУ. URL: https://zaxid.net/news/ (дата звернення: 01.02.2020).

459. Стан роботи зі зверненнями громадян, що надійшли до органів управління Державної прикордонної служби України у 2019 році. URL: https://dpsu.gov.ua/ua/stan-roboti-zi-zvernen nyami-gromadyan-u-2018-roci/ (дата звернення: 04.02.2020).

460. Стратегічний бюлетень прикордонної безпеки «Біла книга 2016». Державна прикордонна служба України. URL: https://web.archive.org/web/20171210104237/http://dpsu.gov.ua/ua/Bila-kniga/ (дата звернення: 15.06.2019).

461. Інформація про структурний підрозділ або відповідальну особу. URL: http://www.ombudsman.gov.ua/ua/page/zpd/obnarodova nie-informatsii/informacziya-pro-strukturnij-pidrozdil-abo-vidpovidalnu-osobu/ (дата звернення: 19.01.2020).

462. Інформаційний комісар: справа зрушила. Що далі? Блог Ірини Кушнір. URL: https://dostup.pravda.com.ua/blogs/publications/bloh-iryny-kushnir-informatsiinyi-komisar-sprava-zrushyla-shcho-dali?fbclid=IwAR0o2EUUmphReXKsrGUUwIrUFqM225Vd0XzLz T59r7tmD7xS4qVIWbgo2Ag (дата звернення: 28.01.2020).

463. Велика палата КСУ перейшла до закритої частини пленарного засідання у справі щодо уповноважених Верховної Ради України. URL: http://www.ccu.gov.ua/novyna/velyka-palata-k su-pereyshla-do-zakrytoyi-chastyny-plenarnogo-zasidannya-u-spra vi-shchodo-5 (дата звернення: 30.10.2019)

464. FRONTEX REGISTER of NOTIFICATIONS pursuant to Articles 25 of EU Regulation (EC) No 45/2001. URL: https://frontex.europa.eu/assets/Data_Protection/Register_2020_01_22.xls (дата звернення: 22.01.2020).

465. Кваліфікований надавач електронних довірчих послуг «Військова частина 2428» ДПСУ. URL: https://acsk.dpsu.gov.ua/ (дата звернення: 28.12.2019).

466. Мота А. Ф. Діяльність Державної прикордонної служби України з протидії нелегальній міграції (адміністративно-правовий аспект) : монографія. Хмельницький, 2018. 492 с.

467. CASE OF AYCAGUER v. FRANCE (Application no. 8806/12). JUDGMENT (extracts). STRASBOURG. 22 June 2017. FINAL.22/09/2017. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-175007%22]} (дата звернення: 15.02.2020).

468. CASE OF GAUGHRAN v. THE UNITED KINGDOM. *(Application no. 45245/15).* JUDGMENT. FIRST SECTION. STRASBOURG. 13 February 2020. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-200817%22]} (дата звернення: 15.02.2020).

469. Про схвалення Концепції розвитку електронного урядування в Україні : розпорядження Кабінету Міністрів України від 20.09.2017 р. № 649-р. URL: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80 (дата звернення: 17.09.2019).

470. Документи для перетинання державного кордону громадянами України. URL: https://dpsu.gov.ua/ua/Dokumenti-dlya-peretinannya-derzhavnogo-kordonu-gromadyanami-Ukraini/ (дата звернення: 17.09.2019).

471. Контактна інформація про органи охорони державного кордону. URL: https://dpsu.gov.ua/ua/kontaktna-informaciya-pro-organi-ohoroni-derzhavnogo-kordonu// (дата звернення: 20.09.2019).

472. Охорона кордону. URL: https://dpsu.gov.ua/ua/activity/ohorona-kordonu/ (дата звернення: 20.09.2019).

473. Калішенко Є. Правове забезпечення розвитку електронного урядування в Україні. *Підприємництво, господарство і право*. 2019. № 7. С. 140–146.

474. Контакти. URL: https://dpsu.gov.ua/ua/contacts/ (дата звернення: 20.09.2019).

475. Регіональні контакти. URL: https://dpsu.gov.ua/ua/contacts/regional/ (дата звернення: 20.09.2019).

476. Запит на інформацію. URL: https://dpsu.gov.ua/ua/info/ (дата звернення: 20.09.2019).

477. Електронне звернення. URL: https://dpsu.gov.ua/ua/Elektronne-zvernennya/ (дата звернення: 20.09.2019).

478. Кушнір І. П., Коротушак А. І. Питання удосконалення впровадження електронного урядування у Державній прикордонній службі України. *Вісник Південного регіонального центру Національної академії правових наук України*. 2019. № 20. С. 96–102.

479. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV. URL: https://zakon3.rada.gov.ua/laws/show/851-15 (дата звернення: 16.09.2019).

480. Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну : постанова Кабінету Міністрів України від 17.01.2018 р. № 55. *Урядовий кур'єр*. 2018. № 46.

481. Про суспільний доступ до документів Європейського Парламенту, Ради та Співтовариства : Регламент (ЄС) 1049/2001 Європейського Парламенту та Ради Європи від 30.05.2001 р. (ОВ L 145, 31.05.2001, С. 43).

482. On electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC : REGULATION (EU) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL : № 910/2014 of 23 July 2014. *Official Journal of the European Union.* L 257/73. 28.08.2014.

483. Про затвердження Положення про інтегровану систему електронної ідентифікації : Закон України від 19.06.2019 р. № 546. *Урядовий кур'єр*. 2019. № 121.

484. Цифрова держава. URL: https://plan2.diia.gov.ua/ (дата звернення: 20.02.2020).

485. Філіппов С.О. Кримінологічні засади протидії транскордонній злочинності : дис. … д-ра юрид. наук: 12.00.08. Дніпро, 2019. 561 с.

486. Кіберфронт. Реальні загрози штучного світу. *Кордон*. 2017. № 5. С. 24–29.

487. Правоохоронці продавали персональні дані українців бойовикам «ДНР». ДБР відкрило справу. URL: https://zmina.info/news/derzhprikordonsluzhba_prodavala_danni_ukrajinciv_bojovikam_dnr__rozsliduvannjia_/ (дата звернення: 19.01.2020).

488. СБУ викрили продаж інформації з баз даних Держприкордонслужби. URL: https://ntktv.ua/news/sbu_vykryla_prodazh_informatsiyi_z_baz_danykh_derzhprykordonsluzhby/ (Дата звернення: 05.07.2020.)

489. Слідчий продав службову інформацію і отримав кошти з РФ. URL: https://ukrainepravo.com/law-practice/practice_public_prosecutor/slidchyy-prodav-sluzhbovu-informatsiyu-i-otrymav-koshty-z-rf/ (дата звернення: 19.01.2020).

490. Воробьев Г. Г. Информационная культура в управленчесом труде. Москва. Экономика. 1971. 106 с.

491. Джинчарадзе Н. Г. Інформаційна культура особи: формування та тенденції розвитку (соціально-філософський аналіз) : автореф. дис. д-ра філос. наук : 09.00.03. Київ, 1997. 45 с.

492. Клімушин П. С., Іванова І. Д. Інформаційна культура державних службовців як чинник розвитку інформаційного суспільства. *Теорія та практика державного управління*. 2011. № 3(34). С. 1–7.

493. Бєляков К. І., Онопрієнко С. Г., Шопіна І. М. Інформаційна культура в Україні: правовий вимір : монографія / за заг. ред. К. І. Бєлякова. Київ : КВІЦ, 2018. 169 с.

494. Кириченко В. В. Інформаційна культура у структурі професійної компетентності державних службовців. *Науковий вісник Херсонського державного університету. Психологічні науки*. 2019. № 2. С. 113–119.

495. Права приватної особи в умовах пандемії COVID-19. Є. О. Харітонов, О. І. Харітонова, К. І. Бєляков та ін. Київ : Гельветика. 2020. С. 404.

496. Максименко Ю. Є. Нормативно-правове регулювання інформаційних відносин в Україні: стан та перспективи. *Юридичний вісник*. 2014. № 3. С. 142–146.

497. Kushnir I. Topical directions for improvement of information relations in activities of the State Border Guard Service of Ukraine. Low and Border: Addressing Security Threats at the Ukrainian Border : collective monograph. Lviv-Torun : Liha-Pres. 2019. P. 89–108.

498. План заходів з реалізації стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору : Указ Президента України від 20.04.2019 р. № 155/2019. URL: https://www.president.gov.ua/documents/1552019-26586 (дата звернення: 28.04.2019).

499. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 р. № 96/2016. *Урядовий кур'єр*. 2016. № 52.

500. Шепета О. В. Адміністративно-правові засади технічного захисту інформації : монографія. Київ : ФОП О. С. Ліпкан, 2012. 296 с.

501. Шкарупа В. К., Цимбалюк В. С. Застосування положень права щодо формування основ теорії інформаційного права. *Правова інформатика*. 2006. № 3 (11). С. 44–51.

502. Красноступа Г. М. До кодифікації інформаційного законодавства України. *Актуальні питання кодифікації законодавства України* / за ред. В. О. Зайчука. Ін-т законодавства Верховної Ради України. Київ. 2009. № 4. С. 119–123.

503. Коваленко Л. П. Деякі питання щодо систематизації інформаційного законодавства. 2013. URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwi8sKfmuavnAhVtlosKHVDtAewQFjAAegQIARAB&url=http%3A%2F%2Ftlaw.nlu.edu.ua%2Farticle%2Fdownload%2F62882%2F58340&usg=AOvVaw02j8eSeNlmJTNfqrRfiWV4 (дата звернення: 07.10.2019).

504. Цимбалюк В. С. Питання кодифікації інформаційного законодавства. *Правова інформатика*. 2009. № 4(24). С. 13–22.

505. Скільки людей перетнули український кордон у 2018-му. URL: https://www.the-village.com.ua/village/city/city-news/280799-skilki-lyudey-peretnuli-ukrayinskiy-kordon-u-2018-mu (дата звернення: 26.06.2019).

506. У 2019 році громадяни значно менше перетинали кордон з Росією, але частіше подорожували морем та повітрям. URL: https://dpsu.gov.ua/ua/news/U-2019-roci-gromadyani-znachno-menshe-peretinali-kordon-z-Rosiyu-ale-chastishe-podorozhuvali-morem-ta-povitryam/ (дата звернення: 11.02.2020).

507. Програма діяльності Кабінету Міністрів України. Проект Концепції державної політики щодо досягнення цілі 13.5 «Українці захищені надійним кордоном та задоволені сервісом при його перетинанні». URL: https://program.kmu. gov.ua/meta/ukrainci-zahiseni-nadijnim-kordonom-ta-zadovoleni-ser visom-pri-jogo-peretini (дата звернення: 10.02.2020).

508. Про Національну гвардію України : Закон України від 13.03.2014 р. № 876-VII. *Відомості Верховної Ради України*. 2014. № 17. Ст. 594.

509. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40–41. Ст. 379.

510. Про державну службу : Закон України від 10.12.2015 р. № 889-VIII. *Урядовий кур'єр*. 2016. № 21.

511. Порядок дій уповноважених службових осіб Державної прикордонної служби України в разі виявлення в пунктах пропуску через державний кордон України та контрольних пунктах в'їзду на тимчасово окуповану територію України та виїзду з неї осіб, стосовно яких надано доручення, та порядок

взаємодії органів охорони державного кордону з уповноваженими державними органами, які надали доручення : наказ МВС України від 23.06.2017 р. № 535. URL: https://zakon.rada.gov.ua/laws/show/z1091-17 (дата звернення: 24.01.2020).

512. Жангожа Р. До питання розширення інформаційного простору України. *Стратегічна панорама*. 2000. № 3, 4. С. 203–206.

513. Баранов О. А. Напрями перспективних досліджень у галузі інформаційного права. *Інформація і право*. 2016. № 2(17). С. 15–31.

514. Рішення Орджонікідзевського районного суду справа справі № 335/13988/17 2-а/335/58/2018 від 6.03.2018 р. URL: https://youcontrol.com.ua/catalog/court-document/72697946/ (дата звернення: 12.09.2019).

515. Кушнір І. П. Щодо поняття «недостовірні відомості» у складі злочину «незаконне перетинання державного кордону України». *Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності* : тези II Всеукраїнської науково-практичної конференції (Хмельницький, 1 березня 2019 року). Хмельницький : Видавництво НАДПСУ, 2019. С. 243–244.

516. Володавська О. С. Кримінально-правова характеристика предмета злочину, передбаченого статтею 330 Кримінального кодексу України, за чинним кримінальним законодавством. *Вісник кримінологічної асоціації України*. 2015. № 2 (10). С. 65–74.

517. Кушнір І. П. Захист інформації, отриманої під час здійснення оперативно-розшукової діяльності в інтересах забезпечення захисту державного кордону України: кримінально-правовий аспект. *Актуальні проблеми кримінально-правового, кримінально-процесуального та криміналістичного забезпечення безпеки України* : тези міжнародної науково-практичної конференції (Дніпро, 30 листопада 2018 року). Дніпро, 30 листопада 2018 р. Дніпро : Видавець Біла К. О., 2018. С. 99–100.

518. Кушнір І. Питання удосконалення термінології інформаційного законодавства. *Українська мова в юриспруденції: стан, проблеми, перспективи*. Тези XV Всеукраїнської науково-практичної конференції. КНУВСУ. Київ. 2019. С. 129–131.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Монографії:

1. Кушнір І. П. Нормативно-правове регулювання інформаційних відносин у діяльності Державної прикордонної служби України: теоретичні та організаційні аспекти : монографія / за заг. ред. д-ра юрид наук Р. М. Ляшука, Хмельницький. Вид-во: ПП «Монускрипт», 2020. 528 с.

Калюжний Р. А. *Рецензія на монографію* Кушнір І. П. «Нормативно-правове регулювання інформаційних відносин у діяльності Державної прикордонної служби України: теоретичні та організаційні аспекти». Юридичний вісник «Повітряне і космічне право». 2020. № 2 (55). С. 224–225.

Орловська Н. А. *Рецензія на монографію* Кушнір І. П. «Нормативно-правове регулювання інформаційних відносин у діяльності Державної прикордонної служби України: теоретичні та організаційні аспекти». Часопис Київського університету права. 2020. № 2. С. 513.

2. Kushnir I. Topical directions for improvement of information relations in activities of The State Border Guard Service Of Ukraine. Low and Border: Addressing Security Threats at the Ukrainian Border : collective monograph / N. Orlovska, S. Filippov, V. Kushar, I. Hloviuk, V. Polovnikov, I. Kushnir, P. Volynets. Lviv-Torun : Liha-Pres. 2019. P. 89–108.

Статті в наукових фахових виданнях України та періодичних наукових виданнях, внесених до міжнародних наукометричних баз:

3. Кушнір І. П. Інформаційні відносини у прикордонній сфері. *Науковий вісник Ужгородського національного університету*. 2016. № 36. Т. 2. С. 36–38.

4. Кушнір І. П. Напрями прикордонної інформаційної безпеки як складова національної безпеки України. *Порівняльно-аналітичне право*. № 5. 2017. С. 230–233. URL: http://pap.in.ua/index.php/arhiv-vidannja/96.

5. Кушнір І. П. Доктринальні підходи до різноманітності інформаційних правовідносин. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки.* 2017. Вип. 4. URL: http://nbuv.gov.ua/UJRN/vnadpcurn_2017_4_8.

6. Кушнір І. П. Класифікація інформаційно-правових відносин у прикордонній сфері. *Вісник Запорізького національного університету. Юридичні науки.* 2017. № 4. С. 56–62. URL : http://nbuv.gov.ua/UJRN/Vznu_Jur_2017_4_9.

7. Кушнір І. П. Основні засади інформаційної політики держави в прикордонній сфері. *Науковий вісник Херсонського державного університету. Юридичні науки*. 2017. Вип. 6. Т. 2. С. 81–84.

8. Кушнір І. П. Види інформації, розпорядником якої є Державна прикордонна служба України, їх сутнісна характеристика. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2018. Вип. 1. URL: http://nbuv.gov.ua/UJRN/vnadpcurn_2018_1_6.

9. Кушнір І. П. Органи охорони державного кордону як суб’єкти інформаційних правовідносин. *Правові новели*. 2018. № 5. С. 71–77.

10. Кушнір І. П. Кримінально-правове забезпечення охорони інформаційних відносин у прикордонній сфері. *Питання боротьби зі злочинністю.* 2018. Вип. 36. 186 с. С. 82–93.

11. Кушнір І. П. Інформаційно-правова діяльність Державної прикордонної служби України: нормативно-правовий аспект. *Конституційно-правові академічні студії*. 2018. № 2. С. 165–170.

12. Кушнір І. П. Інформаційно-правовий статус Державної прикордонної служби України. *Приватне та публічне право*. 2018. № 4. с. 50–53.

13. Кушнір І. П. Аналіз змісту поняття «безпека державного кордону». *Вісник Південного регіонального центру Національної академії правових наук України*. 2018. № 16. С. 76–81.

14. Кушнір І. П. Організаційно-правові питання забезпечення захисту інформації в інформаційних системах Державної прикордонної служби України. *Прикарпатський юридичний вісник*. 2018. № 3. С. 81–84.

15. Кушнір І. П. Співвідношення понять «інформаційна безпека» та «захист інформації» в діяльності Державної прикордонної служби України. Науковий вісник *Міжнародного гуманітарного університету. Юриспруденція.* 2018. № 35. Т. 1. с. 81–84.

16. Кушнір І. П. Особливості правових відносини щодо забезпечення запиту на публічну інформацію, розпорядником якої є Державна прикордонна служба України. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2018. Вип. 4. URL: https://nadpsu.edu.ua/wp-content/uploads/2019/02/visnuk_4_2019_ur.pdf.

17. Кушнір І. П. Адміністративна відповідальність за порушення законодавства про інформацію у прикордонній сфері. *Право і інформація.* № 1(28). 2019. С. 45–51.

18. Кушнір І. П. Інформаційна відкритість у діяльності Державної прикордонної служби України. *Правова позиція.* 2019. № 1 (22). С. 30–36.

19. Кушнір І. П. Інформаційні загрози в діяльності Державної прикордонної служби України. *Підприємництво, господарство і право*. 2019. № 7. С. 147–150.

20. Кушнір І. П. Царенко О. М. Правовий режим інформації з обмеженим доступом у діяльності Державної прикордонної служби України. *Право та державне управління.* 2019. № 3. С. 180–185.

21. Кушнір І. П., Коротушак А. І. Питання удосконалення впровадження електронного урядування у Державній прикордонній службі України. *Вісник Південного регіонального центру Національної академії правових наук України*.

2019. № 20. С. 96–102.

22. Кушнір І. П. Теоретичні засади дослідження інформаційних відносин у діяльності Державної прикордонної служби України. *Держава та регіони. Право.* 2019. № 4. С. 86–91.

23. Кушнір І. П., Царенко С. І., Царенко О. М. Особливості застосування дисциплінарної відповідальності за порушення інформаційного законодавства у діяльності Державної прикордонної служби України *Актуальні проблеми вітчизняної юриспруденції.* 2019. № 6. С. 80–84.

24. Кушнір І. П., Новодранов Р. С. Проблеми та перспективи розвитку консультаційної роботи Контактного центру Державної прикордонної служби України. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2019. Вип. 4. URL: http://periodica.nadpsu.edu.ua/index.php/legal/article/view/316/317.

25. Кушнір І. П. Актуальні питання забезпечення інформаційної приватності у діяльності Державної прикордонної служби України. *Конституційно-правові академічні студії*. 2020. № 1. С. 7–13.

Статті у наукових періодичних виданнях інших держав:

26. Кушнір І., Степанова Ю. Інформаційна безпека держави у прикордонній сфері як об’єкт державної зради. National law journal: theory and practice. 2018. № 4 (32). Т. 1. С. 123–126.

27. Кушнір І. П. Реалізація права на звернення громадян у Державній прикордонній службі України. Visegrad Journal on Human Rights. 2018. 4 (volume 2). С. 56-60.

28. Кушнір І. П. Методологічні засади теорії інформаційних відносин у прикордонній сфері. National law journal: theory and practice. 2019. № 2 (36). С. 17–20.

29. Kushnir I. Information component in preparing and making management decisions in border protection bodies of the state border of Ukraine. Legea si Viata.

2019. № 5. С. 100–104.

30. Кушнір І. П. Основні тенденції інформаційної взаємодії у діяльності Державної прикордонної служби України. Visegrad Journal on Human Rights. 2019. 4 (volume 2). С. 96–101.

31. Kushnir I. A Comparative Analysis of Personal Data and its Protection in the Course of Border Procedures (Ukraine, European Union). *Current Issues in Administrative Law*. Edited by Cătălin-Silviu Săraru. 2020. Cambridge Scholars Publishing. С. 130–141.

Опубліковані праці апробаційного характеру:

32. Кушнір І. П. Суспільні інформаційні відносини в діяльності органів охорони державного кордону. *Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України* : тези VIII Всеукраїнської науково-практичної конференції (Хмельницький, 10 грудня 2015 р.). Хмельницький : Вид-во НАДПСУ, 2015. с. 141.

33. Кушнір І. П. Правове забезпечення захисту інформації пов’язаної із охороною державного кордону. *Кібербезпека України : правові та організаційні питання* : тези Всеукраїнської науково-практичної конференції (м. Одеса, 21 жовтня 2016 р.). Одеса : ОДУВС, 2016. С. 152–154.

34. Кушнір І. П. Забезпечення права подання запиту на інформацію у Державній прикордонній службі України. *Інформаційна безпека: європейські орієнтири та перспективи для України* : збірник наукових праць за матеріалами III Міжнародного науково-практичного столу. Серія «Сектор безпеки України». № 14 (м. Харків, 25 листопада 2016 р.). Харків : «Плеяда», 2016. С. 94–94.

35. Кушнір І. П. Отримання громадянами інформації про діяльність Державної прикордонної служби України. *Освітньо-наукове забезпечення діяльності правоохоронних органів і військових формувань України* : тези IX Всеукраїнської науково-практичної конференції (Хмельницький, 8 грудня 2016 р.). Хмельницький : Вид-во НАДПСУ, 2016. с. 187.

36. Кушнір І. П. Проблемні питання відомчої нормотворчої компетенції Державної прикордонної служби України. *Молодіжний науковий юридичний форум* : тези доповідей Всеукраїнській науково-практичній конференції до Дня науки (м. Київ, 18 травня 2017 р.). Київ : Вид-во ТОВ МП ЛЕСЯ, 2017. С. 27–28.

37. Кушнір І. П. Державна інформаційна політика у прикордонній сфері. *Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України* : тези X Всеукраїнської науково-практичної конференції (Хмельницький, 2 листопада 2017 р.). Хмельницький : Вид-во НАДПСУ, 2017. С. 199–200.

38. Кушнір І. П. Питання кримінально-правової охорони інформації у функціонуванні Державної прикордонної служби України. *Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності* : тези II Всеукраїнської науково-практичної конференції (Хмельницький, 2 березня 2018 р.). Хмельницький: Вид-во НАДПСУ, 2018. С. 169–172.

39. Кушнір І. П. Окремі аспекти забезпечення міжвідомчого обміну інформацією між суб'єктами інтегрованого управління кордонами. *Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи* : тези п'ятої Всеукраїнської науково-практичної конференції (Одеса, 13-14 вересня 2018 р.). Одеса. 2018. С. 57–59.

40. Кушнір І. П. Прикордонна інформаційна безпека як складова національної безпеки України *Освітньо-наукове забезпечення складових сектору безпеки і оборони України* : тези XI Всеукраїнської науково-практичної конференції (Хмельницький, 15 листопада 2018 р.). Хмельницький : Вид-во НАДПСУ, 2018. С. 247–248.

