МІНІСТЕРСТВО НАУКИ І ОСВІТИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВО НАУКИ І ОСВІТИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Кваліфікаційна наукова
праця на правах рукопису

ПЕРУН ТАРАС СТЕПАНОВИЧ

УДК 342.6:342.922(477)

ДИСЕРТАЦІЯ
АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

12.00.07 «Адміністративне право і процес;
фінансове право; інформаційне право»

Подається на здобуття наукового ступеня кандидата юридичних наук
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ **Т. С. Перун**

Науковий керівник: **Хомишин Ірина Юріївна**
кандидат юридичних наук, доцент

Львів – 2019

ЗМІСТ

АНОТАЦІЯ

Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». – Національний університет «Львівська політехніка», Львів, 2019.

У дисертації аналізується адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні. Обґрунтовано науковий підхід, який передбачає, що під інформаційною безпекою, в умовах розвитку інформаційного суспільства і агресії на сході України, розуміється стан захищеності інформаційних ресурсів, базах даних, інформаційних технологій і технічних засобів, призначених для збору, обробки, зберігання та передачі інформації, необхідної для реалізації прав і законних інтересів суб'єктів інформаційної діяльності, особи, суспільства та держави в інформаційному просторі від впливу особливого виду загроз, які виступають в формі цілеспрямованої або стихійної діяльності в інформаційному середовищі.

Акцентовано, що інформаційну безпеку слід розглядати як систему суспільних відносин, що виражає зв'язок між інтересами особи, суспільства та держави в сфері інформації та правовим забезпеченням їх захисту, що охоплює стан захищеності особи, суспільства та держави в інформаційному просторі, інформаційних ресурсів держави, інформації і інформаційних ресурсів, інформаційно-телекомунікаційної інфраструктури від можливих внутрішніх і зовнішніх загроз. в умовах асоціації України і ЄС та формування інформаційного суспільства.

Аргументовано, що інформаційна безпека виступає в якості об’єкта правової захисту. Правові засоби забезпечення інформаційної безпеки є провідним фактором захисту національних інтересів, а їх застосування

визначається: оптимізацією балансу відносин між правом суб'єктів інформаційних відносин на отримання інформації та правом на встановлення обмежень даних відносин з боку інших осіб щодо відомостей, володарями яких вони є; розробкою та реалізацією правових заходів захисту інформації, доступ до якої повинен обмежуватися правовими підставами в процесі захисту інформаційних ресурсів.

Звернено увагу на те, що з позиції методології права парадигма інформаційної безпеки має структуру, яку утворюють: методологія правозастосування, законодавство України, систематика адміністративного права, норми адміністративного права, адміністративно-правові відносини, юридична кваліфікація адміністративно-правових відносин, тлумачення норм права, механізм застосування закону, державна правова політика в галузі інформаційної безпеки, культура і етика застосування законодавства, яке встановлює обмеження прав і свобод людини та громадянина, стратегія та тактика діяльності суб’єктів забезпечення інформаційної безпеки, ефективність застосування законодавства, експертиза актів відомчого нормативно-правового забезпечення інформаційної безпеки.

Зазначено, що нормативно-правове забезпечення інформаційної безпеки є науково обґрунтована, послідовна система правових і інших засобів, за допомогою яких громадянське суспільство та держава здійснює вплив на інформаційні відносини (реалізація інформаційної безпеки, саморегулювання) і відносини, безпосередньо пов'язані з розробкою інформаційної безпеки, виходячи з черговості завдань і переслідуваних цілей, що виникають перед суспільством.

Вказано, що під адміністративно-правовим регулюванням забезпечення інформаційної безпеки розуміється цілеспрямований вплив на інформаційні відносини в сфері державного управління системою адміністративно-правових засобів регулювання, закріплених в нормах чинного законодавства, що визначають напрями забезпечення інформаційної безпеки в різних сферах життєдіяльності держави, суспільства і особи. Модель оптимізації

адміністративно-правового регулювання забезпечення інформаційної безпеки, маючи визначені конструктивні принципи і елементи є єдиний комплекс форм і методів впливу на зазначені відносини у вигляді адміністративно-правової моделі правого регулювання.

З урахуванням того, що інформаційна безпека є об'єктом комплексного правового регулювання різних галузей права, сутність, специфіка і основні напрями та державне регулювання та державне управлінням в сфері забезпечення інформаційної безпеки здійснюється адміністративно-правовим методом.