41. Кушнір І. П. Захист інформації отриманої під час здійснення оперативно-розшукової діяльності в інтересах забезпечення захисту державного кордону України: кримінально-правовий аспект. *Актуальні проблеми кримінально-правового, кримінально-процесуального та криміналістичного*

забезпечення безпеки України : тези Міжнародної науково-практичної конференції (Дніпро, 30 листопада 2018 р.). Дніпро: Вид-во Біла К. О., 2018. С. 99–100.

42. Кушнір І. П. Кібербезпека як складова інформаційної безпеки у сфері охорони державного кордону України. *Кібербезпека України : правові та організаційні питання* : тези Всеукраїнської науково-практичної конференції (м. Одеса, 30 листопада 2018 р.). Одеса : ОДУВС, 2018. С. 48–49.

43. Кушнір І. П. Щодо поняття «недостовірні відомості» у складі злочину «незаконне перетинання державного кордону України». *Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності* : тези II Всеукраїнської науково-практичної конференції (Хмельницький, 1 березня 2019 р.). Хмельницький : Вид-во НАДПСУ, 2019. С. 243–244.

44. Кушнір І. П. Інформаційна взаємодія як основа забезпечення спільних дій правоохоронних органів та військових формувань в охороні державного кордону. *Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи* : тези Міжнародної науково-практичної конференції (Одеса, 13-14 вересня 2019 р.). Одеса. 2019. С. 186–187.

45. Кушнір І. П. Питання контролю та нагляду у функціях Державної прикордонної служби України. *Стан та перспективи розвитку адміністративного права України* : тези IV Міжнародної науково-практичної інтернет-конференції (Одеса, 23 жовтня 2019 р.). Одеса. 2019. С. 64.

46. Кушнір І., Степанова Ю. Критерії класифікації злочинів у сфері службової діяльності. *Пріоритетні напрямки розвитку та реформування правоохоронних органів* : тези науково-практичної інтернет-конференції. (Херсон, 31 жовтня 2019 р.). Херсон. 2019. С. 184–189.

47. Кушнір І. П. Правовий режим інформації як детермінанта прикордонної безпеки. *Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України* : тези Міжнародної науково-практичної

конференції (Хмельницький, 22 листопада 2019 р.). Хмельницький : Вид-во НАДПСУ, 2019. С. 262–263.

48. Кушнір І. Актуальні засади захисту інформації, що обробляється в автоматизованих системах Державної прикордонної служби України. *Кібербезпека України : правові та організаційні питання* : тези Міжнародної науково-практичної конференції (м. Одеса, 22 листопада 2019 р.). Одеса : ОДУВС, 2019. С. 25–26.

49. Кушнір І. Питання удосконалення термінології інформаційного законодавства. *Українська мова в юриспруденції: стан, проблеми, перспективи* : тези XV Всеукраїнської науково-практичної конференції. КНУВСУ (Київ, 28 листопада 2019 р.). Київ. 2019. Ч. 1. С. 129–131.

50. Кушнір І. Щодо наслідків інформаційно-психологічного впливу як прояв військової боротьби. *Військова освіта і наука: сьогодення та майбутнє* : тези XV Міжнародної науково-практичної конференції. (Київ, 29 листопада 2019 р.) Київ. 2019.с. 239–240.

51. Кушнір І. П. Інформаційна функція у контексті інтегрованого управління кордонами. *Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи* : тези Міжнародної науково-практичної конференції (Одеса, 10-11 вересня 2020 р.). Одеса. 2020. С. 462–463.

52. Кушнір І. П. Інформаційна відкритість, як невід’ємна складова забезпечення прикордонного контролю: досвід Державної прикордонної служби України. *Стратегічні комунікації у сфері забезпечення національної безпеки і оборони : проблеми, досвід, перспективи* : тези доповідей І-ої Міжнародної науково-практичної конференції (м. Київ, 1 жовтня 2020 р.). Київ. 2020. С. 65–67.

53. Кушнір І. Термін «забезпечення» у контексті інформаційних відносин. *Українська мова в юриспруденції: стан, проблеми, перспективи* : тези XVI Всеукраїнської науково-практичної конференції. КНУВСУ (Київ, 25 листопада 2020 р.). Київ. 2020. С. 64–67.

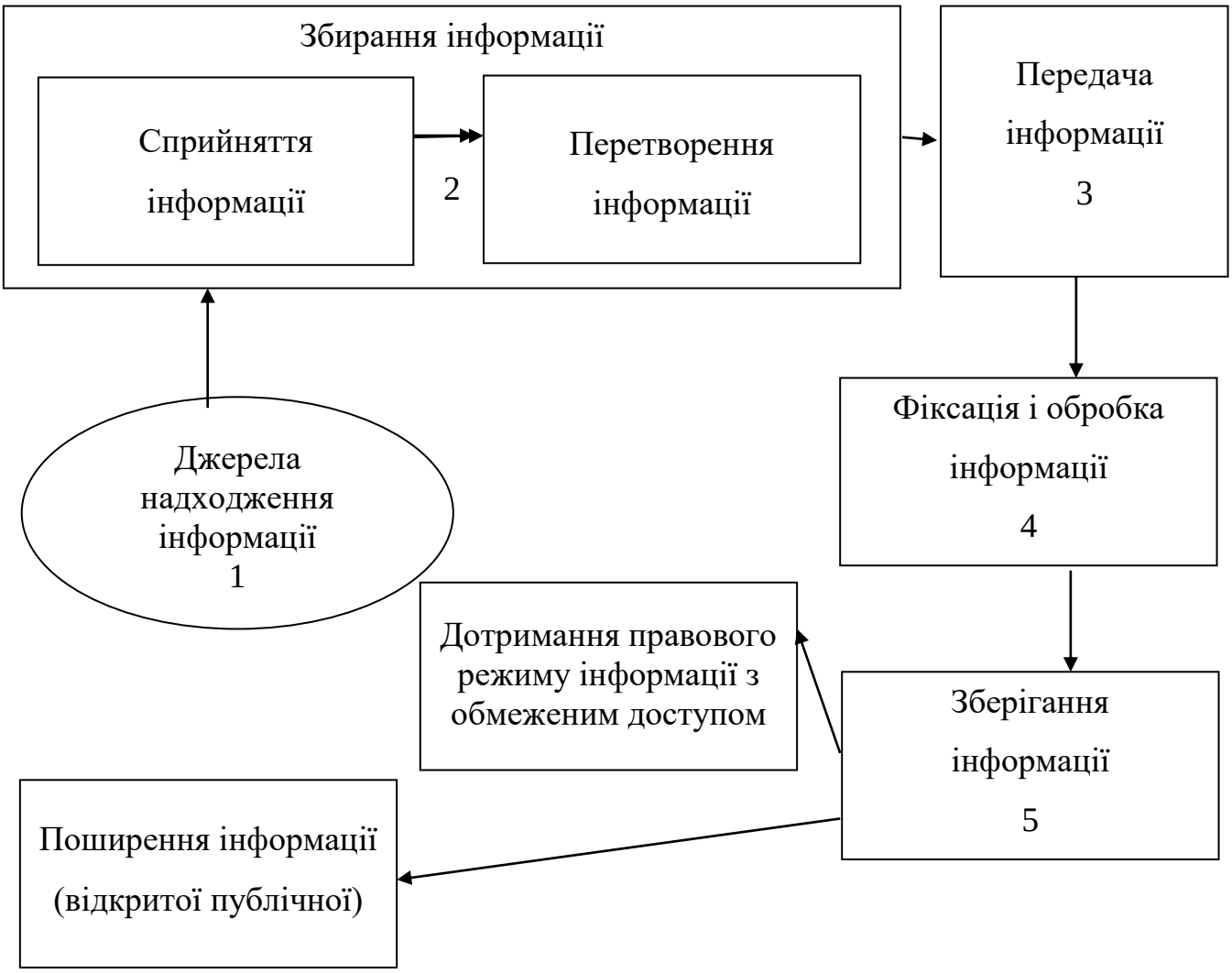
54. Кушнір І. П. Актуальні питання забезпечення прайвесі (правові та соціальні аспекти). *Актуальні проблеми інтелектуального, інформаційного та IT права* : збірник матеріалів четвертої Всеукраїнської науково-практичної конференції (м. Львів, 12 листопада 2020 р.). Львів. 2020. С. 87–91.

Наукові праці, які додатково
відображають результати дисертації:

55. Кушнір І. П., Ляшук Р. М. Результативність та ефективність в діяльності органів охорони державного кордону України. *Право і суспільство*. № 5. 2017. С. 154–159.

Додаток Б

Узагальнена структура процесу обігу інформації



Додаток В

Анкета
для проведення опитування
військовослужбовців Державної прикордонної служби України
з питань правового регулювання обігу інформації, забезпечення правового режиму інформації й інформаційної безпеки

Шановний респонденте, метою проведення даного опитування є дослідження особливостей та стану забезпечення правового регулювання обігу інформації, правового режиму інформації та інформаційної безпеки у Державній прикордонній службі України.

При заповненні анкети просимо обрати одну або декілька варіантів, на Ваш погляд, правильних відповідей.

№ з/п	Запитання	Варіант відповіді	Відповідь
Блок 1. Загальні дані			
1	До якого складу Ви належите?	офіцерський	45,9 %
		сержантський (старшинський)	13,9 %
		рядовий	40,2 %
2	Термін перебування на службі	до 5 років	52,8 %
		до 10 років	7,4 %
		до 15 років	10,4 %
		до 20 років	14,7 %
		більше 20 років	14,7 %
3	Ваша спеціальність	Філологія	13,1 %
		Психологія	6,5 %
		Право	14 %
		Телекомунікації та радіотехніка	10 %
		Безпека державного кордону	10,5 %
		Військове управління (за видами збройних сил)	7 %
		Національна безпека (сфера прикордонної діяльності)	3,5 %
		Правоохоронна діяльність	22,3 %
		Автомобільний транспорт	13,1 %
4	Чи мали Ви досвід роботи у ДПСУ з інформаційною діяльністю (оприлюднення публічної інформації про ДПСУ, забезпечення безпеки та функціонування інформаційних	так	39,9 %
		ні	60,1 %

	систем, інформаційно-аналітична діяльність, робота із запитами і зверненнями громадян)?		
5	Який із видів інформаційної діяльності Вам частіше доводиться реалізовувати у своїй службовій діяльності?	створення інформації	25,1 %
		збирання інформації	55,8 %
		одержання інформації	57,6 %
		зберігання інформації	37,7 %
		використання інформації	52,8 %
		оприлюднення відкритої публічної інформації	7,4 %
		забезпечення безпеки та функціонування інформаційних систем	9,1 %
		інформаційно-аналітична діяльність	23,4 %
		робота із запитами і зверненнями громадян	9,5 %
		охорона та захист інформації	15,6 %
		складно відповісти	19 %
6	З яким видом інформації Вам частіше приходиться стикатись у своїй службовій діяльності	інформація про фізичну особу	33,6 %
		інформація довідково-енциклопедичного характеру	26,1 %
		науково-технічна інформація	31 %
		правова інформація	49,1 %
		статистична інформація	32,7 %
		соціологічна інформація	19 %
		відкрита	57,2 %
		обмеженого доступу	33,6 %
Блок 2. Правове регулювання інформації			
7	Що Ви вкладаєте у зміст поняття «інформація» у сфері діяльності ДПСУ	дані про факти (кількість) перетинання державного кордону	53,5 %
		інформація про персонал відомства	40,7 %
		дані про результати (показники) діяльності посадових осіб (підрозділів) ДПСУ	46 %
		відомості, пов’язані із порядком функціонуванням органів охорони державного кордону та порядком перетинання державного кордону	61,5 %
		інформація про джерела та зміст	47,8 %

		норм права, що врегульовують діяльність ДПСУ	
		об’єкт інформаційних відносин у діяльності ДПСУ	28,3 %
		відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді у сфері діяльності ДПСУ	55,8 %
8	Як Ви вважаєте, хто є розпорядником інформації у сфері діяльності ДПСУ?	Президент України	2,6 %
		Кабінет Міністрів України	2,6 %
		МВС України	11,7 %
		ДПСУ	63,2 %
		військовослужбовці ДПСУ	12,6 %
		особи, що надали свої персональні дані для обробки	7,3 %
9	Як Ви оцінюєте сучасний стан нормативно-правового регулювання відносин пов’язаних зі створенням, збиранням, одержанням, зберіганням, використанням, поширенням, охороною та захистом інформації в діяльності ДПСУ?	позитивно	39,4 %
		задовільно	52,8 %
		незадовільно	7,8 %
10	Як Ви вважаєте, що передбачає державна інформаційна політика?	вироблення, реалізацію та контроль за реалізацією й удосконаленням державної стратегії і тактики в інформаційній сфері	53,7 %
		забезпечення доступу до інформації, її охорона й захист	22,1 %
		регулювання інформаційних процесів	3 %
		політика інформаційної безпеки	5,6 %
		збереження державної таємниці	7,8 %
		забезпечення функціонування інформації в суспільстві	6,1 %
		інформаційна ідеологія держави	1,7 %
11	На Вашу думку, яке поняття є ширшим серед запропонованих?	інформаційна безпека	72,7 %
		захист інформації	27,3 %

12	Як ви розумієте зміст поняття «інформаційна складова» у сфері охорони державного кордону?	система інформаційних відносин у ДПСУ	18,2 %
		порядок обігу інформації у діяльності ДПСУ	38,1 %
		елемент у системі забезпечення охорони державного кордону	26,4 %
		функціонування інформаційних систем ДПСУ	17,3 %
13	Як Ви думаєте, що означає принцип «відкритості перед громадянами»?	можливість громадян відвідувати приміщення органів і підрозділів ДПСУ	12,6 %
		поінформованість громадян про діяльність ДПСУ	73,6 %
		можливість громадян звернутись до посадових осіб ДПСУ за будь-якою інформацією	32,9 %
		можливість громадян звернутись (особисто, письмово) до посадових осіб ДПСУ за інформацією у межах компетенції прикордонного відомства	77,1 %
		можливість громадян прийти на прийом до посадових осіб ДПСУ	35,9 %
14	На Вашу думку, чи є доцільним запровадження електронного обліку відомчих нормативно-правових актів з метою своєчасного отримання інформації з питань правового регулювання діяльності ДПСУ?	так	98,1 %
		ні	1,9 %
15	Як Ви вважаєте, чи потрібно сьогодні офіцеру ДПСУ володіти знаннями щодо: правового регулювання обігу інформації, її видів; поняття та обсягу персональних даних; правового регулювання конфіденційної інформації; інформаційної безпека та захисту інформації; правового режиму	так	91,8 %
		ні	8,2 %

	службової інформації та державної таємниці; настання юридичної відповідальності за порушення норм інформаційного законодавства?		
16	Хотіли б Ви вивчати основи інформаційного законодавства, правові основи інформаційної безпеки та кібербезпеки у НАДПСУ?	так	75,8 %
		ні	24,2 %
17	З якими проблемами ви стикались у ході обробки інформації у сфері діяльності ДПСУ?	відсутність норми, яка б врегульовувала обіг інформації	16,5 %
		суперечність норм інформаційного законодавства	31,6 %
		недосконалий механізм обробки інформації	38,5 %
		недотримання посадовими особами вимог інформаційного законодавства	20,8 %
		складно відповісти	44,2 %
18	Чи достатньо Ви поінформовані про перелік службової інформації у сфері діяльності ДПСУ?	так	70,6 %
		ні	29,4 %
Блок 3. Інформаційна безпека			
19	На вашу думку, які заходи передбачає інформаційна безпека у діяльності ДПСУ?	захист і збереження інформації у сфері діяльності ДПСУ	54,2 %
		захист інформації та захищеність її від загроз	12,1 %
		створення нормальних умов функціонування ДПСУ	5,2 %
		своєчасне реагування на інформаційні загрози у прикордонній сфері	6,9 %
		боротьба з витоком закритої (таємної) інформації, а також з розповсюдженням хибної та ворожої інформацій	19,9 %
		недопущення негативного інформаційного впливу на військовослужбовців ДПСУ	1,7 %
20	Як Ви вважаєте, що найбільш повно відображає зміст поняття «інформаційна безпека»?	захищеність особистості, суспільства та держави від деструктивних та інших	41,1 %

		негативних впливів в інформаційному просторі (статичний стан)	
		сукупність практичних дій, спрямованих на захист даних від несанкціонованого доступу чи змін, як при їх зберіганні, так і при передачі (динамічний стан)	58,9 %
21	Як Ви оцінюєте рівень заходів із забезпечення інформаційної безпеки у ДПСУ?	достатній	43,7 %
		посередній	49,8 %
		недостатній	6,5 %
22	Що необхідно зробити негайно після виявлення шкідливого програмного забезпечення під час роботи на автоматизованому робочому місці?	доповісти по команді	56,9 %
		закрити програму заражену вірусом	6,6 %
		вимкнути комп'ютер	3,9 %
		відключити телекомунікаційну мережу	32,6 %
		продовжувати працювати	-
23	Під час користування соціальними мережами чи Інтернетом Ви можете розпізнати негативний інформаційний вплив?	так	83,5 %
		ні	16,5 %
24	Чи є обмеження для військовослужбовців щодо опублікування фото- та відеоматеріалів, інформації про себе та членів своєї сім'ї у соціальних мережах?	так	82,7 %
		ні	17,3 %
25	Ви особисто обмежуєте висвітлення інформації про себе та свою сім'ю у соціальних мережах?	так	83,1 %
		ні	16,9 %
Блок 4. Персональні дані			
26	Як Ви вважаєте, яка інформація відповідає змісту поняття «персональні дані»?	прізвище, ім'я, дата народження	74,9 %
		номер телефону, місце роботи	69,7 %
		електронна адреса	55 %
		фотографія	49,4 %
		сімейний стан	59,3 %
		інформація, зафіксована в паспортному чи іншому документі	77,1 %
		обіймана посада	44,6 %
		відомості чи сукупність	66,2 %

		відомостей про фізичну особу, яка ідентифікована	
27	Чи потрібна згода суб’єкта персональних даних на обробку її персональних даних?	так	97,4 %
		ні	2,6 %
28	У якій формі надається згода на обробку персональних даних?	письмово	61,9 %
		усно	3,5 %
		у формі, що дає змогу зробити висновок про надання згоди	34,6 %
29	Чи достатньо Ви поінформовані про перелік персональних даних підлеглих, які Ви не маєте право розголошувати?	так	80,1 %
		ні	19,9 %
30	На Вашу думку, чи є відмінність між поняттями «персональні дані» і «інформація про особу»?	так	89,6 %
		ні	10,4 %
31	Яка інформація належить до інформації з обмеженим доступом?	будь-яка інформація у сфері діяльності ДПСУ	23,4 %
		корпоративна інформація	13,9 %
		конфіденційна інформація	71,4 %
		службова інформація	82,7 %
		таємна інформація	80,1 %
32	Що, на Вашу думку, є конфіденційною інформацією?	інформація про фізичну особу	7,8 %
		інформація про посадову особу	4,8 %
		службова інформація	13,4 %
		інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень	74 %
33	Чи потрібне бажання (згода) особи на поширення її конфіденційної інформації?	так	96,5 %
		ні	3,5 %
34	Чи є у ДПСУ посадова особа із захисту персональних даних?	так	24,7 %
		ні	75,3 %
35	Чи зазнавали Ви порушення інформаційних прав у службовій діяльності (ненадання Вам або розголошення Ваших персональних даних тощо)?	так	15,2 %
		ні	84,8 %
36	Чи виникала у Вас потреба у захисті персональних даних з приводу службової діяльності?	так	25,1 %
		ні	74,9 %

37	Чи звертались Ви для захисту своїх персональних даних до посадових осіб ДПСУ?	так	12,1 %
		ні	87,9 %
38	Чи знаєте Ви про функціонування Департаменту у сфері захисту персональних даних Уповноваженого Верховної Ради України з прав людини?	так	58 %
		ні	42 %
Блок 5. Відповідальність за порушення норм інформаційного законодавства			
39	На Вашу думку, хто несе відповідальність за організацію, створення, збирання, одержання, зберігання, використання, поширення, охорону та захист інформації в діяльності ДПСУ?	командири підрозділів ДПСУ	20,3 %
		МВС України	3 %
		компетентні посадові особи	22,1 %
		персонально кожен військовослужбовець ДПСУ	54,6 %
40	Хто, на Вашу думку, несе персональну відповідальність за ненадання чи розповсюдження персональних даних, службової інформації?	командири підрозділів	15,6 %
		компетентні посадові особи	18,6 %
		кожен військовослужбовець	65,8 %
41	Який вид юридичної відповідальності передбачено за незаконне використання інформації, що стала відома особі у зв’язку з виконанням службових повноважень?	кримінальна	61,5 %
		адміністративна	27,7 %
		дисциплінарна	10,4 %
		цивільна	0,4 %
42	Який вид юридичної відповідальності передбачено за несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї:	кримінальна	65,7 %
		адміністративна	23,4 %
		дисциплінарна	10 %
		цивільна	0,9 %
Блок 6. Отримання інформації			
43	Чи достатньою мірою Ви інформовані про нормативно-правове регулювання відносин, пов’язаних зі створенням, збиранням, одержанням, зберіганням, використанням, поширенням, охороною та захистом інформації в діяльності ДПСУ?	так	58,9 %
		ні	13,4 %
		складно відповісти	27,7 %

44	Які джерела Ваших знань про правове регулювання відносин, пов’язаних зі створенням, збиранням, одержанням, зберіганням, використанням, поширенням, охороною та захистом інформації в діяльності ДПСУ	особистий досвід	49,8 %
		нормативно-правові акти	69,3 %
		з досвіду колег (підрозділу)	34,2 %
		навчання в НАДПСУ	59,7 %
		навчання у інших вищих навчальних закладах	13,4 %

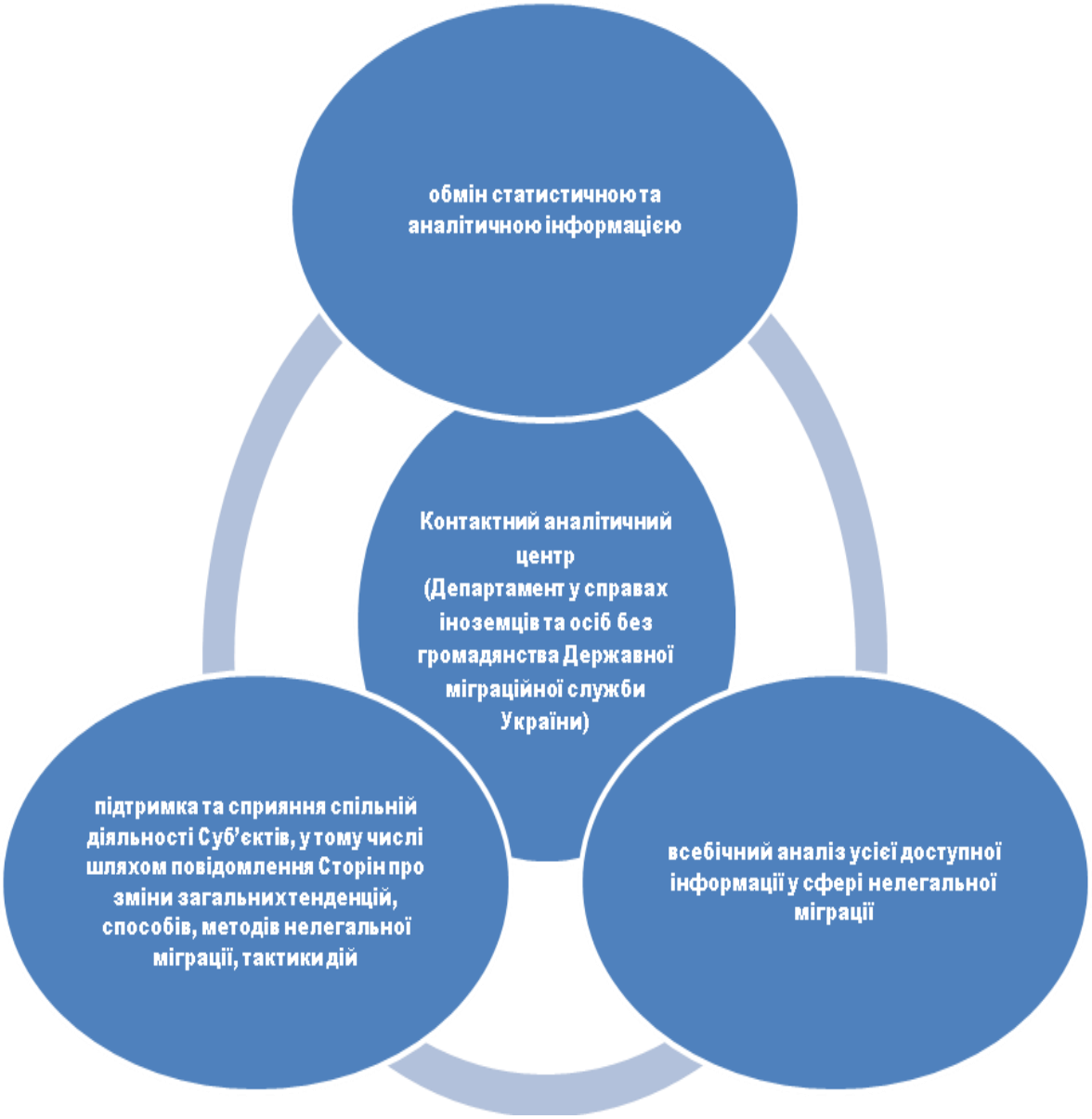
Дякуємо за надані відповіді!

Додаток Г

Елементи правового режиму інформації

Додаток Д

Напрямки діяльності
щодо обміну статистичною та аналітичною інформацією з питань протидії нелегальній міграції між МВС України, МЗС України, Мінісоцполітики, МОН України, СЗР України, СБ України, ДМС України, ДПСУ



Додаток Е

Таблиця 1.
Взаємодія інформаційних систем суб'єктів інформаційного обміну: ДФС України та ДПСУ

<table>
<tr><td colspan="2">здійснюється в електронному вигляді на рівні</td></tr>
<tr><td>центральному</td><td>територіальному</td></tr>
<tr><td colspan="2">шляхом:</td></tr>
<tr><td>обміну інформацією у режимі реального часу</td><td>подання суб'єктами інформаційного обміну запитів на отримання інформації (у разі відсутності можливості обміну інформацією у режимі реального часу)</td></tr>
<tr><td colspan="2">інформація яка передається підрозділами Держприкордонслужби/Адміністрацією Держприкордонслужби до митниць та їх структурних підрозділів/ ФС, а саме:</td></tr>
<tr><td>відомості про транспортні засоби, які перетинають державний кордон України та/або адміністративний кордон ВЕЗ «Крим» (державний реєстраційний номер, державна належність, тип, марка, номер кузова транспортного засобу (за наявності), кількість пасажирів (за наявності))</td><td>відомості про фізичних осіб, які перетинають державний кордон України та/або адміністративний кордон ВЕЗ «Крим» (громадянство, прізвище, ім'я, стать, серія, номер паспортного документа, дата та час останнього перетину державного кордону для в'їзду в Україну/виїзду з України)</td></tr>
</table>

Джерело: Про затвердження Порядку взаємодії інформаційних систем Державної фіскальної служби України та Державної прикордонної служби України щодо обміну інформацією, необхідною для забезпечення контролю при переміщенні осіб та транспортних засобів через державний (митний) кордон України та адміністративний кордон вільної економічної зони «Крим» : наказ МФ України, МВС України від 07.09.2017 № 746/759. *Офіційний вісник України*. 2017. № 85. Ст. 2585.

Таблиця 2.
Порядок організації обміну інформацією з виявлення та припинення корупційних діянь в правоохоронних органах

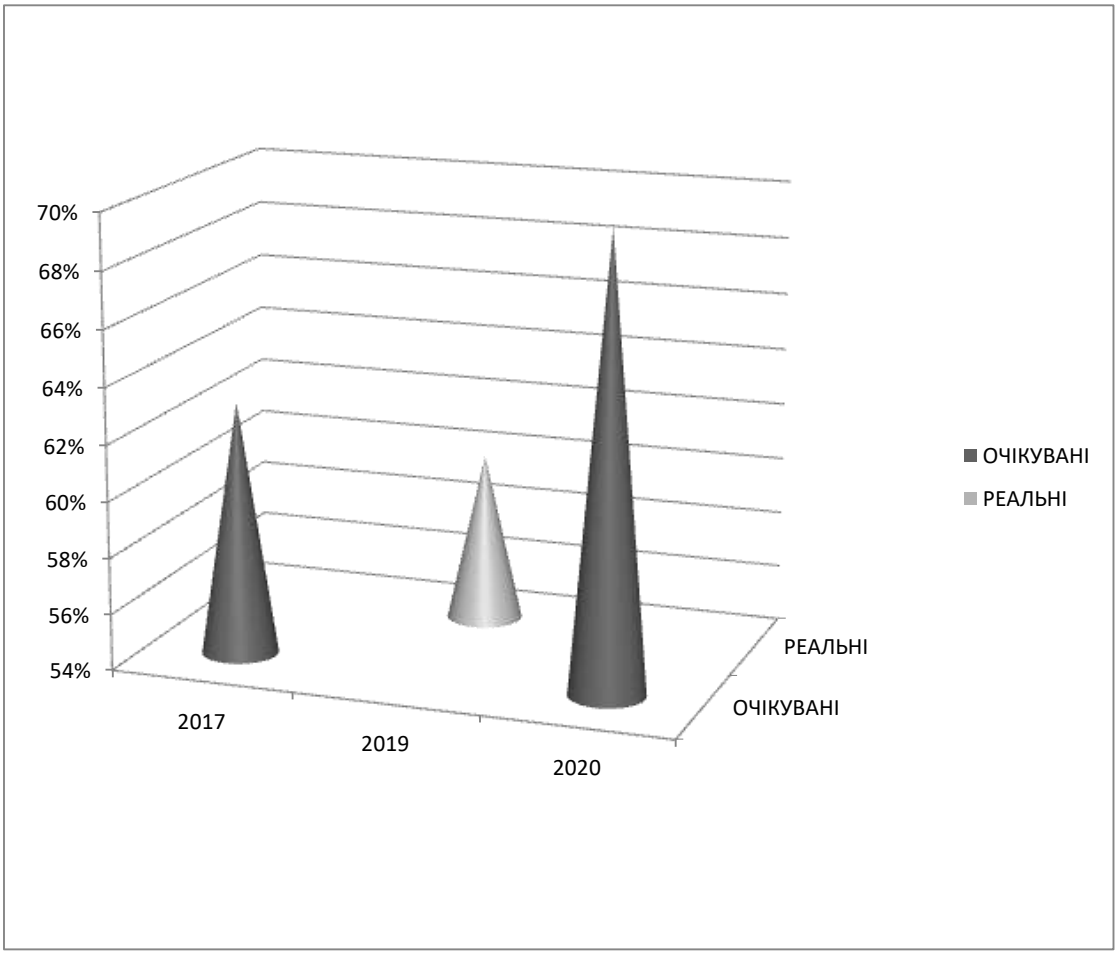
здійснюється на рівні	
на рівні міністерств та інших органів виконавчої влади обмін інформацією здійснюється між центральними апаратами (адміністраціями) уповноважених підрозділів (р. 3)	на регіональному рівні обмін інформацією здійснюється між відповідними уповноваженими підрозділами в регіонах та на залізничному транспорті (крім підрозділів внутрішньої безпеки митних органів). Обмін інформацією на регіональному рівні з підрозділами внутрішньої безпеки митних органів здійснюється через Управління внутрішньої безпеки ДФС України (р. 3)
реалізується шляхом (р. 2):	
– проведення спільних засідань та оперативних нарад уповноважених підрозділів	
– створення спільних робочих груп у складі представників уповноважених підрозділів для вивчення окремих проблем боротьби з корупцією та розроблення пропозицій щодо їх вирішення	
– взаємного інформування уповноваженими підрозділами один одного про виявлення ними в процесі здійснення своїх функцій таких причин і умов, що сприяють корупційним правопорушенням	
– інформування уповноваженими підрозділами один одного про відомі їм факти підготовки чи вчинення посадовими особами корупційного діяння та інших правопорушень, пов'язаних з корупцією, узгодженість дій під час їх документування	
– відрядження до іншого правоохоронного органу працівника уповноваженого підрозділу з метою проведення оперативно-розшукових та профілактичних заходів, спрямованих на боротьбу з корупцією, проведення наукових досліджень	

Джерело: Про затвердження Інструкції про порядок організації обміну інформацією між структурними підрозділами МВС, Служби безпеки України, Державної податкової адміністрації України, Державної прикордонної служби України, Держмитслужби в діяльності з виявлення та припинення корупційних діянь в правоохоронних органах : наказ МВС України, СБ України, ДПА України, Адміністрації ДПСУ, ДМСУ від 23.03.2009 р. № 124/ 936/139/199/250. URL: https://zakon.rada.gov.ua/laws/show/z0670-09 (дата звернення: 24.07.2019).

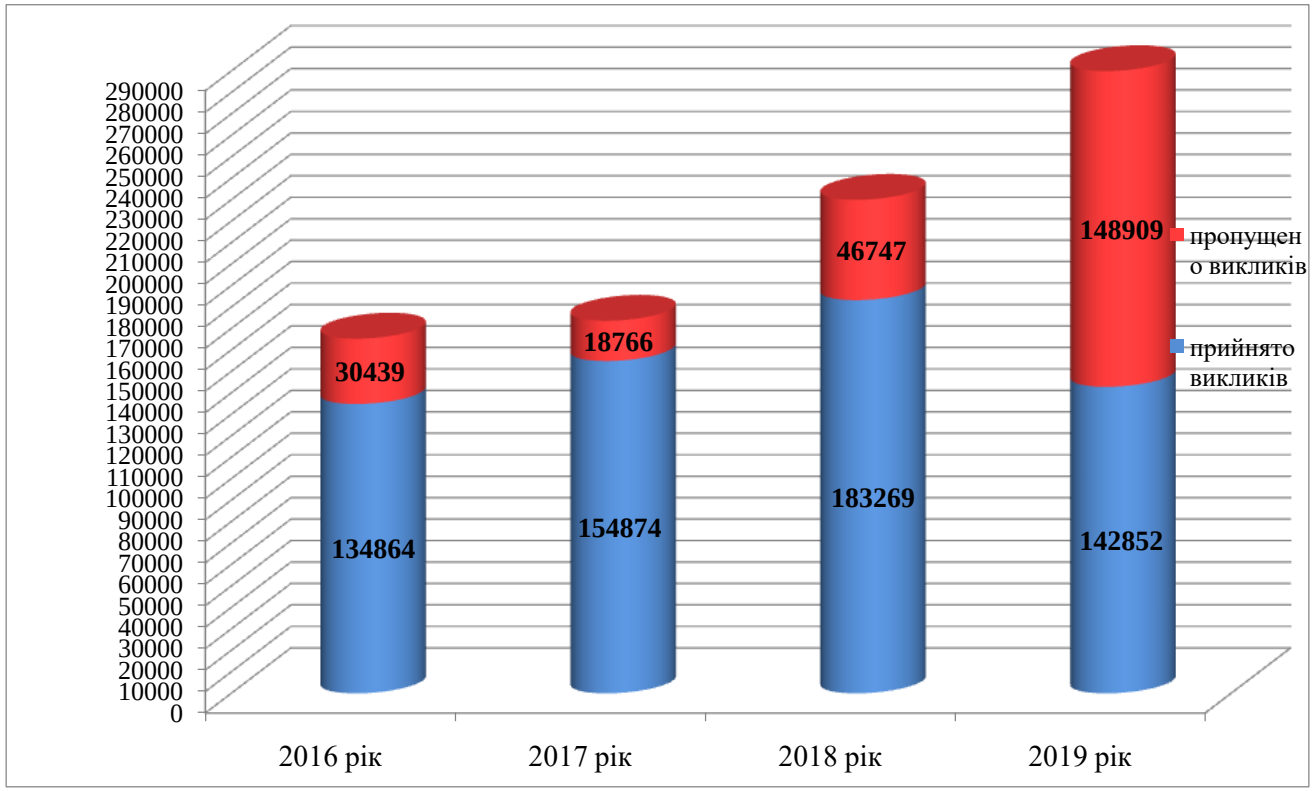
Додаток Ж

Діаграма 1.

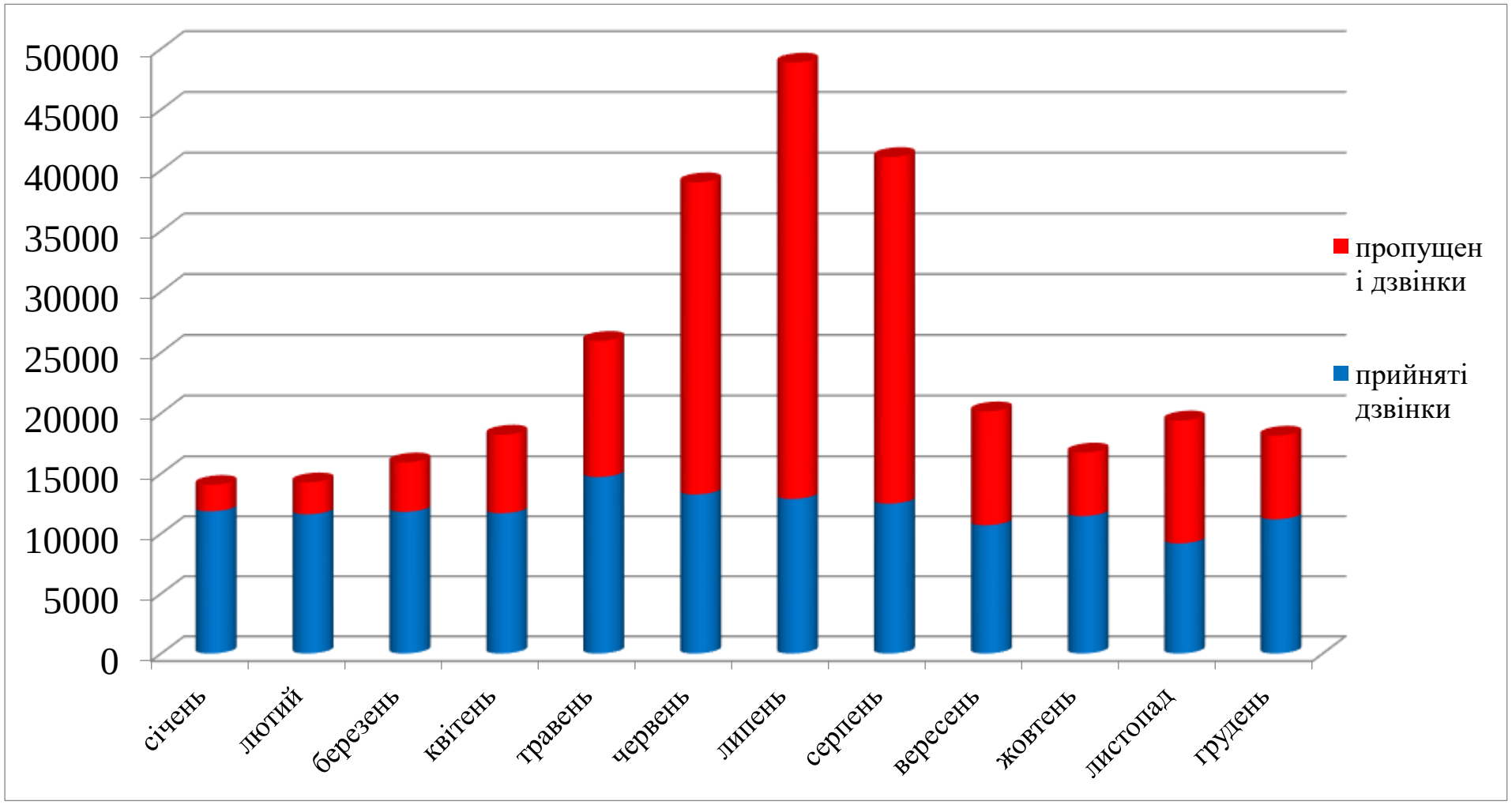
Відповідність перспективи збільшення рівень довіри громадян до ДПСУ заплановані Стратегією розвитку ДПСУ та реального стану



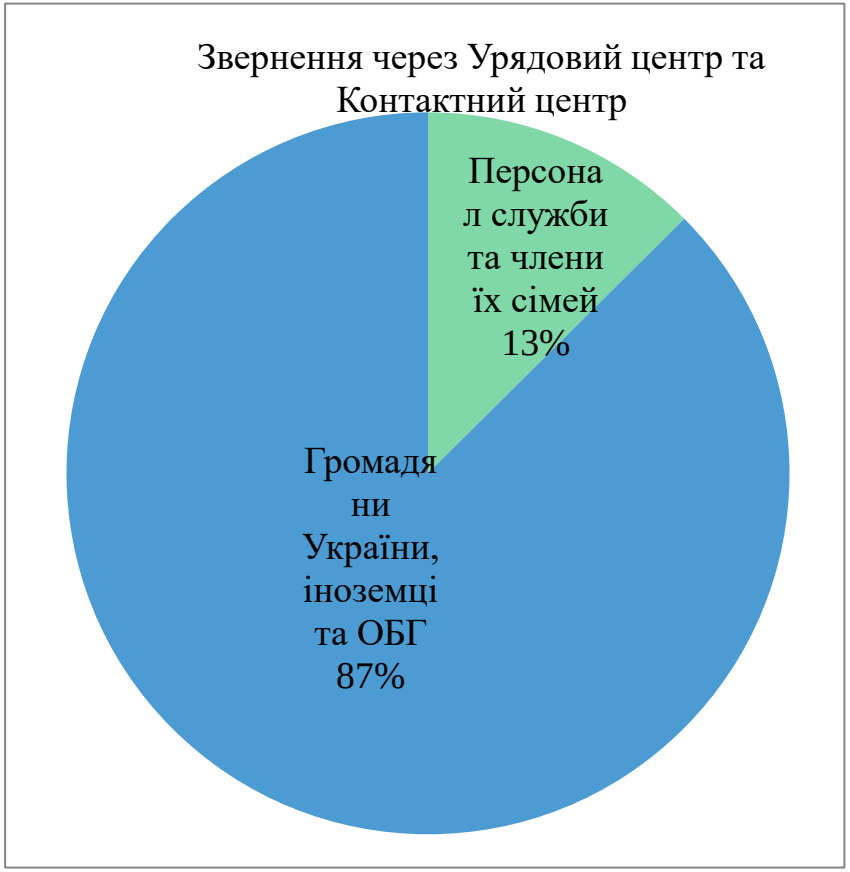
Діаграма 2.
Загальна кількість дзвінків, що надійшли на телефон служби «Довіра» (2016-2019 рр.)

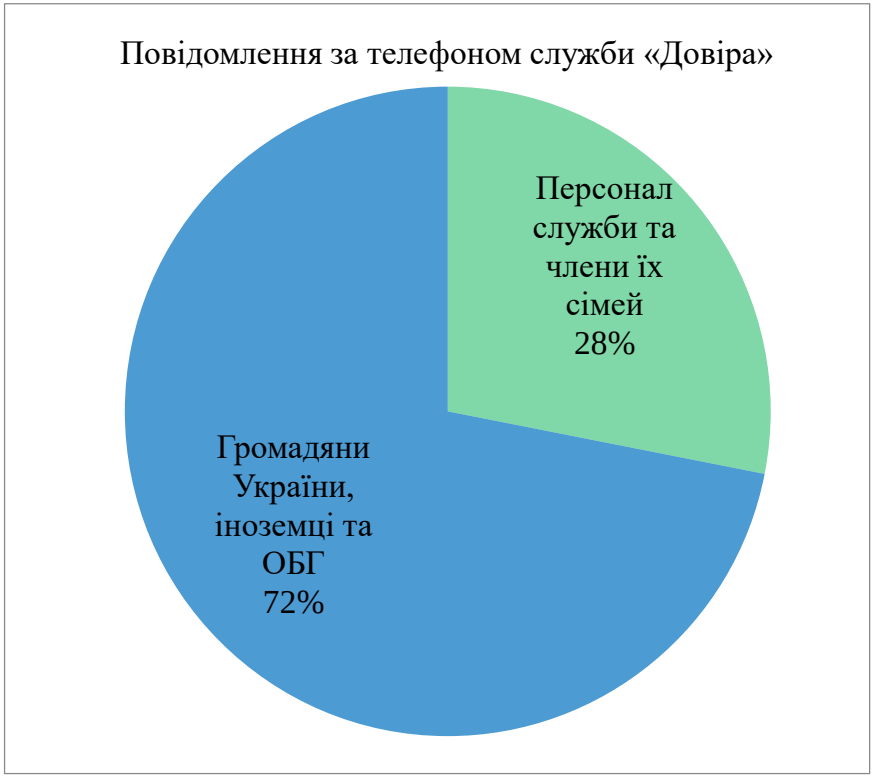


Діаграма 3.
Кількість дзвінків, що надійшли на телефон служби «Довіра»у 2019 році



Діаграма 4.
Звернення та повідомлення, що отримані від громадян України, іноземців та ОБГ і персоналу служби та членів їх сімей у 2019 році





У 2019 році кількість звернень від персоналу служби та членів їх сімей, у порівнянні з 2018 роком, зросла на 45 %

У 2019 році кількість повідомлень від персоналу служби та членів їх сімей, у порівнянні з 2018 роком, зросла на 36 %

Додаток И

Таблиця 1
Частина реєстру повідомлень FRONTEX відповідно до статей 25 Регламенту ЄС (ЄС) № 45/2001

№	Дата	Відділ	Підрозділ/сектор/офіс	Назва обробки	Призначення обробки	Суб'єкти даних	Категорії даних	Основна діяльність	Чи потрібна попередня консультація з EDPS?	Рішення EDPS
1	27.11.2009	АДМІН	HR	Процедури підбору персоналу	Підбір та оформлення персоналу	Персонал, SNE, стажери	Ім'я , прізвище, адреса, відомості про стан здоров'я,	ні	так	С 2009-0287
2	30.10.2009	АДМІН	HR	Дані про здоров'я на робочому місці	Перевірка працездатності; лікарняні листи	Персонал, SNE, стажери	Ім'я, прізвище, адреса, відомості про стан здоров'я	ні	так	С 2010-0071
3	21.06.2010	АДМІН	Послуги адміністрації	Відеоспостереження	Контроль доступу до приміщень Frontex; безпека персоналу та відвідувачів, безпека приміщень та IT-систем	Персонал, SNE, стажери. Підрядники, представники MS / SAC	Зображення та відео	ні	так	С 2006-0291
4	16.12.2010	АДМІН	Послуги адміністрації	Система контролю доступу за технологією сканування IRIS	Контроль доступу до приміщень Frontex; безпека персоналу та відвідувачів, безпека приміщень та IT-систем	Персонал, SNE, стажери. Підрядники, представники MS / SAC	Біометрика	ні	так	С 2010-1008
5	18.11.2010	OPD	JOU / ROS	Збір імен та інших даних повернених для спільних операцій з повернення	Організація спільних операцій з повернення	Повернені, посадові особи MS/SAC	Ім'я, прізвище, дата народження, дані про стан здоров'я	так	так	С 2009-0281
.....										