Підкреслено, що механізм правого регулювання це система спеціально-юридичних засобів, організованих послідовним чином, спрямованих на регулювання суспільних відносин певного виду. Конструювання механізму правового регулювання забезпечення інформаційної безпеки має здійснюватися відповідно до цілі правового регулювання. Ціль правового регулювання залежить від правової політики держави в інформаційній сфері, визначається суб'єктами, що здійснюють нормативно-правове регулювання інформаційної безпеки. Вирішальну роль у формуванні цілей правового регулювання забезпечення інформаційної безпеки, що мають транснаціональний характер, грають норми визначені в актах міжнародних та наднаціональних організацій ЄС і НАТО.

Констатується, що державне управління в сфері забезпечення інформаційної безпеки полягають у створенні умов для гармонійного розвитку національної інформаційної інфраструктури, для реалізації конституційних прав і свобод людини та громадянина, законних інтересів особи, суспільства та держави у національному інформаційному просторі, у отриманні інформації та користування нею фізичними та юридичними особами з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності України, політичної, економічної та соціальної стабільності, в забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

Вказується, що адміністративно-правове регулювання забезпечення інформаційної безпеки є сукупність закріпленої в законодавстві системи заходів і прийомів, спрямованих на забезпечення безпечної діяльності в інформаційному просторі що динамічно розвивається, фізичних і юридичних осіб, сприятливої для інновацій, інвестицій, яка забезпечує населенню високий рівень життя і економічний прогрес.

Обґрунтовується, що система суб'єктів забезпечення інформаційної безпеки – цілісна сукупність елементів, що перебувають у обумовлених функціями забезпечення інформаційної безпеки суспільних відносинах, об'єднаних сферою інтересів і потреб, що відображають правові характеристики адміністративно-правових засобів регулювання, зміст і елементи правового статусу суб'єктів, які беруть участь у відносинах, регульованих нормами інформаційного права, системними за змістом. Для забезпечення інформаційної безпеки характерна багаторівнева система суб'єктів, заснована на принципі єдності та диференціації.

Вказано, що адміністративно-правовий режим забезпечення інформаційної безпеки є комплексною юридичною категорією, дослідження якої доцільно здійснювати на міждисциплінарній основі із застосуванням методології інформаційного права з акцентуванням уваги на інформаційному, комунікаційному та синергетичному аспектах, оскільки за цільовим призначенням адміністративно-правовий режим забезпечення інформаційної безпеки є складною, відкритою, незавершеною інформаційно-комунікаційною системою, що забезпечують правове регулювання процедурних (включаючи інформаційні) відносин, через систему адміністративних процедур які характеризуються високим ступенем динамічності у регулюванні, завдяки новітніх програмних компонентам і засобам комунікації, охоплюючи різні за обсягом напрями – забезпечення інформаційної безпеки особи, суспільства та держави.

Констатовано, що особливість організаційно-правового забезпечення адміністративно-правового режиму інформаційної безпеки обумовлює

застосування технічних стандартів інформаційної безпеки прийнятих у ЄС і НАТО, які сформульовані в результаті виявлення типових (повторюваних) правових випадків і уніфікації техніко-юридичних норм, які регламентують порядок діяльності суб'єктів забезпечення інформаційної безпеки, у контексті відносин, що виникають з адміністративних та інших публічних правовідносин, з метою орієнтації положень на однаковість процедури усунення загроз у інформаційно-телекомунікаційних системах і в національному інформаційному просторі, що інтерпретується як особливий спосіб юрисдикційного усунення прогалин у праві та протиріч, що виникають під час діяльності особи та суб'єктів господарської діяльності у інформаційній сфері.

Показано, що особливості адміністративно-правових режимів забезпечення інформаційної безпеки розкриваються через механізм саморегулювання за участю публічно-правових суб’єктів, встановлення балансу інтересів, у контексті правового регулювання реалізації законних інтересів власників критичної інформаційної інфраструктури, що випливає з адміністративних і інших публічних правовідносин утворюючи баланс публічних і приватних інтересів.