67	4.09.2019	не застосо-вується	MPR	Організація Міжнародного дня Frontex. Захід відбувається раз на рік.	Є дві цілі: 1. Обробка особистих даних учасників для реєстрації та безпеки (наприклад, доступ до місця проведення заходу, управління списком учасників) та 2. Обробка даних, фотографуваних осіб (тих, хто погодився сфотографуватися). Частина фотографій буде опублікована на Informer та / або на внутрішньому веб-сайті Frontex MyFX.	Персонал, SNE, громадські організації, стажери	Ім'я, Прізвище, Зображення, дані для зв'язку: тільки робоча електронна адреса.	ні	ні	не застосо-вується
68	21.10.2019	не застосо-вується	FRO	Відкритий конкурс для подання заявок на відбір громадських організацій для участі у Консультативному форумі Frontex (CF)	Метою цієї операції по обробці є вибір організацій громадянського суспільства для участі у CF	Представники громадських організацій	Ім'я, прізвище, Дані для зв'язку (обліковий запис електронної пошти, номер телефону, адреси робоча чи домашня).	так	ні	не застосо-вується
69	7.11.2019	КБР	ПРУ	Відеозапис презентації Закону «Про море», від 10 жовтня 2019 року.	Запис презентації, яку має винести експерт з морського права. Запис надалі буде використовуватися Агентством як матеріал для освітніх цілей.	З усього персоналу, буде зафіксований лише експерт, який проводить конференцію. Питання учасників також з'являться на кадрі.	Ім'я, прізвище, Особисте зображення від експерта буде записано на відео. Також відбудеться запис голосу від можливих учасників, які задають питання.	ні	ні	не застосо-вується

Джерело: FRONTEX REGISTER of NOTIFICATIONS pursuant to Articles 25 of EU Regulation (EC) No 45/2001. URL: https://frontex.europa.eu/assets/Data_Protection/Register_2020_01_22.xls (дата звернення: 23.11.2019).

Додаток К

Таблиця 1. Вид звернень громадян

	Адміністрація ДПСУ					Регіональні управління, органи охорони державного кордону та забезпечення				
	2014	**2015**	**2017**	**2018**	**2019**	**2014**	**2015**	**2017**	**2018**	**2019**
Всього надійшло звернень	7397	7698	18705	20162	19583	3446	2490 (57,1%)	6854	7472	9482
Заяви (клопотання)	7255 (98,1%)	7637 (9 9,2%)	18647 (99,7%)	20094 (99,7%)	19529 (99,7%)	3295 (95,6%)	363 (8,3%)	6230 (91,9%)	6895 (92,3%)	8767 (92,5%)
Скарги	142 (1,9%)	61 (0,8%)	58 (0,3%)	68 (0,3%)	54 (0,3%)	151 (4,4%)	1510 (34,6%)	624 (9,1%)	577 (7,7%)	715 (7,5%)

Таблиця 2. Характер звернень

	Адміністрація ДПСУ					Регіональні управління, органи охорони державного кордону та забезпечення				
	2014	**2015**	**2017**	**2018**	**2019**	**2014**	**2015**	**2017**	**2018**	**2019**
Усні (подані на особистому прийомі)	156	129	177	235	204	945	926	1098	595	562
Надіслані поштою	7241	7569	18528	19927	19379	–	3437	5756	6877	8920
Повторні звернення	198	198	77	134	88	66	103	169	201	137
Колективні звернення	66	66	40	52	34	29	26	42	33	30
Анонімні звернення	61	61	37	42	23	3	9	112	176	352
Звернення, що не належать до повноважень суб’єктів звернень	218	38	223	251	160	78	167	1246	1305	1674

Таблиця 3. Звернення громадян розглянуто

	Адміністрація ДПСУ					Регіональні управління, органи охорони державного кордону та забезпечення				
	2014	**2015**	**2017**	**2018**	**2019**	**2014**	**2015**	**2017**	**2018**	**2019**
Особисто керівником	1248 (16,9%)	364 (4,7%)	227 (1,2%)	601 (3,0%)	633 (3,2%)	1579 (45,8%)	2490 (57,1%)	4268 (62,3%)	4974 (66,6%)	6653 (70,2%)
Заступниками керівника	4829 (65,3%)	5706 (74,1%)	15270 (81,6%)	7174 (35,6%)	3891 (19,9%)	547 (15,9%)	363 (8,3%)	883 (12,9%)	988 (13,2%)	1187 (12,5%)
Начальниками управлінь (відділів)	1320 (17,8%)	1628 (21,2%)	3208 (17,2%)	12387 (61,4%)	15059 (76,9%)	1320 (38,3%)	1510 (34,6%)	1703 (24,8)	1510 (20,2)	1642 (17,3)

Таблиця 4. Звернення надійшли від

	Адміністрація ДПСУ					Регіональні управління, органи охорони державного кордону та забезпечення				
	2014	2015	2017	2018	2019	2014	2015	2017	2018	2019
Громадяни України	5406 (73,1%)	5518 (71,7%)	14539 (77,7%)	14539 (77,7%)	16101 (82,2%)	3312 (96,1%)	4172 (95,6%)	6462 (94,3%)	7005 (93,8%)	8823 (93,0%)
Іноземні громадяни та ОБГ	1991 (26 %)	2180 (28,3 %)	4166 (22,3%)	4166 (22,3%)	3482 (17,8%)	134 (3,9 %)	191 (4,4 %)	392 (5,7%)	467 (6,2%)	659 (7,0%)

Таблиця 5. Категорії заявників (з загальної кількості звернень)

	Адміністрація ДПСУ					Регіональні управління, органи охорони державного кордону та забезпечення				
	2014	**2015**	**2017**	**2018**	**2019**	**2014**	**2015**	**2017**	**2018**	**2019**
Герої України, Радянського Союзу, Соціалістичної Праці	156	129	0	0	0	945	926	0	0	0
учасники та інваліди Великої Вітчизняної війни	2	0	2	4	0	7 (0,2%)	3 (0,1%)	0	0	6
учасник бойових дій на території інших країн за часів СРСР	12 (0,2%)	8 (0,1%)	29	29	50 (0,3%)	30 (0,9%)	185 (4,2%)	33 (0,5%)	19	36 (0,4%)
учасник бойових дій, який брав безпосередню участь в АТО			26	24	94 (0,5%)			345 (5,0%)	463 (6,2%)	766 (8,1%)
ветеран військової служби ДПСУ			198 (1,1%)	169 (0,8%)	77 (0,4%)			323 (4,7%)	94 (1,3%)	163 (1,7%)
пенсіонер з числа військовослужбовців ДПСУ			338 (1,8%)	362 (1,8%)	809 (4,1%)			73 (1,1%)	163 (2,2%)	195 (2,1%)
Військовослужбовець запасу ПВ/ДПСУ			0	0	41			280 (4,1%)	685 (9,2%)	1050 (11,1%)
ветеран праці ДПСУ			0	3	1			0	18	4
пенсіонер ДПСУ	503 (6,8%)	457 (5,9%)	0	0	0	484 (14,0%)	479 (11,0%)	49 (0,7%)	80 (1,1%)	127 (1,3%)
державний службовець			2	1	1			6	5	11

ДПСУ										
працівник бюджетної сфери ДПСУ	6	4	5	4	2	6	4	98 (1,4%)	26 (0,3%)	62 (0,7%)
член сім'ї військовослужбовця ДПСУ	68 (0,9%)	120 (1,6%)	55 (0,3%)	30	26	225 (6,5%)	222 (5,1%)	335 (6,4%)	239 (3,2%)	239 (2,5%)
член сім'ї учасника бойових дій, який брав безпосередню участь в АТО			4	6	8			37 (0,5%)	53 (0,7%)	88 (0,9%)
військовослужбовці ДПСУ, з них:	59 (0,8%)	18 (0,2%)	33 (0,2%)	24	34	668 (19,4%)	586 (13,4%)	1956 (28,5%)	566 (7,6%)	550 (5,7%)
Офіцерський склад ДПСУ	5	5	16	12	13	199 (5,8%)	190 (4,3%)	1069 (15,6%)	158 (2,1%)	153 (1,6%)
Сержантський і старшинський склад ДПСУ	54 (0,7%)	13	17	12	18	469 (13,6%)	396 (9,1%)	866 (12,6%)	368 (4,9%)	364 (3,8%)
Рядовий склад ДПСУ	59 (0,8%)	18 (0,2%)	0	0	3			21 (0,3%)	40 (0,5%)	33 (0,3%)

Таблиця 6. Основні питання, які порушували громадяни у зверненнях

	Адміністрація ДПСУ					Регіональні управління, органи охорони державного кордону та забезпечення				
	2014	**2015**	**2017**	**2018**	**2019**	**2014**	**2015**	**2017**	**2018**	**2019**
Порядок перетинання державного кордону, не пропуск через державний кордон тощо	1085 (14,7%)	825 (10,7%)	1543 (8,2%)	1302 (6,4%)	1207 (6,1%)	920 (26,7%)	1423 (32,6%)	2237 (32,6%)	2622 (35,1%)	2975 (31,4%)
Фінансове забезпечення	272 (3,7%)	459 (5,9%)	308 (1,6%)	335 (1,7%)	549 (2,8%)	625 (18,2%)	535 (12,3%)	897 (13,1%)	744 (10,0%)	1157 (12,2%)
Порядок проходження служби, поновлення на службі, переведення по службі	271 (3,7%)	180 (2,3%)	148 (0,8%)	136 (0,7%)	168 (0,9%)	292 (8,5%)	358 (8,2%)	492 (7,2%)	402 (5,4%)	496 (5,2%)
Виділення санаторно-курортних путівок на лікування	220 (3,0%)	164 (2,1%)	249 (1,3%)	225 (1,1%)	246 (1,2%)	43 (1,2%)	11 (0,3%)	66 (1,0%)	38 (0,5%)	52 (0,5%)
Отримання житла, поновлення в черзі на його отримання	80 (1,1%)	74 (1,0%)	85 (0,5%)	98 (0,5%)	148 (0,8%)	225 (6,5%)	233 (5,3%)	218 (3,2%)	222 (3,0%)	229 (2,4%)
Неправомірні дії посадових осіб	16 (0,2%)	17 (0,2%)	30 (0,2%)	20 (0,1%)	14 (0,1%)	105 (3,0%)	96 (2,2%)	197 (2,9%)	210 (2,8%)	298 (3,1%)

Неправомірні дії прикордонників	11 (0,1%)	9 (0,1%)	7	4	2	70 (2,0%)	216 (5,0%)	329 (4,8%)	286 (3,8%)	265 (2,8%)
Надання інформації про перетинання кордону	3064 (41,4%)	3852 (50,0%)	7476 (40,0%)	9633 (47,8%)	8661 (44,2%)	—	—	—	—	—
Тимчасове обмеження права виїзду за межі України	1887 (25,5%)	1894 (24,6%)	8494 (45,4%)	8081 (40,1%)	8282 (42,3%)	—	—	—	—	—
Інші питання	472 (6,3%)	202 (2,7%)	365 (2,0%)	328 (1,6%)	285 (1,5%)	1166 (33,9%)	1491 (34,1%)	2418 (35,2%)	2948 (39,4%)	4010 (42,4%)

Таблиця 7. Структурними підрозділами Державної прикордонної служби України за напрямами службової діяльності розглянуто звернень

	Адміністрація ДПСУ					Регіональні управління, органи охорони державного кордону та забезпечення				
	2014	**2015**	**2017**	**2018**	**2019**	**2014**	**2015**	**2017**	**2018**	**2019**
Департамент охорони державного кордону (штаб)	6078 (82,3%)	6525 (84,7%)	1640 (8,8%)	1769 (8,8%)	1467 (7,5%)	1175 (34,1%)	1175 (34,1%)	1467 (21,4%)	2060 (27,6%)	2290 (24,2%)
Управління (відділ) кадрового менеджменту	218 (2,9%)	170 (2,2%)	178 (1,0%)	122 (0,6%)	147 (0,8%)	407 (11,8%)	407 (11,8%)	614 (9,0%)	606 (8,1%)	897 (9,5%)
Управління охорони здоров'я (мед. служба)	247 (3,3%)	192 (2,5%)	308 (1,6%)	267 (1,3%)	283 (1,4%)	60 (1,7%)	60 (1,7%)	227 (3,3%)	147 (2,0%)	267 (2,8%)
Управління (відділ) тилового забезпечення	87 (1,2 %)	78 (1,0 %)	105 (0,6 %)	91 (0,5 %)	117 (0,6 %)	498 (14,4%)	487 (11,2%)	650 (9,5%)	591 (7,9%)	668 (7,0%)
Управління (відділ) озброєння та інженерно-технічного забезпечення	-	-	1	8	6	-	-	12	16	15
Фінансово-економічне (відділ) управління	275 (3,7%)	462 (6,0%)	324 (1,7%)	343 (1,7%)	543 (2,8%)	630 (18,3%)	582 (13,3%)	795 (11,6%)	819 (11,0%)	1460 (15,4%)

Управління (відділ) соціально-гуманітарного забезпечення	85 (1,1%)	29 (0,4%)	70 (0,4%)	75 (0,4%)	49 (0,3%)	149 (4,3%)	304 (7,0%)	564 (8,2%)	214 (2,9%)	153 (1,6%)
Управління юридичного забезпечення (юридична служба)	21 (0,3%)	5 (0,1%)	25 (0,1%)	20 (0,1%)	33 (0,2%)	179 (5,2%)	166 (3,8%)	565 (8,2%)	127 (1,7%)	147 (1,6%)
Головний центр обробки спеціальної інформації			15927 (85,1%)	17300 (85,8%)	16759 (85,6%)			——	——	——
Інші структурні підрозділи	386 (5,2%)	237 (3,1%)	127 (0,7%)	167 (0,8%)	1797 (0,9%)	331 (9,7%)	437 (10,1%)	1972 (28,8%)	2892 (38,6%)	3585 (37,7%)

Таблиця 8. На звернення громадян відповідь надано у термін

	Адміністрація ДПСУ					**Регіональні управління, органи охорони державного кордону та забезпечення**				
	2014	**2015**	**2017**	**2018**	**2019**	**2014**	**2015**	**2017**	**2018**	**2019**
До 15 днів	3225 (93,6%)	6557 (85,2%)	17115 (91,4%)	19232 (95,4%)	18862 (96,3%)	3225 (93,6%)	3883 (89,0%)	5992 (87,4%)	6708 (89,8%)	8742 (92,2%)
У місячний термін	175 (5,1%)	961 (12,5%)	1245 (6,7%)	630 (3,1%)	351 (1,8%)	175 (5,1%)	372 (8,5%)	714 (10,4%)	594 (7,9%)	586 (6,2%)
До 45 днів	21 (0,6%)	32 (0,4%)	32 (0,2%)	16 (0,1%)	33 (0,2%)	21 (0,6%)	42 (1,0%)	60 (0,9%)	67 (0,9%)	51 (0,5%)
Перебуває у стадії розгляду	25 (0,7%)	148 (1,9%)	313 (1,7%)	284 (1,4%)	337 (1,7%)	25 (0,7%)	66 (1,5%)	88 (1,3%)	103 (1,4%)	103 (1,1%)

Таблиця 9. За результатами розгляду звернень громадян

	Адміністрація ДПСУ					Регіональні управління, органи охорони державного кордону та забезпечення				
	2014	**2015**	**2017**	**2018**	**2019**	**2014**	**2015**	**2017**	**2018**	**2019**
Перебуває у стадії розгляду	127 (1,7%)	148 (1,9%)	313 (1,7%)	284 (1,4%)	337 (1,7%)	25 (0,7%)	66 (1,5%)	88 (1,3%)	103 (1,4%)	103 (1,1%)
Надано роз'яснення	2575 (34,8%)	2088 (27,1%)	3905 (20,9%)	4073 (20,2%)	4456 (22,8%)	1432 (41,6%)	2180 (50,0%)	1945 (28,4%)	2603 (34,8%)	3173 (33,5%)
Вирішено позитивно	3996 (62,4%)	4568 (59,4%)	9299 (49,7%)	13050 (64,7%)	13466 (68,8%)	1732 (50,3%)	1761 (40,4%)	2593 (37,8%)	2588 (34,6%)	3378 (35,6%)
Відмовлено у задоволенні вимог	481 (6,6%)	652 (8,5%)	4873 (26,0%)	2385 (11,8%)	1013 (5,2%)	179 (5,2%)	189 (4,3%)	294 (4,3%)	260 (3,5%)	163 (1,7%)
Звернення, що повернуто авторові відповідно до статей 5 і 7 Закону України «Про звернення громадян»	–	–	50 (0,3%)	71 (0,4%)	123 (0,6%)	–	–	640 (9,3%)	464 (6,2%)	666 (7,0%)
Звернення, що не підлягає розгляду відповідно до статей 8 і 17 Закону України «Про звернення громадян»	–	–	42 (0,2%)	48 (0,2%)	28 (0,1%)	–	–	48 (0,7%)	149 (2,0%)	325 (3,4%)
Надіслано на розгляд за належністю іншому органу влади, установі тощо	38 (0,5%)	31 (0,4%)	223 (1,2%)	251 (1,3%)	160 (0,8%)	78 (2,3%)	167 (3,8%)	1246 (18,2%)	1305 (17,5%)	1674 (17,7%)

Таблиця 10. У регіональні управління, органи охорони державного кордону та забезпечення Державної прикордонної служби України надійшло

Регіональні управління, органи охорони державного кордону та забезпечення Державної прикордонної служби України	Кількість звернень				
	2014	2015	2017	2018	2019
Північне регіональне управління	819 (23,8%)	1254 (28,7%)	519 (7,6%)	570 (7,6%)	766 (8,1%)
Східне регіональне управління	420 (12,2%)	624 (14,3%)	876 (12,8%)	797 (10,7%)	1524 (16,1%)
Донецько-Луганське регіональне управління	–	–	–	336 (4,5%)	400 (4,2%)
Азово-Чорноморське регіональне управління	74 (2,1%)	218 (5,0%)	280 (4,1%)	290 (3,9%)	312 (3,3%)
Південне регіональне управління	613 (17,8%)	780 (17,9%)	878 (12,8%)	818 (10,9%)	858 (9,0%)
Західне регіональне управління	702 (20,4%)	780 (17,9%)	1070 (15,6%)	1406 (18,8%)	1754 (18,5%)
НАДПСУ	64 (1,9%)	102 (2,3%)	112 (1,6%)	131 (1,8%)	139 (1,5%)
ОКПП “Київ”	114 (3,3%)	155 (3,6%)	255 (3,7%)	386 (5,1%)	339 (3,6%)
Головний центр підготовки особового складу ДПСУ ім. генерал-майора Ігоря Момота	170 (4,9%)	130 (3,0%)	58 (0,8%)	104 (1,4%)	123 (1,3%)
Мобільний прикордонний загін	0	3	7	12	16
Головний центр зв’язку, автоматизації та захисту інформації	2	3	5	23 (0,3%)	20 (0,3%)
Окрема комендатура охорони і забезпечення	420 (12,2%)	253 (5,8%)	410 (6,0%)	49 (0,7%)	24 (0,3%)
Центральна база зберігання та постачання	11	9	6	4	4
Головний військово-медичний клінічний центр	18	13	23	31 (0,4%)	62 (0,6%)
Центральна військово-лікарська комісія	19	39 (0,9%)	87 (1,3%)	97 (1,3%)	82 (0,9%)
Контактний центр ДПСУ	–	–	2268 (33,1%)	2418 (32,4%)	3053 (32,2%)

Джерело: Статистика звернень громадян до ДПСУ URL: https://dpsu.gov.ua/ua/stan-roboti-zi-zvernennyami-gromadyan-u-2018-roci/ (дата звернення: 27.01.2020).

Додаток Л

Діаграма 1

Кількість опрацьованих запитів з питань публічної інформації в Адміністрації Державної прикордонної служби України

Джерело: Державна прикордонна служба України. Публічна інформація. Звіти. URL: https://dpsu.gov.ua/ua/zviti/ (дата звернення: 16.01.2020).

Додаток М

Таблиця 1
Систематизована таблиця порушень інформаційного законодавства за які передбачена відповідальність у КК України та КУпАП

КК УКРАЇНИ		
Група правопорушень	***Стаття***	***Примітка***
Завідомо неправдива інформація	ст. 259 «Завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об’єктів власності»	Застосування завідомо неправдивої інформації становить не явну, а приховану загрозу безпеці інформаційних систем
	ст. 358 «Підроблення документів, печаток, штампів та бланків, збут чи використання підроблених документів, печаток, штампів»	
	ст. 359 «Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації»	
	ст. 366 «Службове підроблення»	
	ст. 383 «Завідомо неправдиве повідомлення про вчинення злочину»	
Злочини, в яких інформація (інформаційна зброя) виступає знаряддям їх вчинення, злочини, де засобом досягнення суспільно-небезпечної (шкідливої) мети є обман	ст. 161 «Порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками» (кваліфікуюча ознака вчинення службовою особою)	становлять найчисельнішу групу

	ст. 191 «Привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем»	
	ст. 192 «Заподіяння майнової шкоди шляхом обману або зловживання довірою», за відсутності ознак шахрайства	
	ст. 262 «Викрадення, привласнення, вимагання вогнепальної зброї, бойових припасів, вибухових речовин чи радіоактивних матеріалів або заволодіння ними шляхом шахрайства або зловживання службовим становищем»	
	ст. 357 «Викрадення, привласнення, вимагання документів, штампів, печаток, заволодіння ними шляхом шахрайства чи зловживання службовим становищем або їх пошкодження»	
	ст. 364 «Зловживання владою або службовим становищем»	
	ст. 369-2 «Зловживання впливом»	
	ст. 410 «Викрадення, привласнення, вимагання військовослужбовцем зброї, бойових припасів, вибухових або інших бойових речовин, засобів пересування, військової та спеціальної техніки чи іншого військового майна, а також заволодіння ними шляхом шахрайства або зловживання службовим становищем»	

Приховуванні або неподанні інформації	ст. 285 «Неповідомлення капітаном назви свого судна при зіткненні суден»	Мова йде про неповідомлення тій чи іншій інформаційній системі (яка виступатиме мішенню як впливу, так і злочинного посягання) тієї інформації, що є необхідною для її нормальної життєдіяльності (функціонування), тобто відсутність правомірного інформаційного впливу, не лише нешкідливого, але й необхідного для інформаційної системи, зумовлена, у свою чергу, протиправними діями винного
	ст. 396 «Приховування злочину»	
	ст. 426 «Бездіяльність військової влади»	
	ст. 136 «Ненадання допомоги особі, яка перебуває в небезпечному для життя стані»	
	ст. 385 «Відмова свідка від давання показань або відмова експерта чи перекладача від виконання покладених на них обов'язків»	
Погроза	ст. 129 «Погроза вбивством»	передбачено в усіх злочинах, які визначаються в диспозиції відповідних статей як такі, що вчиняються за допомогою (шляхом) погрози або в яких діяння (обов'язкова ознака об'єктивної сторони) реалізується як погроза, має місце здійснення інформаційного впливу на обраного суб'єкта (мішень впливу), тобто потерпілого
	ст. 195 «Погроза знищення майна»	
	ст. 258 «Терористичний акт» (погроза вчинення терористичного акту)	
	ст. 266. «Погроза вчинити викрадання або використати радіоактивні матеріали» (з метою впливу на службові дії представників ДПСУ)	
	ст. 345 «Погроза або насильство щодо працівника правоохоронного органу»	
	ст. 350 «Погроза або насильство щодо службової особи чи громадянина, який виконує громадський обов'язок»	
	ст. 404 «Опір начальникові або примушування його до порушення службових обов'язків»	
	ст. 405 «Погроза або насильство щодо начальника»	

Порушення приватності	ст. 182 «Порушення недоторканності приватного життя»	
	ст. 367 «Службова недбалість»	
	ст. 425 «Недбале ставлення до військової служби»	
	ст. 145 «Незаконне розголошення лікарської таємниці»	
	ст. 163 «Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер»	
У сфері державної таємниці (заборонена інформація та інформаційні впливи, що завідомо призводять до злочинних наслідків)	ст. 111 «Державна зрада» (у разі вчинення цих дій громадянином України);	Заборона може стосуватися здійснення різноманітних дій, предметом (об'єктом) яких є інформація певного змісту. Зокрема, однієї, декількох дій чи комплексної інформаційної діяльності щодо створення або розповсюдження такої інформації. Фактично, саме в цій групі злочинів інформаційна зброя виявляє себе як така, тобто як зброя, що й констатує законодавець. Так само, як і для традиційної зброї, мова йде про обмеження обігу інформаційної зброї. При цьому для такого різновиду інформаційної зброї, який зараз розглядається, характерним є не просто обмеження участі в обігу, але й повна його заборона
	ст. 114 «Шпигунство» (якщо ці дії вчинені іноземцем або особою без громадянства)	
	ст. 328 «Розголошення державної таємниці»	
	ст. 329 «Втрата документів, що містять державну таємницю»	
	ст. 330 «Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни»	
	ст. 422 «Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості»	

У ІТ-сфері «комп'ютерні злочини»	ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»	
	ст. 361-1 «Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»	
	ст. 361-2 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації»	
	ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї»	несанкціоновані зміна, знищення або блокування інформації (ч. 1)
		несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації (ч. 2)

	ст. 363 «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється»	
	ст. 363-1 «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку»	умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів
КУпАП		
За вчинення інформаційних правопорушень, передбачених КУпАП, військовослужбовці несуть **дисциплінарну відповідальність**.	ст. 186-3 «Порушення порядку подання або використання даних державних статистичних спостережень»	
	ст. 188-39 «Порушення законодавства у сфері захисту персональних даних»	
	ст. 188-41 «Порушення законодавства про державну реєстрацію нормативно-правових актів»	
	ст. 212-2 «Порушення законодавства про державну таємницю»	містить дев'ять пунктів, більшість із яких встановлюють відповідальність за декілька різних адміністративних порушень у сфері інформаційної

		безпеки
	ст. 212-3 «Порушення права на інформацію та права на звернення»	встановлює відповідальність за сім різних адміністративних правопорушень у сфері обігу інформації
	ст. 212-6 «Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем»	
для військовослужбовців – посадових осіб ДПСУ за порушення інформаційного законодавства згідно зі статтею 15 може бути застосована **адміністративна відповідальність на загальних підставах**, за такими статтями КУпАП:	172-8 (незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових або інших визначених законом повноважень);	
	195-5 (незаконне зберігання спеціальних технічних засобів негласного отримання інформації);	
	212-2 (порушення законодавства про державну таємницю);	
	212-5 (порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію).	

Додаток Н

Пам’ятка

щодо забезпечення інформаційної безпеки при роботі в мережі Інтернет

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

ДЕПАРТАМЕНТ
КОНТРРОЗВІДУВАЛЬНОГО ЗАХИСТУ ІНТЕРЕСІВ ДЕРЖАВИ
У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ПАМ’ЯТКА
ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ РОБОТІ В МЕРЕЖІ ІНТЕРНЕТ

м. Київ
2019 рік

ЗМІСТ

І. ПЕРЕЛІК ОСНОВНИХ ЧИННИКІВ, ЩО ВПЛИВАЮТЬ НА СТАН ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЗВ'ЯЗКУ ІЗ ВИКОРИСТАННЯМ ЗАГАЛЬНОДОСТУПНИХ ТА СОЦІАЛЬНО ОРІЄНТОВАНИХ РЕСУРСІВ МЕРЕЖІ ІНТЕРНЕТ

• *Військова агресія Російської Федерації та пов'язані з нею масштабні кібератаки, масові антиукраїнські інформаційні кампанії та їх психологічний вплив на користувачів українського сегменту мережі Інтернет, отримання несанкціонованого доступу до персональних даних та іншої важливої інформації з електронних поштових скриньок та соціальних мереж: тощо.*

• *Існування загрози для державних установ (міністерств, відомств, агентств, фінансових установ тощо) у зв'язку із використанням працівниками у службовій діяльності та повсякденному житті програмного забезпечення російського виробництва, а також поштових електронних сервісів та соціальних мереж*

«ВКонтакте» та «Одноклассники», доступ до яких на даний час обмежено відповідно до Указу Президента України № 133/2017 від 15.05.2017 року.

• Підконтрольність найбільших та найвпливовіших медіа особам, котрі використовують дані ресурси для лобіювання та відстоювання особистих, а не державних інтересів.

• Активне наповнення соціальних мереж замовними дописами відповідного контенту із використанням т.зв. бот-мереж («ботів») та технології масового «тролінгу».

• Маніпуляції у засобах масової інформації та соціальних мережах з метою приваблення більшої аудиторії шляхом використання методів соціальної інженерії.

• Використання соціальних мереж для поширення недостовірної (фейкової), викривленої, деструктивної інформації та здійснення маніпулятивного впливу на суспільну свідомість користувачів українського сегменту мережі Інтернет.

ІІ. ХАРАКТЕРИСТИКА КЛЮЧОВИХ ФАКТОРІВ РИЗИКУ ТА РЕКОМЕНДАЦІЇ ЩОДО ЇХ НЕЙТРАЛІЗАЦІЇ

1. Зберігання та передача даних

Недотримання окремих правил безпеки під час здійснення службових обов'язків працівниками органів виконавчої влади та місцевого самоврядування, посадовими особами державних підприємств, установ, організацій, а також військовослужбовцями може призвести до втрати чи крадіжки мобільних телефонів, персональних ноутбуків, магнітних носіїв інформації тощо. Вказане ставить під загрозу збереження персональних даних та може призвести до розголошення інформації з обмеженим доступом.

➢ З метою уникнення негативних наслідків у випадку втрати або викрадення носіїв інформації необхідно:

• встановити паролі на усі пристрої, що перебувають у користуванні (PIN-коди, паролі на вхід до всіх облікових записів, паролі на планшетах та ноутбуках тощо);

• систематично робити резервне копіювання важливих файлів;

• блокувати пристрої щоразу після закінчення роботи з ними.

2. Соціальні мережі

Соціальні мережі у наш час стали зручним та ефективним засобом комунікації. За допомогою соціальних медіа можна обмінюватись повідомленнями, публікувати особисті фото- та відеоматеріали, розміщувати інформацію про місце роботи і відпочинку, колег, друзів, навчання, дозвілля, політичні погляди тощо. Така кількість приватної інформації у разі її потрапляння до зацікавлених осіб може поставити під загрозу як службову діяльність так і приватне життя державних службовців, керівників підприємств, установи, організації, установ державної влади та місцевого самоврядування, а також військовослужбовців.

➢ ***З метою уникнення несанкціонованого доступу до персональних акаунтів, зареєстрованих у соціально орієнтованих ресурсах мережі Інтернет,***

необхідно:

• встановити надійний пароль для входу в обліковий запис. При цьому рівень захищеності акаунту та інформації, що знаходиться у ньому, залежить від складності встановленого паролю;

• використовувати функцію подвійної авторизації. Щоб увійти до профілю з незнайомого пристрою, сервіс вимагатиме пройти додаткову ідентифікацію як власника акаунту. При цьому на вказаний номер телефону або на поштову скриньку буде надіслано повідомлення з кодом підтвердоісення, або необхідно буде ввести один із паролів, які попередньо були збережені через інший обраний спосіб підтвердоісення;

• здійснити додаткові налаштування профілю в соціальних мережах з метою отримання інформації щодо несанкціонованих входів до ресурсів з невідомого пристрою або Інтернет- браузера;

• при створенні акаунтів у соціальних мережах використовувати у якості «логіна» поштову адресу надійного сервісу (наприклад, «Google», «Yahoo») або українських поштових сервісів. Не рекомендується користуватися російськими сервісами, доступ до яких заборонено в Україні, оскільки через персональну електронну скриньку можна отримати пароль, а відтак доступ до профілів, зареєстрованих у соціальних мережах;

*• **не здійснювати** авторизацію особистих чи робочих, корпоративних профілів з незнайомих чи незахищених пристроїв. Існує ймовірність, що після завершення роботи не буде здійснено вихід із свого облікового запису або пристрій запам ’ятає вказаний при вході логін та пароль. Крім того, існує ймовірність ураження такого пристрою шкідливим програмним забезпеченням, що може здійснювати збір та передачу відомостей щодо паролів та логінів зацікавленим особам;*

*• **пам’ятайте**, що саме фішинг (довідково: **фішинг** - вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі Інтернет персональних даних клієнтів, сервісів із переказу або обміну валюти, Інтернет-магазинів) є найпоширенішим способом отримання зловмисниками паролів до поштових скриньок та сторінок у соціальних мережах.*

Крім того, у ході гібридної агресії з боку РФ соціальні мережі активно використовуються для збору додаткових відомостей щодо місць регулярного перебування особи, її родичів, колег, особистих уподобань та іншої приватної інформації. Водночас, через соцмережі здійснюється збір та передача інформації щодо місць дислокації та складу окремих підрозділів Збройних сил України, які залучені до проведення операції об’єднаних сил на сході України, яка частково є конфіденційною.

➢ ***З метою недопущення отримання зацікавленими особами додаткової (приватної) інформації щодо особи, членів її сім’ї, колег, уподобань тощо, стосовно військовослужбовців - інформації щодо місць дислокації та складу окремих підрозділів Збройних сил України, які залучені до проведення операції***

об'єднаних сил на сході України, необхідно дотримуватись наступних правил:

• ***не публікувати*** *у соціальних мережах інформацію, що може поставити під загрозу особисте життя особи, життя членів її сім 'ї та інших осіб*

• *військовослужбовцям та членам їх сімей не варто публікувати фото- та відеоматеріали, за допомогою яких можна визначити місцезнаходження військової частини окремих збройних військових формувань, що беруть участь у проведенні операції об'єднаних сил на сході України. Вказані дії можуть загрожувати життю та здоров'ю людей;*

• *обмежити доступ до приватної інформації в налаштуваннях конфіденційності соціальної мережі. Вибрати налаштування, які найбільше захищають додаткові відомості про власника акаунта. Зокрема, не зазначати геолокацію (місце розташування) та доступність пошуку акаунта в соціальній мережі за номером мобільного телефону та адресою поштової скриньки;*

• *періодично переглядати список друзів у соціальній мережі. Якщо серед них є незнайомі або підозрілі люди (акаунти), необхідно їх видалити, оскільки статус «друга» відкриває доступ до більшого обсягу приватної інформації про особу. В подальшому необхідно бути уважними під час додавання до списку «друзів» нових користувачів;*

• ***не рекомендується*** *використовувати російські соціальні мережі, «ВКонтакте» та «Одноклассники» доступ до яких заборонено, оскільки останні на вимогу спецслужб РФ можуть передавати відомості щодо персональних даних власників акаунтів (е-таіі, номер мобільного телефону, дата та IP-адреса реєстрації, дата та IP-адреса останнього відвідування тощо).*

• *військовослужбовцям* ***не використовувати*** *російських мобільних додатків «ДМБ Таймер», «ДМБ», «ДМБ Таймер +», «Дембель» та інших, під час реєстрації в яких вказуються власні персональні дані та військовий підрозділ, в якому проходять військову службу, а також дані товаришів по службі.*

Зазначені додатки отримують автоматичний доступ до геолокації, особистих контактів, фотографій, мультмедіа, файлів й документів, дозволяють читати, змінювати чи видаляти вміст на карті SD, переглядати мережеві з'єднання та отримувати повний доступ до мережі.

3. Використання російських соціально орієнтованих ресурсів мережі Інтернет

З 2016 року усі російські сервіси відповідно до федеральних законів РФ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» від 05.05.2014 року № 97-ФЗ, «О внесении изменений в Федеральный закон «О противодействии терроризму» від 06.07.2016 року № 374-ФЗ, «О внесении изменений в Уголовный кодекс РФ и Уголовно-процессуальный кодекс РФ в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» від 06.07.2016 року № 375-ФЗ та інших окремих законодавчих актів на постійній основі

надають спецслужбам РФ відомості щодо персональних даних користувачів та їх особистого листування. Зважаючи на це, українські Інтернет-провайдери зобов'язані обмежити доступ користувачам до російських соціальних мереж та сервісів.

Крім того, слід пам'ятати, що доступ до російських соціальних мереж «ВКонтакте» та «Одноклассники» на території України заборонено рішенням Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», введеного в дію Указом Президента України від 15.04.2017 року № 133.

➢ ***Головна порада – перехід на західні та українські сервіси, такі як «Gmail», «Googlet», «Facebook», «Twitter», «Ukr.net» тощо.***

4. Використання додатків до смартфонів

Під час встановлення тих чи інших додатків на власний телефон ці програмні продукти можуть вимагати доступу до певної інформації на використовуваному пристрої, насамперед геолокації, списку контактів, акаунтів у соціальних мережах та поштових скриньок.

За наявними даними, більшість шпигунських програм «вшиваються» саме в мобільні додатки, які цікавлять конкретну аудиторію. Тому необхідно бути уважним під час встановлення додатків, особливо якщо робити це з невідомих та неперевірених сервісів.

➢ ***З метою унеможливлення завантаження на особистий пристрій програм- шпигунів необхідно дотримуватись таких правил:***

• *встановлювати додатки лише з офіційних та перевірених сервісів (Chrome Store, Addons та Play Market для Android, App Store для OS);*

• ***заборонити*** *операційній системі смартфона (планшета, ПЕОМ) автоматично встановлювати додатки з невідомих джерел шляхом здійснення відповідних налаштувань пристрою;*

• *періодично здійснювати чистку усіх особистих пристроїв від додатків, які не використовуються.*

5. Електронне листування

Електронні поштові скриньки зберігають не тільки величезний обсяг особистих та робочих даних (листів), але й зазвичай прикріплені до акаунтів у соціальних мережах, месенджерах, хмарних сервісах тощо. Тому несанкціонований доступ до поштової скриньки може мати серйозні наслідки, такі як отримання інформації конфіденційного характеру, зміна паролів до сайтів, акаунтів без відома їх власників, отримання доступу до особистих фотографій та відео, розсилання спаму від імені інших осіб тощо.

➢ ***Щоб уникнути зламу електронної поштової скриньки, необхідно:***

• *увімкнути двофакторну автентифікацію за допомогою мобільного пристрою. В такому випадку під час спроби отримання паролю до поштової скриньки сторонніми особами буде надходити попередоісення на мобільний телефон у вигляді SMS-повідомлення про спробу злому;*

• встановити надійний пароль;

*• **не використовувати** для відновлення паролю російські сервіси («Yandex.ru», «Mail.ru» тощо);*

*• **не запускати** на пристроях вкладення підозрілих листів, що містять виконуваний файл з такими розширеннями як «.exe», «.bat», «.cmd», «.vbs», «.docm», «.xlsm» тощо;*

• державні службовці та військовослужбовці повинні пам'ятати, що службові електронні скриньки не слід використовувати для приватного листування.

6. Вихід до мережі Інтернет

Одним із найпоширеніших способів входу до мережі Інтернет у публічних місцях є підключення до відкритих точок Wi-Fi. Зазвичай вони є безплатними та вхід до них здійснюється без введення паролів. Саме відсутність паролю робить їх вразливішими для злому з боку зацікавлених осіб, які мають на меті отримати доступ до персональних даних та відомостей, що зберігаються на телефоні, планшеті, ПЕОМ тощо.

➢ ***Щоб уникнути перехоплення даних сторонніми особами, необхідно:***

• під час здійснення входу до мережі використовувати лише ті точки доступу до Wi-Fi, які мають протоколи безпеки для захисту бездротового з 'єднання WPA чи WPA-2;

• у публічних місцях найкраще користуватись особистим Wi-Fi модемом або здійснювати вхід до мережі Інтернет з мобільного пристрою за передплаченим пакетом послуг мобільного оператора;

• на ПЕОМ, мобільних пристроях та планшетах необхідно вимкнути функцію «Автоматичне підключення до Wi-Fi»;

• військовослужбовцям, які виконують завдання в зоні проведення ООС, обмежити використання особистих модемів чи роутерів для входу до мережі Інтернет через передачу сигналу, який можна зафіксувати спеціальною технікою та визначити місцезнаходження.

7. Перелік російських веб-ресурсів, якими не рекомендовано користуватись:

Указом Президента України від 15.05.2017 року № 133/2017 введено у дію рішення РНБО щодо обмеження діяльності в Україні російських соціальних мереж та сервісів. У переліку російських компаній, щодо яких вжито санкційні заходи, зазначено сервіси «Mail.Ru Group» та «Яндекс». Повний перелік ресурсів з Додатку до Указу, доступ до яких повинні заборонити Інтернет-провайдери:

1. afisha.yandex.ru;
2. audience.yandex.ru;
3. auto.ru;
4. avia.yandex.ru;
5. brouser.yandex.ru;

27. rasp.yandex.ru;
28. realty.yandex.ru;
29.speech kit.yandex.ru;
ЗО. sprav.yandex.ru;
31. stat.yandex.ru;

6. calendar.yandex.ru;
7. delivery.yandex.ru/promo;
8. direct.yandex.ru;
9. disk.yandex.ru;
10. dns.yandex.ru;
11. fotki.yandex.ru;
12. kassa.yandex.ru;
13. ail.yandex.ru;
14. market.yandex.ru;
15. metrika.yandex.ru;
16. metro.yandex.ru;
17. money.yandex.ru;
18. money.yandex.ru/card2card;
19. money.yandex.ru/new;
20. money.yandex.ru/newcard;
21. music.yandex.ua;
22. yandex.ru/pogoda/moscov;
23. news.yandex.ru;
24. partner.yandex.ru;
25. pdd.yandex.ru;
26. yandexdatafactory.com/ru;
32. taxi.yandex.ru;
33. tech.yandex.ru;
34. telephony.yandex.ru;
35. translate.yandex.ru;
36. travel.yandex.ru;
37. tv.yandex.ru;
38. webmaster.yandex.ru;
39. www.kinopoisk.ru;
40. xml.yandex.ru;
41. yandex.ru;
42. yandex.ru/adv?from=all;
43. yandex.ru/blog;
44. yandex.ru/images;
45. yandex.ru/intemet;
46. yandex.ru/maps;
47. yandex.ru/people;
48. n.maps.yandex.ru;
49. yandex.ru/suvenirka;
50. yandex.ru/time;
51. yandex.ru/yaca;
52. abota.yandex.ru.

Крім того, з огляду на введення в дію у Російській Федерації «антитерористичного» закону від 01.08.2014 року, що надав право спеціальним службам отримувати особисті дані користувачів Інтернет-ресурсів, сервери яких знаходяться на території РФ, не рекомендовано користуватись наступними Інтернет-ресурсами:

1. Автокадабра - autokadabra.ru;
2. БебиБлог - babyblog.ru;
3. Блоги@тai1.Ки - blogs.mail.ru;
4. Блогус - blogus.ru/blog.php;
5. Вебкруг - webkrug.ru;
6. Дневник на TKS.RU - blogs.tks.ru/portal.php;
7. За Баранкой - zabarankoi.ru;
8. Карта для любителей рыбалки - fishingmap.ru;
9. Клерк.ги - klerk.ru;
10. ЛИМП - limpa.ru;
11. Мой Круг - moikrug.ru;
12. Моя живая страница - mylivepage.ru;
13. Отдохнули.ру - otdohnuli.ru;
14. Привет.ру - privet.ru;

15. Рыбловный клуб - fion.ru;
16. Сообщество влюбленных в кино - ilovecinema.ru;
17. Соседи-Онлайн - sosedi-online.ru;
18. Тейст - mmm-tasty.ru;
19. Факультет.ру - facultet.ru;
20. Фотострана - fotostrana.ru;
21. Юмама - u-mama.ru;
22. Я талант - yatalant.ru;
23. Beon.ru - beon.ru;
24. Diary.ru - diary.ru;
25. Dogster - dogster.ru;
26. ITBlogs - itblogs.ru;
27. Liveintemet - liveintemet.ru;
28. LiveLib - livelibe.ru;
29. LJ.Rossia.org-lj.rossia.org;
30. MirTesen.ru-mirtesen.ru;
31. Re:vision - revision.ru;
32. RuSpace - ruspace.ru;
33. Spaces.ru - spaces.ru;
34. Telefoner.ru - telefoner.ru;
35. TooDoo-toodoo.ru;
36. VeniVidi-venividi.ru;
37. 100 Друзей - 100druzei.ru.

8. Рекомендації посадовій особі органу виконавчої влади, місцевого самоврядування, представникам міністерств та відомств:

• прес-службам державних органів під час суспільно-політичних подій в країні необхідно надавати коментарі та роз'яснення рішень на випередження, щоб уникнути інтерпретацій та викривлень у ході обговорення тієї чи іншої ситуації в загальнодоступних та соціально орієнтованих ресурсах мережі Інтернет;

• державним органам, установам необхідно розробити та затвердити чіткий план дій для оприлюднення представниками їхніх прес-служб інформації у випадку виникнення резонансних інцидентів;

• офіційні представники органів державної влади повинні оприлюднювати суспільно значущу інформацію, якщо вона не належить до тієї категорії, що не підлягає оприлюдненню. Не варто забувати, що приховування такої інформації від суспільства може знизити довіру до них;

• представникам органів державної влади під час надання коментарів, інтерв'ю, брифінгів не рекомендується використовувати оціночні судження, що можуть призвести до неоднозначного тлумачення наданої інформації її споживачами;

• органам державної влади необхідно розробити правила використання офіційній сторінок та акаунтів у соціальних мережах для уникнення непорозумінь з користувачами та окреслення формату комунікації через соціальні мережі. Крім того, вважається за доцільне здійснити верифікацію (довідково: ***верифікація*** *- це офіційне підтвердження походження сторінки, її офіційного власника (фізичної, юридичної особи) автентичності викладеної інформації через службу технічної підтримки) офіційних представництв органів державної влади та установ, які у своїй діяльності використовують акаунти у соціальній мережах, насамперед «Facebook», «Twitter», «Google+» та канали у відеохостингу «Youtube»;*

• держслужбовцям та військовослужбовцям, а також іншим особам, які відповідно до своїх функціональних обов'язків працюють з інформацією з обмеженим доступом, необхідно пам 'ятати, що під час оформлення допуску до державної таємниці при заповненні відповідних анкет вони повинні вносити достовірні дані про свої контакти з іноземними громадянами, наявність власних електронних скриньок, сайтів, профілів у соціальних мережах та тематичних форумах.

ІІІ. ВИТЯГ З КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ

1. Злочини проти основ національної безпеки України

Стаття 109. Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади

1. Дії, вчинені з метою насильницької зміни чи повалення конституційного ладу або на захоплення державної влади, а також змова про вчинення таких дій, -

карається позбавленням волі на строк від п'яти до десяти років.

2. Публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів до вчинення таких дій, -

карається обмеженням волі на строк до трьох років або позбавленням волі на той самий строк.

3. Дії, передбачені частиною другою цієї статі, вчинені особою, яка є представником влади, або повторно, або організованою групою, або з використанням засобів масової інформації, -

карається обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк.

Стаття 110. Посягання на територіальну цілісність і недоторканість України

1. Умисні дії, вчинені з метою зміни меж території або державного кордону на порушення порядку, встановленого Конституцією України, а також публічні заклики чи розповсюдження матеріалів із закликами до вчинення таких дій, -

карається обмеженням волі на строк до трьох років або позбавленням волі на той самий строк.

2. Ті самі дії, якщо вони вчинені особою, яка є представником влади, або повторно, або за попередньою змовою групою осіб, або поєднані з розпалюванням національної чи релігійної ворожнечі, -

карається обмеженням волі на строк від трьох до п'яти років або позбавленням волі на той самий строк.

3. Дії, передбачені частинами першою або другою цієї статті, які призвели до загибелі людей або інших тяжких наслідків, -

караються позбавленням волі на строк від семи до дванадцяти років.

Стаття 111. Державна зрада

1. Державна зрада, тобто діяння, умисно вчинене громадянином України на шкоду суверенітетові, територіальній цілісності та недоторканості, обороноздатності, державній, економічній чи інформаційній безпеці України: перехід на бік ворога в умовах воєнного стану або в період збройного конфлікту, шпигунство, надання іноземній державі, іноземній організації або їх представникам допомогти в проведенні підривної діяльності проти України, -

карається позбавленням волі на строк від десяти до п'ятнадцяти років.