Підвищення ефективності правового регулювання інформаційної безпеки неможливо без опори на теоретичний фундамент, формування якого, в свою чергу, має враховувати змістовні основи правової ідеї, суть якої полягає в нерозривній єдності ідей незалежності, територіальної цілісності та суверенітету, справедливості та національного інтересу, що можливо на основі реалізації комплексу правових заходів, до яких відносяться: чітке відображення в праві і державних інститутах орієнтації на поєднання публічних і приватних економічних інтересів в інформаційній сфері; постійне та послідовне використання всіх правозахисних механізмів і процедур для подолання конфліктів в інформаційній сфері; підвищення правового рівня свідомості та діяльності державних службовців, представників всіх гілок і рівнів влади, населення країни.

Доказано, що як інструмент державного впливу на адміністративні

процеси в сфері забезпечення інформаційної безпеки, слід більш активно використовувати взаємодію суб'єктів забезпечення інформаційної безпеки, визначених Доктриною інформаційної безпеки України, де законодавчі параметри є визначальними і обумовлюють подобу структурно-владних форм, що конкретизують характеристики адміністративно-правового режиму предметно-конкретним змістом з реалізації техніко-юридичних норм, втілену в інституційно-логічну організацію.

Ключові слова: інформаційна безпека, адміністративно-правовий механізм, суб'єкти забезпечення інформаційної безпеки, правові норми, інформаційні технології, критично важлива інформаційна інфраструктури.

SUMMRY

Perun T. S. Administrative and legal mechanism of information security in Ukraine. – Qualified scientific work on the rights of the manuscript.

Dissertation for the degree of Doctor of Law in specialty 12.00.07 – «Administrative law and process; finance law; information law». – Lviv Polytechnic National University of the Ministry of Education and Science of Ukraine, Lviv Polytechnic National University of the Ministry of Education and Science of Ukraine, Lviv, 2019.

The dissertation analyzes the administrative and legal mechanism of ensuring information security in Ukraine. The scientific approach is substantiated, which assumes that under information security, in the conditions of development of information society and aggression in the east of Ukraine, the state of security of information resources, databases, information technologies and technical means intended for gathering, processing, storage and transfer of information necessary is understood. to realize the rights and legitimate interests of information subjects, persons, society and the state in the information space from the influence of a specific type of threats, which appear in the form of purposeful Language not or spontaneous activity in the information environment.

It is emphasized that information security should be considered as a system of public relations, which expresses the connection between the interests of the person, society and the state in the sphere of information and the legal security of their protection, which covers the state of protection of the person, society and the state in the information space, information resources of the state, information and information resources, information and telecommunication infrastructure from possible internal and external threats. in the context of the association between Ukraine and the EU and the formation of an information society.

It is argued that information security acts as an object of legal protection. Legal means of ensuring information security are a leading factor in the protection of national interests, and their application is determined by: optimizing the balance of relations between the right of information relations subjects to receive information and the right to set restrictions on these relations by other persons with regard to the information they own; development and implementation of legal measures for the protection of information, access to which should be limited to the legal bases in the process of protection of information resources.

Attention is drawn to the fact that from the standpoint of the methodology of law, the paradigm of information security has a structure, which is formed by: the methodology of law enforcement, the legislation of Ukraine, systematic of administrative law, norms of administrative law, administrative-legal relations, legal qualification of administrative-legal relations, interpretation of rules of law, mechanism application of the law, state legal policy in the field of information security, culture and ethics of the application of legislation that establishes restrictions on human rights and freedoms may arise, strategy and tactics of the subjects of information security, the effectiveness of law enforcement expertise of acts of departmental regulatory information security.

It is stated that the normative legal support of information security is a scientifically grounded, consistent system of legal and other means by which civil society and the state influence the information relations (implementation of information security, self-regulation) and relations directly related to the development

of information security. based on the priority of the tasks and goals pursued by society.

It is stated that administrative and legal regulation of providing information security means purposeful influence on information relations in the sphere of public administration of the system of administrative and legal means of regulation, enshrined in the rules of the current legislation, which determine the directions of providing information security in various spheres of life of the state, society and person. Optimization model administrative and legal regulation of ensuring information security, having certain structural principles and elements, is the only set of forms and methods of influencing these relations in the form of administrative and legal model of right regulation.

Given that information security is the subject of comprehensive legal regulation of various branches of law, the essence, specificity and main directions and state regulation and public administration in the field of information security is carried out by the administrative-legal method.