2. Звільняється від кримінальної відповідальності громадянин України, якщо він на виконання злочинного завдання іноземної держави, іноземної організації або їх представників ніяких дій не вчинив і добровільно заявив органам державної влади про свій зв'язок з ними та про отримане завдання.

2. Злочини у сфері використання електронно обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку втрати, підробки, блокування інформації, створення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, -

карається штрафом від шестисот до тисячі неоподаткованих мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації

1. Несанкціонований збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, -

карається штрафом від п'ятисот до тисячі неоподаткованих мінімумів доходів громадян або позбавленням волі на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі від трьох до п'яти років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно- обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, -

карається штрафом від шестисот до тисячі неоподаткованих мінімумів доходів громадян або виправними роботами на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи.

2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої

інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, -

карається позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.

3. Дії передбачені частиною першою, або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється.

1. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, -

карається штрафом від п'ятисот до тисячі неоподаткованих мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюджень повідомлень електрозв'язку.

1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно- обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, -

карається штрафом від п'ятисот до тисячі неоподаткованих мінімумів доходів громадян або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, -

караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися

певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено масове розповсюдження повідомлень електрозв'язку, які є власністю винної особи.

Додаток П

Таблиця 1.
Частина таблиці 1 «Рейтинг інформаційної прозорості офіційних веб-сайтів міністерств та інших центральних органів виконавчої влади у першому півріччі 2019 року», розміщеної у додатку 1 до аналітичної довідки

№	Найменування органу виконавчої влади	Адреса офіційного веб-сайту органу виконавчої влади	Показник наявності інформації, Пн (%)	Показник якості інформаційного наповнення, Пя (%)	Показник інформаційної прозорості, Пі (%)	Показник динаміки інформаційної прозорості, Пд (%)	Коефіцієнт інформаційної доступності (Кід)
1	Міністерство аграрної політики та продовольства України	http://minagro.gov.ua	100	100	100	25	1
2	Міністерство інфраструктури України	http://mtu.gov.ua	100	100	100	0,19	1
3	Державна служба України з лікарських засобів та контролю за наркотиками	http://www.dls.gov.ua	100	100	100	0	1
4	Міністерство інформаційної політики України	http://mip.gov.ua	100	100	100	0	1
5	Державна служба України з питань праці	http://dsp.gov.ua	100	100	100	0	1
6	Державна служба України з надзвичайних ситуацій	http://www.dsns.gov.ua	100	100	100	0	1
7	**Адміністрація Державної прикордонної служби України**	http://dpsu.gov.ua	100	100	100	0	1
Всього 69 органа виконавчої влади							

Джерело: Аналітичні довідки за результатами моніторингу веб-сайтів органів виконавчої влади. URL: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=157241&cat_id=112507 (дата звернення: 16.01.2020)

Таблиця 2.
Частина таблиці 1«Рейтинг інформаційної прозорості офіційних веб-сайтів міністерств та інших центральних органів виконавчої влади у другому півріччі 2019 року», розміщеної у додатку 1 до аналітичної довідки

№	Найменування органу виконавчої влади	Адреса офіційного веб-сайту органу виконавчої влади	Показник наявності інформації, Пн (%)	Показник якості інформаційного наповнення, Пя (%)	Показник інформаційної прозорості, Пі (%)	Показник динаміки інформаційної прозорості, Пд (%)	Коефіцієнт інформаційної доступності (Кід)
1	**Адміністрація Державної прикордонної служби України**	http://dpsu.gov.ua	100	100	100	0	1
2	Державна служба України з лікарських засобів та контролю за наркотиками	http://www.dls.gov.ua	100	100	100	0	1
3	Державна служба України з питань праці	http://dsp.gov.ua	100	99,62	99,81	0,19	1
4	Державна казначейська служба України	http://www.treasury.gov.ua	100	99,23	99,62	0	1
5	Міністерство соціальної політики України	http://www.msp.gov.ua	100	98,85	99,42	-0,39	1
Всього 64 органа виконавчої влади							

Джерело: Аналітичні довідки за результатами моніторингу веб-сайтів органів виконавчої влади. URL: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=162482&cat_id=112507 (дата звернення: 16.01.2020)

Таблиця 3.
Частина таблиці 1«Рейтинг інформаційної прозорості офіційних веб-сайтів міністерств та інших центральних органів виконавчої влади у першому півріччі 2020 року», розміщеної у додатку 1 до аналітичної довідки

№	Найменування органу виконавчої влади	Адреса офіційного веб-сайту органу виконавчої влади	Показник наявності інформації, Пн (%)	Показник якості інформаційного наповнення, Пя (%)	Показник інформаційної прозорості, Пі (%)	Показник динаміки інформаційної прозорості, Пд (%)	Коефіцієнт інформаційної доступності (Кід)
1	Державна служба фінансового моніторингу України	https://fiu.gov.ua/	100	100	100	25	1
2	Адміністрація Державної прикордонної служби України	http://dpsu.gov.ua	100	100	100	0	1
3	Державна служба України з лікарських засобів та контролю за наркотиками	http://www.dls.gov.ua	100	100	100	0	1
4	Державна служба України з питань праці	http://dsp.gov.ua	100	99,23	99,62	-0,19	1
5	Державна регуляторна служба України	http://www.drs.gov.ua	100	99,20	99,60	0,40	1
Всього 78 органів виконавчої влади							

Джерело: Аналітичні довідки за результатами моніторингу веб-сайтів органів виконавчої влади. URL: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=167745&cat_id=112507 (дата звернення: 05.08.2020)

Додаток Р

Методичні рекомендації по роботі зі зверненнями громадян у Державній прикордонній службі України (проект)

ЗМІСТ

ВСТУП

Відносини Державної прикордонної служби України з інформаційною сферою суспільства будуються за принципом інформаційної відкритості. Дієвість цього принципу зумовлена отриманням громадянами необхідної інформації у сфері компетенції прикордонного відомства за їх потребами та інтересами. Зрілість громадянського суспільства виявляється через активність громадян, зокрема через такі його правові форми, як право на звернення. Тому невід'ємним елементом становлення та розвитку сучасного інформаційного суспільства є розширення перспективних взаємозв'язків громадян і держави. У межах діяльності ДПСУ удосконалення такого спілкування сприяє формуванню ефективного механізму комунікацій з громадськістю для реалізації державної політики у сфері охорони державного кордону України. Розширення такого формату інформаційних відносин стає можливим за умови забезпечення відкритості, коли кожен отримує інформацію (у межах, визначених законодавством), яка необхідна для особистого розвитку й потреб, підвищення рівня правосвідомості, дотримання норм прикордонного законодавства, а також здійснення громадського контролю за діяльністю ДПСУ. При цьому у ДПСУ підвищується якість та ефективність охорони державного кордону України та зростає довіра громадян до діяльності прикордонників.

Звернення громадян у діяльності ДПСУ є необхідним для забезпечення права вільного виїзду з України та в'їзду на її територію, створюються умови для надання інформації громадянам про особливості перетинання державного кордону в індивідуальному порядку та вирішення особистих питань у зв'язку із функціонуванням ДПСУ.

Мета цих методичних рекомендацій – допомогти посадовим особам ДПСУ, на яких покладені обов'язки по роботі із зверненнями громадян, більш чітко організувати роботу із зверненнями громадян відповідно до вимог законодавства України.

1. Нормативно-правове регулювання звернення громадян

Стаття 40. **Конституція України** закріплює, що усі мають право направляти індивідуальні чи колективні письмові звернення або особисто звертатися до органів державної влади, органів місцевого самоврядування та посадових і службових осіб цих органів, що зобов'язані розглянути звернення і дати обґрунтовану відповідь у встановлений законом строк (Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР).

Закон України «Про звернення громадян» регулює питання практичної реалізації громадянами України наданого їм Конституції України права вносити в органи державної влади, об'єднання громадян відповідно до їх статуту пропозиції про поліпшення їх діяльності, викривати недоліки в роботі, оскаржувати дії посадових осіб, державних і громадських органів. Закон забезпечує громадянам України можливості для участі в управлінні державними і громадськими справами, для впливу на поліпшення роботи органів державної влади і місцевого самоврядування, підприємств, установ, організацій незалежно від форм власності, для відстоювання своїх прав і законних інтересів та відновлення їх у разі порушення (Про звернення громадян : Закон України від 02.10.1996 р. № 393/96-ВР).

Указ Президента України від 07.02.2008 р. № 109/2008 «Про першочергові заходи щодо забезпечення реалізації та гарантування конституційного права на звернення до органів державної влади та органів місцевого самоврядування».

Постанова Кабінету Міністрів України від 24.09.2008 р. № 858 «Про затвердження класифікатора звернень громадян».

Постанова Кабінету Міністрів України від 24.06.2009 р. № 630 «Про затвердження Методики оцінювання рівня організації роботи із зверненнями громадян в органах виконавчої влади».

Інструкція з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об’єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, в засобах масової інформації : постанова Кабінету Міністрів України від 14.04.1997 р. № 348.

Графік особистого прийому громадян, осіб для надання безоплатної первинної правової допомоги та запитувачів на отримання публічної інформації керівництвом і керівниками структурних підрозділів Адміністрації Державної прикордонної служби України : наказ Адміністрації ДПСУ 24.01.2018 р. № 50 АГ.

2. Основні принципи у роботі зі зверненнями громадян

Законність. Точне та неухильне дотримання норм законодавства, що регулює порядок, підстави та терміни звернення громадян посадовою особою ДПСУ, що розглядає звернення, а не керується власними переконаннями чи поглядами.

Своєчасність. Дотримання термінів при розгляді звернень громадян установлених законодавством.

Обов'язковість прийняття та розгляду звернення. Оформлені належним чином і подані у встановленому порядку звернення підлягають обов'язковому прийняттю та розгляду.

Дотримання права громадянина при розгляді заяви чи скарги. Необхідно надавати громадянину можливості: особисто викласти аргументи особі, що перевіряла заяву чи скаргу, та брати участь у перевірці поданої скарги чи заяви; знайомитися з матеріалами перевірки; подавати додаткові матеріали або наполягати на їх запиті органом, який розглядає заяву чи скаргу; бути присутнім при розгляді заяви чи скарги; користуватися послугами адвоката або представника трудового колективу, організації, яка здійснює правозахисну функцію, оформивши це уповноваження у встановленому законом порядку; одержати письмову відповідь про результати розгляду заяви чи скарги; висловлювати усно або письмово вимогу щодо дотримання таємниці розгляду заяви чи скарги; вимагати відшкодування збитків, якщо вони стали результатом порушень установленого порядку розгляду звернень.

Недопустимість переслідування громадян за подання звернення. Заборонено переслідувати громадян за подання звернень, за критику у зверненні органів і посадових осіб ДПСУ, їх діяльності та рішень.

Недопустимість розголошення відомостей, що містяться у зверненнях. Відомості, які стали відомі посадовій особі ДПСУ під час розгляду звернення громадянина, без його згоди заборонено розголошувати. Також аналогічна заборона стосується іншої інформації, якщо це обмежує права і законні інтереси громадян, на прохання громадянина не підлягає розголошенню його прізвище, місце проживання та роботи. Не допускається з'ясування даних про особу громадянина, які не стосуються звернення.

3. Обов'язки посадових осіб ДПСУ щодо розгляду заяв і скарг

Посадові особи ДПСУ в межах своїх повноважень зобов'язані:

об'єктивно, усебічно і вчасно перевіряти заяви чи скарги;

у разі прийняття рішення про обмеження доступу громадянина до відповідної інформації під час розгляду заяви чи скарги скласти про це мотивовану постанову;

на прохання громадянина запрошувати його на засідання відповідного органу, що розглядає його заяву чи скаргу;

скасовувати або змінювати оскаржувані рішення у випадках, передбачених законодавством України, якщо вони не відповідають закону або іншим нормативним актам, невідкладно вживати заходів до припинення неправомірних дій, виявляти, усувати причини та умови, які сприяли порушенням;

забезпечувати поновлення порушених прав, реальне виконання прийнятих у зв'язку із заявою чи скаргою рішень;

письмово повідомляти громадянина про результати перевірки заяви чи скарги і суть прийнятого рішення;

вживати заходів щодо відшкодування у встановленому законом порядку матеріальних збитків, якщо їх було завдано громадянину в результаті обмеження його прав чи законних інтересів, вирішувати питання про відповідальність осіб, з

вини яких було допущено порушення, а також на прохання громадянина не пізніш як у місячний термін довести прийняте рішення до відома органу місцевого самоврядування, трудового колективу чи об'єднання громадян за місцем проживання громадянина;

у разі визнання заяви чи скарги необґрунтованою роз’яснити порядок оскарження прийнятого за нею рішення;

не допускати безпідставної передачі розгляду заяв чи скарг іншим органам;

особисто організовувати та перевіряти стан розгляду заяв чи скарг громадян, вживати заходів до усунення причин, що їх породжують, систематично аналізувати й інформувати населення про хід цієї роботи.

4. Особливості роботи зі зверненнями громадян у ДПСУ

Розгляд звернень громадян у ДПСУ належить до одного з основних напрямків діяльності – формування ефективного механізму комунікації з громадськістю для реалізації державної політики у сфері охорони державного кордону.

Закон України «Про звернення громадян» від 2 жовтня 1996 року № 393/96-ВР закріплює, що громадянин може звернутись до органів влади із пропозицією (зауваженням), заявою (клопотанням) і скаргою, які можуть бути викладені у письмовій або усній формі (ч. 1. ст. 3). Отже, Закон закріплює два способи звернення: усно та письмово. Усне звернення викладається громадянином на особистому прийомі або за допомогою засобів телефонного зв’язку через Контактний центр, телефон «гарячої лінії» (службу «Довіра») та записується (реєструється) посадовою особою (ч. 5. ст. 5).

Письмове звернення надсилається поштою або передається громадянином до відповідного органу, установи особисто чи через уповноважену ним особу, повноваження якої оформлені відповідно до законодавства. Письмове звернення також може бути надіслане з використанням мережі Інтернет, засобів електронного зв’язку (електронне звернення).

Усні звернення можна подавати особисто на прийомі в посадової особи ДПСУ, за допомогою засобів телефонного зв’язку через Контактний центр ДПСУ за телефоном служби «Довіра».

Особистий прийом громадян у ДПСУ здійснюють керівники структурних підрозділів у визначені дні та години. Наказом Адміністрації ДПСУ від 24 січня 2018 № 50 АГ затверджено «Графік особистого прийому громадян, осіб для надання безоплатної первинної правової допомоги та запитувачів на отримання публічної інформації керівництвом та керівниками структурних підрозділів Адміністрації Державної прикордонної служби України». Інформація про прийомні дні, години начальників та їх заступників регіональних управлінь, прикордонних загонів міститься на офіційних сайтах відповідних структурних підрозділів ДПСУ.

Письмові звернення у ДПСУ можуть надходити через поштовий зв’язок, листом або їх можуть принести до розташування органу чи підрозділу, до керівника якого особа звертається. У цьому разі всі письмові звернення, які надійшли до керівників ДПСУ, підлягають обов’язковій реєстрації у день їх

надходження (або у перший робочий день, якщо звернення надійшло у вихідний день), відповідно до постанови Кабінету Міністрів України від 14 квітня 1997 р. № 348, якою затверджена Інструкція з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, в засобах масової інформації (п. 2).

Письмове звернення може надсилатись поштою або громадянин передає його до відповідного органу, установи особисто чи через уповноважену ним особу, повноваження якої оформлені відповідно до законодавства. Використання мережі Інтернет та засобів електронного зв'язку (електронне звернення) є різновидом письмового звернення (Про звернення громадян : Закон України від 2 жовтня 1996 року № 393/96-ВР, ч. 6 ст. 5).

Окремою формою задоволення інформаційних потреб і реалізації інформаційних прав громадян шляхом звернення до ДПСУ є консультації з використанням електронної пошти в режимі on-line та телефонів «гарячих ліній».

Особисте усне звернення громадян за телефоном «гарячої лінії» забезпечує можливість вирішення проблеми чи питання у режимі реального часу.

Громадяни України мають право звернутися за телефоном служби «Довіра» у межах функціональних обов'язків ДПСУ із зауваженнями, скаргами та пропозиціями, що стосуються їх статутної діяльності, заявою або клопотанням щодо реалізації своїх соціально-економічних, політичних та особистих прав і законних інтересів та скаргою про їх порушення (Про звернення громадян : Закон України від 2 жовтня 1996 року № 393/96-ВР, ч. 1 ст. 1).

Відповідно до ч. 3 ст. 1 Закону України «Про звернення громадян» установлені обмеження щодо подання звернення для осіб, які не є громадянами України, вони мають право їх подавати, якщо законно знаходяться на території України. Тобто коли особи, які не є громадянами України, перебувають за межами території України, вони мають право звертатись до ДПСУ лише через відповідні дипломатичні установи своєї країни, а в ДПСУ не зобов'язані приймати звернення, що надіслані особисто такими особами, за умови, що вони перебувають за кордоном.

У такому випадку обов'язковим елементом є встановлення місця перебування іноземця на момент подання звернення. Якщо за письмовим зверненням можливо з'ясувати місце відправлення (на конверті є інформація про відправника, населений пункт, країну, а також є відповідні відбитки поштових організацій держав), то у разі отримання в електронній формі чи телефонним зв'язком звернення встановити остаточно таке місце (в Україні чи за кордоном) неможливо.

Під час телефонної розмови представник Контактного центру може запитати, з якої країни телефонує особа, але відповідь не буде гарантованою, а «лише зі слів особи».

Іноземець, якого не пропустили на територію України, перебуваючи у пункті пропуску через державний кордон України (який фактично є територією України), не може одразу подати звернення у будь-якій формі. Відповідно до ч. 3 ст. 1 Закону України «Про звернення громадян» звернення підлягає розгляду,

але у цій статті вказана ще одна умова, що під час подання такого звернення іноземець має перебувати на території України «на законних підставах».

Закон України «Про правовий статус іноземців та осіб без громадянства» встановлює (ч. 7 ст. 1), що «перебування на території України на законних підставах» означає, що іноземець у встановленому законодавством чи міжнародним договором України порядку в'їхав в Україну та постійно або тимчасово проживає на її території, або тимчасово перебуває в Україні. Отже, у разі відмови у в'їзді на територію України іноземцю подавати звернення особисто він не має права (може лише через дипломатичні установи своєї країни), а Контактний центр може їх не приймати.

Відповідно до ч. 7 ст. 5 Закону України «Про звернення громадян» обов'язковими елементами звернення має бути прізвище, ім'я, по батькові, місце проживання громадянина, суть порушеного питання, зауваження, пропозиції, заяви чи скарги, прохання чи вимоги. При цьому письмове звернення повинно бути підписано заявником (заявниками) із зазначенням дати. Щодо направлення електронного звернення, зазначена норма ст. 5 Закону України «Про звернення громадян» електронного цифрового підпису не вимагає.

У випадку, коли у зверненні міститься вимога, у тому числі про надання інформації про перетинання фізичною особою державного кордону України, про наявність або відсутність стосовно фізичної особи тимчасового обмеження у праві виїзду з України, а також обмеження права в'їзду іноземцю в Україну необхідно керуватись нормами Закону України «Про захист персональних даних». Частина 1 статті 14 цього Закону зобов'язує отримання згоди від суб'єкта персональних даних щодо передачі відомостей про цю фізичну особу (поширення персональних даних). Виключенням є випадки, визначені Законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини (Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI, ч. 2 ст. 14). Крім цього, якщо особа хоче отримати таку інформацію про себе, це ставить перед персоналом ДПСУ завдання встановити особу запитувача інформації.

5. Відмова у прийнятті та розгляді звернення

Стаття 8 Закону України «Про звернення громадян» визначає підстави відмови у розгляді та вирішенні питань, а саме: коли у письмовому зверненні відсутнє зазначене місця проживання, звернення не підписане автором (авторами), а також таке, з якого неможливо встановити авторство, визнається анонімним і розгляду не підлягає. Отже, якщо не виконана одна з умов, установлених до письмового звернення, такі звернення не підлягають розгляду.

Звернення, оформлене без дотримання цих вимог, повертається заявникові з відповідними роз'ясненнями не пізніш як **через десять днів** від дня його надходження.

Не розглядаються повторні звернення одним і тим же органом від одного і того ж громадянина з одного і того ж питання, якщо перше вирішено по суті. Скарги, подані з порушенням зазначеного терміну, не розглядаються, зокрема скарга на рішення, що оскаржувалось, може бути подана до органу або посадовій

особі вищого рівня **протягом одного року** з моменту його прийняття, **але не пізніше одного місяця** з часу ознайомлення громадянина з прийнятим рішенням.

Рішення про припинення розгляду такого звернення приймає керівник органу, про що повідомляється особі, яка подала звернення.

Рішення вищого державного органу, який розглядав скаргу, у разі незгоди з ним громадянина може бути оскаржено лише в судовому порядку.

6. Терміни розгляду звернень громадян

Звернення розглядаються і вирішуються не більше **одного місяця** від дня їх надходження, а ті, які не потребують додаткового вивчення, – невідкладно, але **не пізніше п'ятнадцяти днів** від дня їх отримання.

Якщо в місячний термін вирішити порушені у зверненні питання неможливо, керівник відповідного органу встановлює необхідний термін для його розгляду, про що повідомляється особі, яка подала звернення. При цьому загальний термін вирішення питань, порушених у зверненні, **не може перевищувати сорока п'яти днів**.

На обґрунтовану письмову вимогу громадянина термін розгляду *може бути скорочено* від встановленого цією статтею терміну.

Звернення громадян, які мають установлені законодавством пільги, розглядаються у *першочерговому порядку*.

7. **Відповідальність за порушення законодавства про звернення громадян**

Стаття 24 Закону України «Про звернення громадян» закріплює, що особи, винні у порушенні цього Закону, несуть цивільну, адміністративну або кримінальну відповідальність, передбачену законодавством України.

Стаття 25 встановлює підстави відшкодування збитків громадянину у зв'язку з порушенням вимог цього Закону при розгляді його скарги.

Так, у разі задоволення скарги орган або посадова особа, які прийняли неправомірне рішення щодо звернення громадянина, відшкодовують йому завдані матеріальні збитки, пов'язані з поданням і розглядом скарги, обґрунтовані витрати, понесені у зв'язку з виїздом для розгляду скарги на вимогу відповідного органу, і втрачений за цей час заробіток. Спори про стягнення витрат розглядаються в судовому порядку.

Громадянину на його вимогу і в порядку, встановленому чинним законодавством, можуть бути відшкодовані моральні збитки, завдані неправомірними діями або рішеннями органу чи посадової особи при розгляді скарги. Розмір відшкодування моральних (немайнових) збитків у грошовому виразі визначається судом.

Відповідальність несе і громадянин за подання звернень протиправного характеру (стаття 26 Закону України «Про звернення громадян»). Подання громадянином звернення, яке містить наклеп і образи, дискредитацію органів державної влади, органів місцевого самоврядування, об'єднань громадян та їхніх посадових осіб, керівників та інших посадових осіб підприємств, установ і організацій незалежно від форм власності, заклики до розпалювання національної,

расової, релігійної ворожнечі та інших дій, тягне за собою відповідальність, передбачену чинним законодавством.

Витрати, зроблені органом державної влади, місцевого самоврядування, підприємством, установою, організацією незалежно від форм власності, об'єднанням громадян, засобами масової інформації у зв'язку з перевіркою звернень, які містять завідомо неправдиві відомості, можуть бути стягнуті з громадянина за рішенням суду (стаття 27 Закону України «Про звернення громадян»).

Стаття 212-3 Кодексу України про адміністративні правопорушення передбачає відповідальність за *порушення права на інформацію та права на звернення*.

Частина 4 Обмеження доступу до інформації або віднесення інформації до інформації з обмеженим доступом, якщо це прямо заборонено законом, – тягне за собою накладення штрафу на посадових осіб від шістдесяти до вісімдесяти неоподатковуваних мінімумів доходів громадян.

Частина 7 Незаконна відмова у прийнятті та розгляді звернення, інше порушення Закону України «Про звернення громадян», – тягнуть за собою накладення штрафу на посадових осіб від двадцяти п'яти до п'ятдесяти неоподатковуваних мінімумів доходів громадян.

Частина 9 Повторне протягом року вчинення будь-якого з цих порушень, за яке особу вже було піддано адміністративному стягненню, – тягне за собою накладення штрафу на посадових осіб від шістдесяти до вісімдесяти неоподатковуваних мінімумів доходів громадян або громадські роботи на строк від двадцяти до тридцяти годин.

Але відповідно до статті 15 Кодексу України про адміністративні правопорушення за вчинення цих інформаційних правопорушень військовослужбовці несуть **дисциплінарну відповідальність.**

Додаток С

Алгоритм формування інформаційної культури у Державній прикордонній службі України

ОБҐРУНТУВАННЯ

прогресуючий розвиток інформаційних відносин, зростання цінності інформації у забезпечення прикордонної безпеки держави, необхідність забезпечення захисту інформації та приватності всіх суб'єктів цих відносин, а також складне й динамічне безпекове середовище довкола України, запровадження європейських стандартів інтегрованого управління кордонами обумовлюють необхідність формування нового типу свідомості прикордонника у межах модернізації інформаційної складової системи охорони державного кордону

МЕТА

необхідність вироблення такого типу поведінки у персоналу прикордонних підрозділів, який би відповідав вимогам законодавства, інформаційного суспільства щодо обробки й захисту інформації, розпорядником якої є ДПСУ;

унеможливлення деструктивного впливу, недопущення маніпулювання

ҐРУНТУЄТЬСЯ:

на системі загальноправових цінностей (правова аксіологія) щодо забезпечення справедливості, рівності, відповідно до законодавства свободи доступу до відкритої публічної інформації,

суворому дотриманні та обґрунтованому балансі між приватністю і захистом інформації (службової, таємної) у сфері інтересів прикордонної безпеки

ЗАСОБИ ФОРМУВАННЯ

освітньої-правовий вплив
сприятиме розвитку інформаційної культури представників ДПСУ, підвищенню обізнаності з теоретичних засад у сфері формування та обігу інформації з урахуванням особливостей завдань, що виконує ДПСУ, з подальшим екстраполюванням у практичну діяльність

ПРОГНОЗОВАНІ ЯКІСНІ НАВИЧКИ

- володіння базовими (для всіх) або поглибленими (для осіб, що здійснюють інформаційну діяльність) знаннями інформаційного законодавства;
- знання принципових вимог інформаційної діяльності, зокрема створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації та їх особливостей у діяльності ДПСУ;
- балансування принципу транспарентності інформаційних відносин із захистом персональних даних і прикордонною безпекою;
- розуміння основних понять та їх змісту («інформація», «персональні дані», «володілець інформації», «розпорядник інформації» тощо);
- розмежовування категорії «відкрита інформація», «інформація з обмеженим доступом» тощо;
- володіння обсягом правових режимів «конфіденційна інформація», «службова інформація», «таємна інформація»;
- нерозповсюдження особистої приватної інформації (зображення) у мережі Інтернет;
- уміння використовувати комп'ютерну техніку із врахуванням «комп'ютерної гігієни»;
- знання інформаційних правопорушень, за які застосовується кримінальна, адміністративна, дисциплінарна та цивільно-правова відповідальність

Додаток Т

Таблиця
Пропозиції щодо внесення змін та доповнень
до нормативно-правових актів України

Зміст положень чинного законодавства	**Положення законодавчого акта, що пропонується**
Закон України «Про Державну прикордонну службу України»	
Частина 3 статті 2. «***Основні функції Державної прикордонної служби України»*** Відсутня.	**Частина 3 статті 2.** «***Основні функції Державної прикордонної служби України»*** Здійснення інформаційної функції.
Абзац 9 частини 1 статті 3. «***Основні принципи діяльності Державної прикордонної служби України»*** Відсутня.	**Абзац 9 частини 1 статті 3.** «***Основні принципи діяльності Державної прикордонної служби України»*** Транспарентність.
Стаття 5-1 «***Інформування про діяльність Державної прикордонної служби України»*.** Відсутня.	**Стаття 5-1** «***Інформування про діяльність Державної прикордонної служби України»*.** Голова Державної прикордонної служби України систематично інформує Верховну Раду України про виконання Державною прикордонною службою України покладених на неї завдань, додержання законодавства, забезпечення прав і свобод людини та з інших питань. Голова Державної прикордонної служби України щороку подає Верховній Раді України письмовий звіт про діяльність Державної прикордонної служби України. Державна прикордонна служба України інформує: органи доходів і зборів про факт наміру перетинання державного кордону України особами, стосовно яких органами доходів і зборів було виявлено порушення митних правил; відповідні державні органи та громадян про події на державному кордоні України, у прикордонній смузі та в

	контрольованих прикордонних районах; уповноважені державні органи, які надали доручення про факт перетинання державного кордону особами або про факт їх в'їзду на тимчасово окуповану територію України чи виїзду з неї, стосовно яких уповноваженими державними органами проводяться оперативно-розшукові, контррозвідувальні або розвідувальні заходи. Державна прикордонна служба України повідомляє Департамент у сфері захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини про обробку персональних даних відповідно до умов та порядку, визначеного у статті 9. Закону України «Про захист персональних даних». Державна прикордонна служба України здійснює систематичне та оперативне висвітлення офіційної інформації: в офіційних друкованих виданнях; на офіційних веб-сайтах в мережі Інтернет; на єдиному державному веб-порталі відкритих даних; на інформаційних стендах; будь-яким іншим способом. Державна прикордонна служба України надає інформацію за запитами на інформацію.
Стаття 5-3 **«*Захист приватності у діяльності Державної прикордонної служби України*».** Відсутня.	**Стаття 5-3** **«*Захист приватності у діяльності Державної прикордонної служби України*».** Державна прикордонна служба України обробляє персональні дані у межах виконання своїх повноважень в інтересах охорони державного кордону України. Державна прикордонна служба України повідомляє суб'єкта персональних даних про дії з його персональними даними на умовах, визначених статтею 21 Закону України «Про захист персональних даних». Військовослужбовці та працівники

	Державної прикордонної служби України, які мають доступ до персональних даних, дають письмове зобов'язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням службових обов'язків
Частина 30 статті 19. «***Обов'язки Державної прикордонної служби України»:*** Відсутня.	**Частина 30 статті 19.** «***Обов'язки Державної прикордонної служби України»:*** надання інформаційних послуг згідно з чинним законодавством
Частина 4 статті 33 «***Відповідальність особового складу Державної прикордонної служби України»*:** Відсутня.	**Частина 4 статті 33** «***Відповідальність особового складу Державної прикордонної служби України»*:** Військовослужбовці та працівники Державної прикордонної служби України несуть відповідальність, передбачену законом за надання недостовірної інформації, а також за неправомірну відмову у наданні відповідної інформації, несвоєчасне надання інформації, порушення порядку збереження та розповсюдження персональних даних та інші правопорушення у сфері інформаційних відносин
Закон України «Про прикордонний контроль»	
Стаття 3-1 ***«Обробка персональних даних осіб, що перетинають державний кордон».*** Відсутня.	**Стаття 3-1** ***«Обробка персональних даних осіб, що перетинають державний кордон».*** Під час прикордонного контролю посадові особи Державної прикордонної служби України забезпечують обробку персональних даних відповідно до Закону України «Про захист персональних даних» осіб, що перетинають державний кордон України. Обсяг персональних даних не може перевищувати даних, що необхідні для здійснення повноважень ДПСУ, формування бази даних «Відомості про осіб, які перетнули державний кордон України» та прийняття рішення про надання дозволу/заборони

	в'їзду (виїзду) на територію України. Прибуття особи у пункт пропуску через державний кордон України з пред'явленням нею паспортних та інших документів, надання інформації уповноваженими службовими особами Державної прикордонної служби України під час опитування є добровільною згодою особи на обробку її персональних даних. Метою обробки персональних даних є ідентифікація особи, установлення законних підстав для надання дозволу уповноваженими службовими особами Державної прикордонної служби України на перетинання державного кордону України, установлення відсутності\наявності заборони в'їзду (виїзду) на територію України, фіксації факту перетинання державного кордону, забезпечення безпеки державного кордону
Про затвердження Положення про базу даних «Відомості про осіб, які перетнули державний кордон України»: наказ Адміністрації Державної прикордонної служби України від 25.06.2007 № 472	
Пункт 19: Інформація, що зберігається в Базі даних осіб, є сукупністю *відкритої адміністративної інформації та інформації про осіб* і є власністю Державної прикордонної служби України *та не належить до інформації з обмеженим доступом*	**Пункт 19**: Інформація, що зберігається у Базі даних осіб, є сукупністю *персональних даних осіб, що перетинають державний кордон України* і є власністю Державної прикордонної служби України
КК України	
ч. 1 ст. 332-2 1. Перетинання державного кордону України з метою заподіяння шкоди інтересам держави або особою, якій заборонено в'їзд на територію України, або представниками підрозділів збройних сил чи інших силових відомств	**ч. 1 ст. 332-2** 1. Перетинання державного кордону України з метою заподіяння шкоди інтересам держави або особою, якій заборонено в'їзд на територію України, або представниками підрозділів збройних сил чи інших силових відомств держави-агресора у будь-який спосіб поза пунктами пропуску через державний

держави-агресора у будь-який спосіб поза пунктами пропуску через державний кордон України або в пунктах пропуску через державний кордон України без відповідних документів, або за документами, що містять *недостовірні відомості*	кордон України або в пунктах пропуску через державний кордон України без відповідних документів, або за документами, що містять *відомості, які не відповідають дійсності*

Додаток У

Проект
Концепції інформаційного забезпечення
Державної прикордонної служби України

Ця Концепція інформаційного забезпечення Державної прикордонної служби України (далі – Концепція) спрямована на розвиток інформаційної сфери в діяльності ДПСУ, у поєднанні вимог сучасного інформаційного суспільства та розвитку системи інформаційної безпеки в охороні державних кордонів.

Метою Концепції є забезпечення ефективної реалізації інформаційних відносин та інформаційної безпеки у сфері діяльності Державної прикордонної служби України.

Правовою основою реалізації Концепції є Конституція України, Закон України «Про національну безпеку України», «Про інформацію», «Про захист персональних даних», «Про доступ до публічної інформації», «Про звернення громадян», «Про доступ до публічної інформації», «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» та інші закони України, Укази Президента України Стратегія національної безпеки України, Доктрина інформаційної безпеки України, наказу Уповноважений Верховної Ради України з прав людини яким затверджені «Типовий порядок обробки персональних даних»; «Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних»; «Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації»; розпоряджень Кабінету Міністрів України Стратегія розвитку Державної прикордонної служби України, Стратегія інтегрованого управління кордонами на період до 2025 року, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Відповідно до цієї Концепції розробляються і затверджуються стратегії, програми та плани, посадові інструкції, які пов'язані з інформаційною сферою діяльності Державної прикордонної служби України.

Діяльність Державної прикордонної служби України в інформаційній сфері ґрунтується на інтересах:

державної політики інформаційної безпеки;

реалізації завдань щодо забезпечення надійної охорони державного кордону;

задоволенні інформаційних прав громадян та суспільства у сфері охорони державного кордону;

функціонуванні, розвитку та захищеності інформаційно-телекомунікаційних систем внутрішньовідомчого та міжвідомчого (у межах інтегрованого управління кордонами).

Принципи діяльності Державної прикордонної служби України в інформаційній сфері:

реалізація державної політики інформаційної безпеки;

прийняття управлінських рішень лише на підставі об'єктивної та достовірної інформації;

транспарентність;

реалізація та дотримання інформаційних прав усіх суб'єктів прикордонних відносин;

достовірність і повнота публічної інформації про діяльність Державної прикордонної служби України;

вираження особистих поглядів, переконань, персональних даних (у тому числі у мережі Інтернет) персоналу Державної прикордонної служби України з урахуванням засад прикордонної безпеки;

обмін інформацією з іншими органами публічної адміністрації відповідно до вимог чинного законодавства та виключно в інтересах охорони державного кордону;

сприяння розвитку інформаційної складової охорони державного кордону;

посилений захист інформації з обмеженим доступом;

системність вжиття своєчасних та адекватних заходів захисту інформації у сфері службової діяльності Державної прикордонної служби України.

Суб'єктами забезпечення ефективної реалізації інформаційних відносин та інформаційної безпеки у сфері діяльності Державної прикордонної служби України є:

усі військовослужбовці та працівники Державної прикордонної служби України (загальні суб'єкти);

посадові особи, до повноважень яких віднесено здійснення інформаційної діяльності (спеціальні суб'єкти).

Напрямки розвитку інформаційних відносин у діяльності Державної прикордонної служби України:

розвиток нормативно-правового регулювання у напрямку створення відповідно до вимог інформаційного суспільства інформаційного простору у Державній прикордонній службі України;

розвиток відкритості та доступності у діяльності Державної прикордонної служби України;

чітке усвідомлення та розмежування усім особовим складом Державної прикордонної служби України категорій «відкрита публічна інформація», «персональні дані», «конфіденційна інформація», «службова інформація» та «таємна інформація», та їх правових режимів;

створення та удосконалення безпекового інформаційного й інформаційно-ресурсного забезпечення;

забезпечення дотримання балансу між інформаційною приватною та публічною сферою;

урахування стандартів ЄС щодо дотримання приватності у прикордонній сфері;

розвиток інформаційної культури персоналу Державної прикордонної служби України.

Додаток Ф

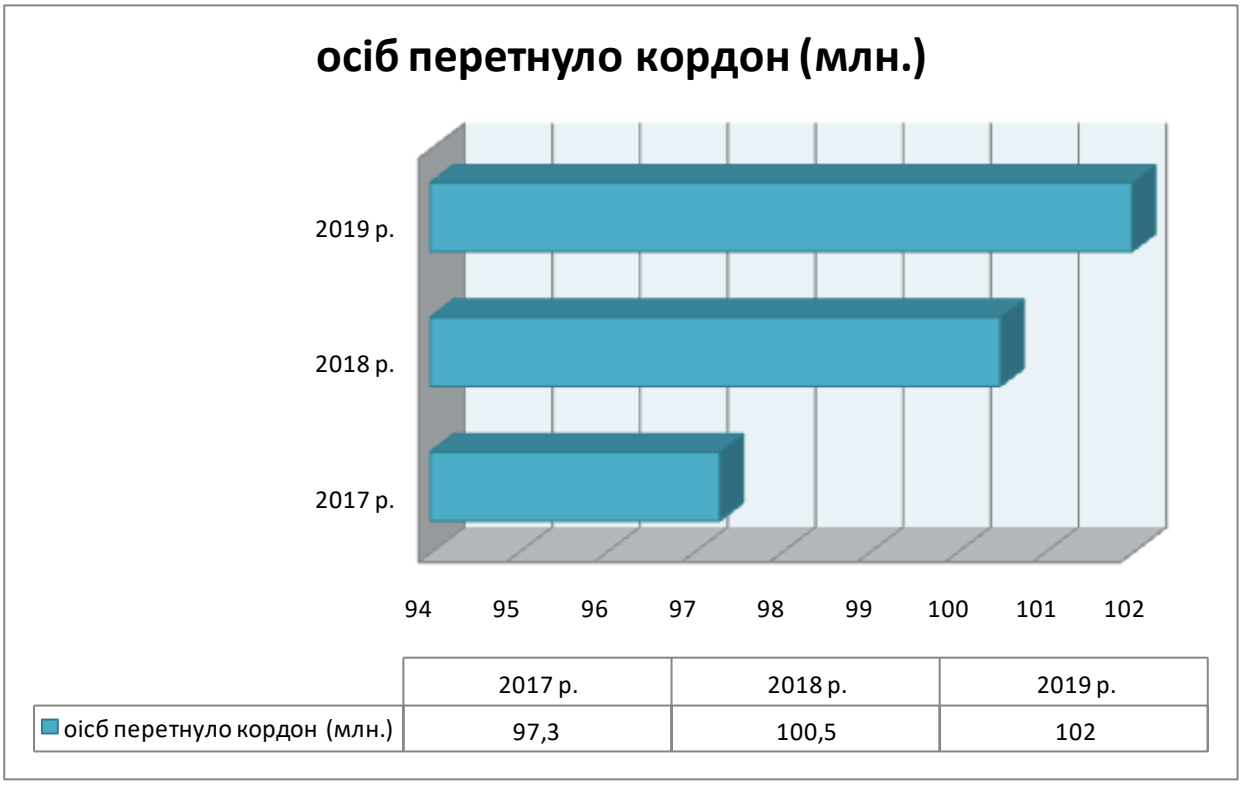
Проект
структури Інформаційного кодексу України

1. Загальні положення (визначення термінів, предмет правового регулювання Кодексу, мова інформації, основні принципи та гарантії права на інформацію).
2. Суб'єкти інформаційних відносин (право на інформацію, закріплення правового становища держави, людини та громадянина в інформаційній сфері, напрями державної інформаційної політики).
3. Об'єкти інформаційних відносин (види інформації, режим конфіденційної, службової та таємної інформації, джерела інформації).
4. Інформаційна діяльність (правові механізми створення, поширення, використання, зберігання, знищення, охорони та захисту інформації, електронне урядування).
5. Доступ до публічної інформації (правові засади обігу офіційної інформації про діяльність органів державної влади).
6. Інформація про особу (правові засади використання та обігу інформації про особу, захист персональних даних).
7. Звернення громадян (підстави, порядок і механізми реалізації прав громадян на звернення).
8. Запит на інформацію (підстави, порядок і механізми реалізації прав громадян на запит на інформацію).
9. Засоби масової інформації (регулювання правового становища засобів масової інформації).
10. Інформаційна безпека (державна політика інформаційної безпеки, її напрямки, правові засади розвитку національного інформаційного простору, загрози інформаційній безпеці, система інформаційної безпеки).
11. Відповідальність за порушення інформаційного законодавство (підстави застосування відповідальності, звільнення від відповідальності за порушення норм інформаційного законодавства).

Додаток Х

Діаграма 1.

Динаміка зростання пасажиропотоку за 2017-2019 рр..

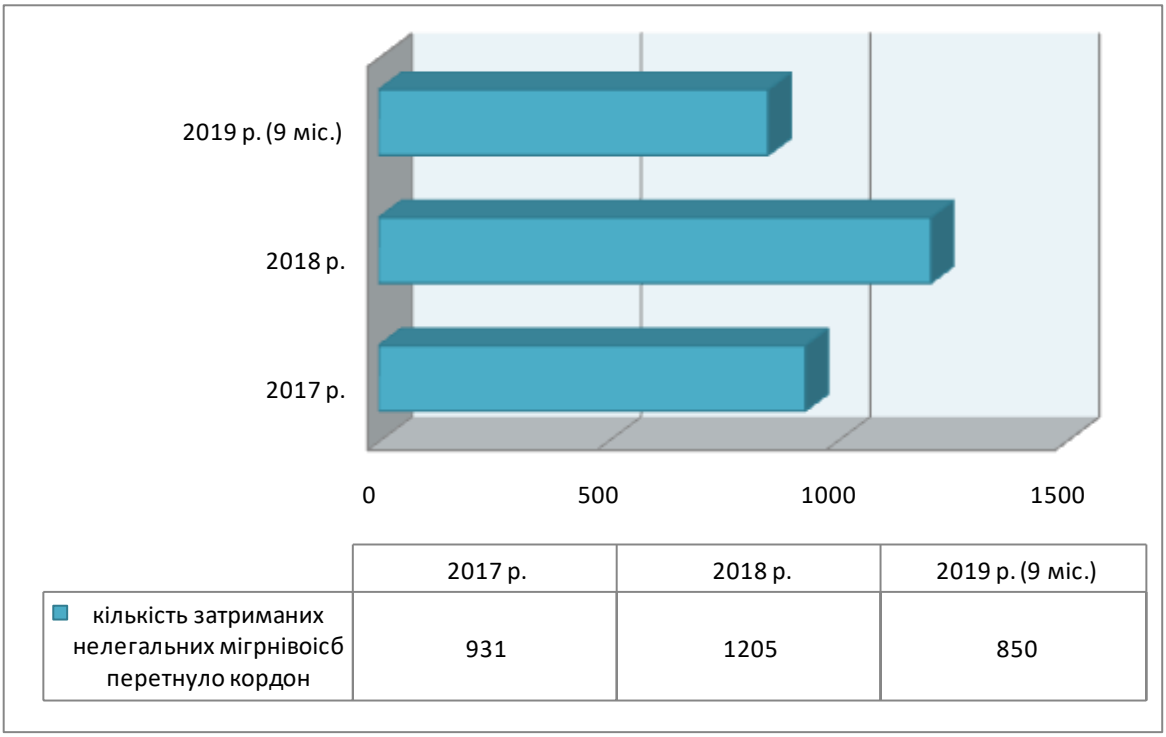


	2017 р.	2018 р.	2019 р.
оісб перетнуло кордон (млн.)	97,3	100,5	102

Джерело: Програма діяльності Кабінету Міністрів України. Проект Концепції державної політики щодо досягнення цілі 13.5 «Українці захищені надійним кордоном та задоволені сервісом при його перетинанні». URL: https://program.kmu.gov.ua/meta/ukrainci-zahiseni-nadijnim-kordonom-ta-zadovoleni-servisom-pri-jogo-peretini (дата звернення: 10.02.2020).

Діаграма 2.

Кількість затриманих на державному кордоні нелегальних мігрантів за 2017-2019 рр..



	2017 р.	2018 р.	2019 р. (9 міс.)
кількість затриманих нелегальних мігрнівоісб перетнуло кордон	931	1205	850

Джерело: Програма діяльності Кабінету Міністрів України. Проект Концепції державної політики щодо досягнення цілі 13.5 «Українці захищені надійним кордоном та задоволені сервісом при його перетинанні». URL: https://program.kmu.gov.ua/meta/ukrainci-zahiseni-nadijnim-kordonom-ta-zadovoleni-servisom-pri-jogo-peretini (дата звернення: 10.02.2020).

ВЕРХОВНА РАДА УКРАЇНИ

Комітет з питань правової політики

01008, м. Київ-8, вул. М. Грушевського, 5, тел.: 255-35-84

№ 0426/17-2020/172667 (дата 59) «30» вересня 2020 р.

Акт

впровадження результатів дисертаційного дослідження

Кушнір Ірини Павлівни у законотворчу діяльність

Комісія у складі: Голови Комітету Верховної Ради України з питань правової політики Костіна А. Є., члена Комітету Стефанчука М. О. та керівника секретаріату Комітету Колісника І. В., склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження докторанта Національної академії Державної прикордонної служби України імені Богдана Хмельницького Кушнір Ірини Павлівни на тему: «Теоретичні та організаційні засади нормативно-правового регулювання інформаційних відносин у діяльності Державної прикордонної служби України», поданого на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право».

Комісія вважає, що представлені пропозиції, отримані на основі проведеного комплексного дисертаційного дослідження, мають необхідний теоретичний та методологічний рівень, практичну значимість, є надзвичайно актуальними та можуть бути використані для вдосконалення нормативно-правових актів України як основної форми права в нашій державі.

Цей акт наданий для подання у відповідну спеціалізовану вчену раду із захисту дисертацій на здобуття наукового ступеня доктора юридичних наук.

Голова Комітету **А. Є. КОСТІН**

Член Комітету **М. О. СТЕФАНЧУК**

Керівник секретаріату Комітету **І. В. КОЛІСНИК**

Підпис А.Є. Костіна, М.О. Стефанчука, І.В. Колісника підтверджую
Управління кадрів Апарату Верховної Ради України
29 09 2020 р.

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

(Адміністрація Держприкордонслужби)

вул. Володимирська, 26, м. Київ, 01601; тел.: (044) 235-11-00, факс: (044) 239-84-80

E-mail: adpsu@dpsu.gov.ua, www.dpsu.gov.ua

ЗАТВЕРДЖУЮ
Заступник Голови Державної
прикордонної служби України
кандидат педагогічних наук
генерал-майор

Сергій СЕРДЮК

«26» червня 2020 року

АКТ
про впровадження результатів дисертаційного дослідження
Ірини КУШНІР на тему «Теоретичні та організаційні засади
нормативно-правового регулювання інформаційних відносин
у діяльності Державної прикордонної служби України»

Комісія у складі: Голови комісії – начальника управління адміністративної юрисдикції Департаменту охорони державного кордону канд. юрид. наук, полковника КУРИЛЮКА Юрія та членів комісії: начальника відділу Департаменту оперативно-розшукової діяльності д-ра юрид. наук, доцента, полковника ПРИТУЛИ Анатолія, головного консультанта відділу управління юридичного забезпечення канд. наук з держ. упр., полковник юстиції КОРОТУШАКА Андрія, склала цей акт про те, що науково-теоретичні положення, висновки, пропозиції та практичні рекомендації докторанта докторантури Національної академії Державної прикордонної служби України імені Б. Хмельницького Ірини КУШНІР, які оприлюднені у наукових виданнях за темою її дисертаційного дослідження: «Теоретичні та організаційні засади нормативно-правового регулювання інформаційних відносин у діяльності Державної прикордонної служби України» проаналізовані та можуть бути враховані при: удосконаленні законодавства України про державний кордон в

частині забезпеченням інформаційної діяльності органів Державної прикордонної служби України; організації й удосконаленні діяльності, пов'язаної зі створенням, збиранням, одержанням, зберіганням, використанням, поширенням, обміном, охороною та захистом інформації, що перебуває у розпорядженні Державної прикордонної служби України; покращанні роботи із зверненнями громадян та запитами на публічну інформацію у Державній прикордонній службі України, підвищенні довіри громадян до прикордонного відомства; впровадженні електронного урядування й електронного документообігу.

Голова комісії:
канд. юрид. наук, полковник Юрій КУРИЛЮК

Члени комісії:
д-р юрид. наук, доцент
полковник Анатолій ПРИТУЛА

канд. наук з держ. упр.
полковник юстиції Андрій КОРОТУШАК

ДЕРЖАВНА ПРИКОРДОННА СЛУЖБА УКРАЇНИ
РЕГІОНАЛЬНЕ УПРАВЛІННЯ МОРСЬКОЇ ОХОРОНИ АДМІНІСТРАЦІЇ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ
вул. Приморська, 3-А, Одеса-26, 65026, тел.: (048) 230-92-35, факс: (048) 723-38-39
e-mail: rvus_rumo@dpsu.gov.ua

ЗАТВЕРДЖУЮ
Начальник Регіонального управління Морської охорони Адміністрації Державної прикордонної служби України
контр-адмірал Олег КОСТУР
«12» 06 2020 р.

АКТ
про впровадження результатів дисертаційного дослідження Ірини КУШНІР

Комісія у складі: Голови комісії – заступник начальника регіонального управління з персоналу капітан 1 рангу Юрій АЛЕЙНИКОВ, та членів комісії: начальник сектору документального забезпечення штабу – секретар колегії капітан 1 рангу Анатолій ХАРЛАШ, начальник відділу підготовки персоналу капітан 1 рангу Володимир КАПЛЯР, старший офіцер (адміністративно-юрисдикційної діяльності) відділу організації служби штабу капітан 2 рангу Павло МАМАЙ, склала цей акт про те, що наукові результати Ірини КУШНІР, які викладені у наукових статтях за темою дисертаційного дослідження: «Теоретичні та організаційні засади нормативно-правового регулювання інформаційних відносин у діяльності Державної прикордонної служби України», а саме:

Кушнір І. П. Види інформації, розпорядником якої є Державна прикордонна служба України, їх сутнісна характеристика. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2018. Вип. 1. URL: http://nbuv.gov.ua/UJRN/vnadpcurn_2018_1_6;

Кушнір І. П. Органи охорони державного кордону як суб'єкти інформаційних правовідносин. *Правові новели*. 2018. № 5. С. 71–77;

Кушнір І. П. Інформаційно-правовий статус Державної прикордонної служби України. *Приватне та публічне право*. 2018. № 4. С. 50–53;

Кушнір І. П. Організаційно-правові питання забезпечення захисту інформації в інформаційних системах Державної прикордонної служби України. *Прикарпатський юридичний вісник*. № 3. 2018. С. 81–84;

Кушнір І. П. Особливості правових відносини щодо забезпечення запиту на публічну інформацію, розпорядником якої є Державна прикордонна служба

України. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2018. Вип. 4. 13 с. URL: https://nadpsu.edu.ua/wp-content/uploads/2019/02/visnuk_4_2019_ur.pdf;

Кушнір І. П. Реалізація права на звернення громадян у Державній прикордонній службі України. *Visegrad Journal on Human Rights*. 2018. 4 (volume 2). С. 56–60;

Кушнір І., Степанова Ю. Інформаційна безпека держави у прикордонній сфері як об'єкт державної зради. *National law journal: theory and practice*. 2018. № 4 (32). Т. 1. С. 123–126;

Кушнір І. П. Кримінально-правове забезпечення охорони інформаційних відносин у прикордонній сфері. *Питання боротьби зі злочинністю*. 2018. Вип. 36. 186 с. С. 82–93;

Кушнір І. П. Інформаційна відкритість у діяльності Державної прикордонної служби України. *Правова позиція*. 2019. № 1 (22). С. 30–36;

Кушнір І. П. Царенко О. М. Правовий режим інформації з обмеженим доступом у діяльності Державної прикордонної служби України. *Право та державне управління*. 2019. № 3. С. 180–185;

Кушнір І. П. Інформаційна складова підготовки та прийняття управлінських рішень в органах охорони державного кордону України». *Legea si Viata*. 2019. № 5. С. 100–104;

Кушнір І. П. Інформаційні загрози в діяльності Державної прикордонної служби України. *Підприємництво, господарство і право*. 2019. № 7. С. 147–150;

Кушнір І. П. Адміністративна відповідальність за порушення законодавства про інформацію у прикордонній сфері. *Право і інформація*. № 1(28). 2019. С. 45–51;

Кушнір І. П., Коротушак А. І. Питання удосконалення впровадження електронного урядування у Державній прикордонній службі України. *Вісник Південного регіонального центру Національної академії правових наук України*. 2019. № 20. С. 96–102;

Кушнір І. П., Царенко С. І., Царенко О. М. Особливості застосування дисциплінарної відповідальності за порушення інформаційного законодавства у діяльності Державної прикордонної служби України. *Актуальні проблеми вітчизняної юриспруденції*. № 6. 2019. С. 80–84;

Кушнір І. П. Основні тенденції інформаційної взаємодії у діяльності Державної прикордонної служби України. *Visegrad Journal on Human Rights*. 2019. 4 . С. 96–101, *проаналізовані та враховані:*

- у нормотворчій діяльності при відпрацюванні проектів наказів та інструкцій пов'язаних: з обігом інформації у сфері охорони державного кордону; забезпеченням інформаційної діяльності; дотриманням режиму інформації з обмеженим доступом; захистом персональних даних громадян, їх реалізацією права на звернення та запит на публічну інформацію, а також захистом персональних даних військовослужбовців, що проходять службу в Регіональному управлінні Морської охорони Державної прикордонної служби України;

- в організації й удосконаленні інформаційної діяльності, під час створення, збирання, одержання, зберігання, використання, поширення, обміну, охорони та захисту інформації, що перебуває у розпорядженні Регіонального управління;
- у рекомендаціях: посадовим особам, що забезпечують реалізацію прав громадян на звернення та запиту на публічну інформацію про необхідність урахування балансу між дотриманням приватності і реалізацією інформаційних прав та захистом і збереженням інформації у сфері прикордонної безпеки; усім військовослужбовцям та працівникам Державної прикордонної служби України про необхідність дотримання «комп'ютерної гігієни», вжиття необхідних заходів щодо захисту та збереження інформації у сфері охорони державного кордону, обмеження розповсюдження інформації про себе, свою сім'ю, службову діяльність, колег тощо, з метою недопущення деструктивного інформаційного впливу на них та поширення інформаційних загроз у сфері діяльності Державної прикордонної служби України;
- для підвищення довіри громадян до Державної прикордонної служби України, рівня інформаційної культури особового складу, доведення до військовослужбовців правових засобів охорони інформаційних відносин у функціонуванні Державної прикордонної служби України, зокрема застосування кримінальної, адміністративної, дисциплінарної та цивільної-правової відповідальності за порушення норм інформаційного законодавства.

Розроблені Іриною КУШНІР окремі положення, висновки та рекомендації щодо удосконалення нормативно-правового регулювання відносин пов'язаних з обігом інформації у діяльності Державної прикордонної служби України дозволять покращити впровадження державної інформаційної політики, забезпечити відкритість і прозорість у діяльності Державної прикордонної служби України, сприятимуть підвищенню ефективності отримання, обробки та захисту інформації, розпорядником якої Державна прикордонна служба України, загалом сприятимуть підвищенню прикордонної безпеки й забезпеченню розвитку інформаційної складової частини системи охорони державного кордону України.

Голова комісії капітан 1 рангу Юрій АЛЕЙНИКОВ
Члени комісії
капітан 1 рангу Анатолій ХАРЛАШ
капітан 1 рангу Володимир КАПЛЯР
капітан 2 рангу Павло МАМАЙ

ДЕРЖАВНА ПРИКОРДОННА СЛУЖБА УКРАЇНИ
ЗАХІДНЕ РЕГІОНАЛЬНЕ УПРАВЛІННЯ
ЛЬВІВСЬКИЙ ПРИКОРДОННИЙ ЗАГІН

вулиця Личаківська, будинок 74, місто Львів, 71010,
телефон: (032) 239-01-91, факс: (032) 239-01-11
Код ЄДРПОУ 14321653

«26» 05 2020 № 44/5519

ЗАТВЕРДЖУЮ
Начальник Львівського прикордонного загону
підполковник Ігор РИМАРЧУК
«___» _____ 2020 р.

АКТ

про впровадження результатів
дисертаційного дослідження Ірини КУШНІР
за темою: «Теоретичні та організаційні засади нормативно-правового регулювання інформаційних відносин у діяльності Державної прикордонної служби України»

Комісія у складі:

Голова: *Перший заступник начальника Львівського прикордонного загону – начальник штабу, полковник, Василь ВІТРОВЧАК*

та членів комісії: *Заступник начальника штабу Львівського прикордонного загону – начальник відділу прикордонної служби, підполковник, Анатолій НАГІРНИЙ*

Начальник відділу зв'язку та інформаційних систем штабу Львівського прикордонного загону, підполковник, Денис КІЗІМ

склала відповідний акт про те, що результати дисертаційного дослідження на тему «Теоретичні та організаційні засади нормативно-правового регулювання інформаційних відносин у діяльності Державної прикордонної служби України», висновки, узагальнення та рекомендації розроблені Іриною КУШНІР, які були оприлюднені у наукових фахових виданнях:

1. Кушнір І. П. Види інформації, розпорядником якої є Державна прикордонна служба України, їх сутнісна характеристика. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2018. Вип. 1. URL: http://nbuv.gov.ua/UJRN/vnadpcurn_2018_1_6.
2. Кушнір І. П. Органи охорони державного кордону як суб'єкти інформаційних правовідносин. *Правові новели*. 2018. № 5. С. 71–77.
3. Кушнір І. П. Кримінально-правове забезпечення охорони інформаційних відносин у прикордонній сфері. *Питання боротьби зі злочинністю*. 2018. Вип. 36. 186 с. С. 82–93.
4. Кушнір І. П. Інформаційно-правова діяльність Державної прикордонної служби України: нормативно-правовий аспект. *Конституційно-правові академічні студії*. 2018. № 2. С. 165–170.
5. Кушнір І. П. Інформаційно-правовий статус Державної прикордонної служби України. *Приватне та публічне право*. 2018. № 4. С. 50–53.
6. Кушнір І. П. Організаційно-правові питання забезпечення захисту інформації в інформаційних системах Державної прикордонної служби України. *Прикарпатський юридичний вісник*. № 3. 2018. С. 81–84.
7. Кушнір І. П. Особливості правових відносини щодо забезпечення запиту на публічну інформацію, розпорядником якої є Державна прикордонна служба України. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2018. Вип. 4. 13 с. URL : https://nadpsu.edu.ua/wp-content/uploads/2019/02/visnuk_4_2019_ur.pdf
8. Кушнір І. П. Адміністративна відповідальність за порушення законодавства про інформацію у прикордонній сфері. *Право і інформація*. № 1(28). 2019. С. 45–51.
9. Кушнір І. П. Інформаційна відкритість у діяльності Державної прикордонної служби України. *Правова позиція*. 2019. № 1 (22). С. 30–36.
10. Кушнір І. П. Інформаційні загрози в діяльності Державної прикордонної служби України. *Підприємництво, господарство і право*. 2019. № 7. С. 147–150.
11. Кушнір І. П. Царенко О. М. Правовий режим інформації з обмеженим доступом у діяльності Державної прикордонної служби України. *Право та державне управління*. 2019. № 3. С. 180–185.
12. Кушнір І. П., Коротушак А. І. Питання удосконалення впровадження електронного урядування у Державній прикордонній службі України. *Вісник Південного регіонального центру Національної академії правових наук України*. 2019. № 20. С. 96–102.

13. Кушнір І. П., Царенко С. І., Царенко О. М. Особливості застосування дисциплінарної відповідальності за порушення інформаційного законодавства у діяльності Державної прикордонної служби України *Актуальні проблеми вітчизняної юриспруденції*. № 6. 2019. С. 80–84.

14. Кушнір І., Степанова Ю. Інформаційна безпека держави у прикордонній сфері як об'єкт державної зради. *National law journal: theory and practice*. 2018. № 4 (32). Т. 1. С. 123–126.

15. Кушнір І. Інформаційна складова підготовки та прийняття управлінських рішень в органах охорони державного кордону України. *Legea si Viata*. 2019. № 5. С. 100–104.

16. Кушнір І. П. Реалізація права на звернення громадян у Державній прикордонній службі України. *Visegrad Journal on Human Rights*. 2018. 4 (volume 2). С. 56–60.

17. Кушнір І. П. Основні тенденції інформаційної взаємодії у діяльності Державної прикордонної служби України. *Visegrad Journal on Human Rights*. 2019. 4 . С. 96–101.

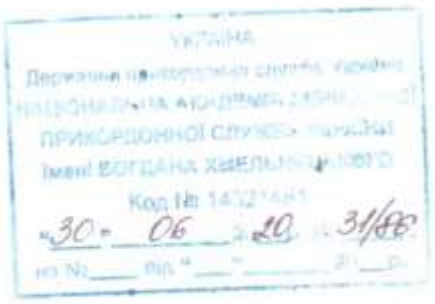
використовуються у практичній діяльності Львівського прикордонного загону в частині забезпечення інформаційних прав громадян, підвищення довіри громадян до Державної прикордонної служби України, правового регулювання обігу публічної інформації, конфіденційної, службової та таємної інформації розпорядником якої є орган охорони державного кордону, ужиття відповідних організаційно-правових заходів забезпечення захисту інформації з урахуванням сучасних інформаційних загроз.

Дисертаційне дослідження Ірини КУШНІР стосується актуальних організаційних питань у сфері інформаційної складової діяльності органів охорони державного кордону, а одержані результати й сформульовані рекомендації мають важливе практичне значення.

Голова комісії:
Перший заступник начальника Львівського прикордонного загону – начальник штабу
полковник Василь ВІТРОВЧАК

Члени комісії:
Заступник начальника штабу Львівського прикордонного загону – начальник відділу прикордонної служби
підполковник Анатолій НАГІРНИЙ

Начальник відділу зв'язку та інформаційних систем штабу Львівського прикордонного загону
підполковник Денис КІЗІМ



ЗАТВЕРДЖУЮ
Заступник ректора Національної академії Державної прикордонної служби України імені Богдана Хмельницького з наукової роботи, доктор педагогічних наук, полковник Сергій БІЛЯВЕЦЬ
"30" 06 2020 р.

АКТ
впровадження результатів дисертаційного дослідження підполковника юстиції Ірини КУШНІР в освітній та науково-дослідній діяльності Національної академії Державної прикордонної служби України імені Богдана Хмельницького

Комісія у складі:
Голови: начальника науково-дослідного відділу кандидат педагогічних наук, доцента Юрія ДЕМ'ЯНЮКА
та членів комісії: начальника навчального відділу кандидат юридичних наук, доцента, полковник Андрія СОРОКИ;
начальника кафедри теорії, історії держави і права та приватноправових дисциплін доктора юридичних наук, полковника юстиції Романа ЛЯШУКА;
начальника кафедри конституційного, адміністративного та міжнародного права, доктора юридичних наук, доцента, полковника юстиції Валентина ЗЬОЛКИ;
начальника кафедри кримінального права та процесу, доктора юридичних наук, професора, майора юстиції Наталії ОРЛОВСЬКОЇ
начальника кафедри національної безпеки (сфера прикордонної діяльності) та управління, доктора військових наук, доцента, полковника Юрія ІВАШКОВА

склала цей акт про те, що опубліковані результати дисертаційного дослідження Ірини КУШНІР за темою «Теоретичні та організаційні засади нормативно-правового регулювання інформаційних відносин у діяльності Державної прикордонної служби України», на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право використані й впроваджені в освітньому процесі кафедр: теорії, історії держави і права та приватноправових

дисциплін; конституційного, адміністративного та міжнародного права; кримінального права та процесу; національної безпеки (сфера прикордонної діяльності) та управління.

Комісією встановлено, що теоретичні висновки та практичні пропозиції, що стосуються удосконалення нормативно-правого регулювання інформаційних відносин у діяльності Державної прикордонної служби України використані у навчальному процесі при підготовці, проведенні лекційних, семінарських й практичних занять та включено до методичних матеріалів з навчальних дисциплін:

«Актуальні проблеми інформаційного права»: у темі № 1 «Інформація у правовідносинах» доповнено характеристику інформації як об'єкта інформаційного права, класифікацію інформації в діяльності Державної прикордонної служби України; у темі № 2 «Інформаційне право. Інформаційні відносини» враховано характерні особливості інформаційних відносин в діяльності Державної прикордонної служби України; тему № 3 «Правові основи інформаційної безпеки» доповнено правовим аналізом поняття «інформаційна безпека у діяльності Державної прикордонної служби України», враховано особливості інформаційної безпеки у прикордонній сфері; тему № 4 «Правові режими інформації та інформаційних ресурсів» доповнено характеристикою та елементами правового режиму інформації з обмеженим доступом у діяльності Державної прикордонної служби України»; тему № 9 «Правові основи захисту інформації» доповнено теоретичними положеннями щодо розмежування понять «захист інформації» і «інформаційна безпека»;

«Теорія держави і права»: тему № 1 «Предмет, методологія і функції теорії держави та права» доповнено теоретичними положеннями про методологію та її значення для юридичної науки; у темі № 7 «Професійна культура прикордонника» враховано теоретичне розроблення щодо необхідності формування та змісту інформаційної культури, її алгоритм; у темі № 16 «Держава та особистість» викладено положення про теоретичне обґрунтування змісту правового статусу; у темі № 30 «Юридична відповідальність», враховано особливості юридичної відповідальності військовослужбовців Державної прикордонної служби України за порушення норм інформаційного законодавства, зокрема підстави застосування дисциплінарної відповідальності за вчинені адміністративні проступки в інформаційній сфері;

«Інформаційна політика та інформаційна безпека»: тему № 1 «Концептуальні основи інформаційної політики» доповнено напрямками державної інформаційної політики, які актуальні для прикордонної сфери, теоретичним обґрунтуванням поняття «інформаційна безпека» у контексті

діяльності Державної прикордонної служби України, враховано поняття «державна політика у сфері прикордонної інформаційної безпеки», обґрунтування інформаційної відкритості як основи комунікації Державної прикордонної служби України з інформаційною сферою суспільства; у темі № 3 «Суспільно-психологічна характеристика інформаційного простору» ураховано доктринальний та нормативний аналіз інформаційних загроз у діяльності Державної прикордонної служби України, поняття «інформаційні загрози у діяльності Державної прикордонної служби України», алгоритм формування інформаційної культури у Державній прикордонній службі України;

«Адміністративне право»: у темі № 6 «Спеціальні адміністративно-правові режими» враховані особливості та місце правового режиму державної таємниці у системі інформацію з обмеженим доступом; у темі № 13 «Управління в сфері охорони державного кордону» викладено положення про необхідність забезпечення відкритості та приватності у комунікації із громадянами, з урахуванням положень чинного інформаційного законодавства та дотриманням прикордонної безпеки;

«Кримінальне право»: тему № 29 «Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації» доповнено характеристикою таємної інформації, роз'ясненням змісту поняття «недостовірні відомості» у складі злочину «незаконне перетинання державного кордону України»; у темі № 30 «Кримінальні правопорушення проти авторитету органів державної влади, місцевого самоврядування та об'єднань громадян і кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» враховано обґрунтування доцільності та важливості кримінально-правової охорони відносин пов'язаних з обігом інформації в інформаційно-телекомунікаційних системах Державної прикордонної служби України.

Використання отриманих результатів дало можливість покращити змістове наповнення навчально-методичних матеріалів для проведення лекційних, семінарських та практичних занять, а також підвищити якісний рівень підготовки слухачів (курсантів) академії.

Теоретичні та емпіричні матеріали, отримані Іриною КУШНІР за результатами власного наукового пошуку при виконанні дисертаційної роботи на здобуття наукового ступеня доктора юридичних наук, реалізовані й впроваджені у науково-дослідній діяльності Національної академії Державної прикордонної служби України імені Богдана Хмельницького, а саме для виконання науково-дослідних робіт кафедри теорії, історії держави і права та приватноправових дисциплін «Проблеми юридичної відповідальності за

правопорушення у інформаційній сфері охорони державного кордону України» (219-0107 І), «Методологічний аналіз інституту інформаційних відносин у прикордонній сфері» (219-0108 І). Зокрема використані авторські розробки Ірини КУШНІР в частині: розроблення загальнотеоретичних засад інформаційних відносин у прикордонній сфері; аналізу методологічних засад їх дослідження; з'ясування правової природи інформаційних відносин у діяльності Державної прикордонної служби України, їх видів, особливостей; характеристика елементів структури інформаційних відносин у прикордонній сфері; установлення особливостей, сутності та зміст окремих видів юридичної відповідальності за порушення норм інформаційного законодавства у сфері охорони державного кордону України; виокремлення групи правових норм у межах КК України, КУпАП, ДС ЗСУ та ЦК України, які передбачають настання юридичної відповідальності за порушення норм інформаційного законодавства у межах діяльності Державної прикордонної служби України.

Голова комісії:
Начальник науково-дослідного відділу
кандидат педагогічних наук, доцент,
полковник Юрій ДЕМ'ЯНЮК

Члени комісії:
Начальник навчального відділу
кандидат юридичних наук, доцент,
полковник Андрій СОРОКА

Начальник кафедри теорії, історії держави і права
та приватноправових дисциплін доктор юридичних наук,
полковник юстиції Роман ЛЯШУК

Начальник кафедри конституційного, адміністративного
та міжнародного права, доктор юридичних наук, доцент,
полковник юстиції Валентин ЗЬОЛКА

Начальник кафедри кримінального права та процесу
доктор юридичних наук, професор,
майор юстиції Наталя ОРЛОВСЬКА

Начальник кафедри національної безпеки (сфера прикордонної діяльності)
та управління, доктор військових наук, доцент
полковник Юрій ІВАШКОВ