It is emphasized that the mechanism of right regulation is a system of special legal means, organized in a consistent way, aimed at regulating social relations of a certain kind. The design of a mechanism for the legal regulation of information security should be carried out in accordance with the purpose of the legal regulation. The purpose of legal regulation depends on the legal policy of the state in the information sphere, determined by the entities that carry out regulatory regulation of information security. The rules set out in the acts of international and supranational organizations of the EU and NATO play a decisive role in shaping the objectives of the legal regulation of information security, which are transnational in nature.

It is stated that the state administration in the field of information security consists in creating conditions for the harmonious development of the national information infrastructure, for the realization of the constitutional rights and freedoms of the individual and the citizen, the legitimate interests of the individual, society and the state in the national information space, in obtaining information and using it physical and legal entities in order to ensure the integrity of the constitutional system,

sovereignty and territorial integrity of Ukraine, political, economic social and social stability, in order to ensure the rule of law and order, the development of equal and mutually beneficial international cooperation.

It is stated that the administrative and legal regulation of information security is a set of measures and techniques enshrined in the legislation aimed at ensuring safe activity in the dynamically developing information space, individuals and legal entities, favorable for innovation, investment, which provides a high standard of living for the population and economic progress.

It is substantiated that the system of information security entities is a complete set of elements that are in the defined functions of information security of public relations, united by the sphere of interests and needs, reflecting the legal characteristics of administrative and legal means of regulation, content and elements of the legal status of sub entities that participate in relationships governed by information law, systemic in content. To ensure information security is characterized by a multi-level system of subjects based on the principle of unity and differentiation.

It is stated that the administrative-legal regime of providing information security is a complex legal category, the research of which is advisable to be conducted on an interdisciplinary basis using the methodology of information law, with emphasis on information, communication and synergetic aspects, since the purpose of administrative-legal regime is the provision of information security. complex, open, incomplete information and communication system providing legal regulation of urnyh (including information) relations through administrative procedures which are characterized by high dynamism in regulation thanks to the newest software and communication components, including different volume areas - information security of individuals, society and the state.

It is stated that the peculiarity of organizational and legal support of the administrative and legal regime of information security determines application of technical standards of information security adopted in the EU and NATO, which are formulated as a result of identification of typical (recurring) legal cases and unification of technical and legal norms that regulate the order of activity of

information security entities, in the context of relations arising from administrative and other public relations, with a view to orienting the provisions on the uniformity of the procedure for eliminating threats in the information and telecommunication systems and in the national interpreter uyetsya as a special way jurisdictional gaps in law and contradictions that arise when business persons and business entities in the information sphere.

It is shown that the peculiarities of administrative and legal regimes for providing information security are revealed through the mechanism of self-regulation with participation of public-legal entities, establishment of balance of interests, in the context of legal regulation of the legitimate interests of the owners of critical information infrastructure arising from administrative and other public legal relationships. public and private interests.

Improving the effectiveness of the legal regulation of information security is impossible without reliance on a theoretical foundation, the formation of which, in turn, must take into account the substantive foundations of the legal idea, the essence of which is the indissoluble unity of ideas of independence, territorial integrity and sovereignty, justice and national interest, possible national interest. implementation of a set of legal measures to which they relate: a clear reflection in the law and state institutions of the orientation on the combination of public and private economic interests in the information sphere; continuous and consistent use of all human rights mechanisms and procedures for overcoming conflicts in the information sphere; raising the legal level of consciousness and activity of civil servants, representatives of all branches and levels of government, population of the country.

It is proved that as an instrument of state influence on administrative processes in the field of information security, the interaction of information security entities, defined by the Information Security Doctrine of Ukraine, where legislative parameters are decisive and determine the similarity of structural-power forms specifying characteristics, should be used more actively administrative-legal regime of subject-specific content on the implementation of technical and legal norms, embodied in an institutional-logical organization.

Key words: information security, administrative and legal mechanism, subjects of providing information security, legal norms, information technologies, critical information infrastructure.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Перун Т. С. Історія розвитку права на інформацію. *Митна справа*. 2013. № 2 (86). Ч. 2. К. 1. С. 417–422.

2. Перун Т. Загальна характеристика правовідносин у сфері забезпечення інформаційної безпеки в Україні. *Вісник Національного університету «Львівська політехніка»*. Серія: Юридичні науки. 2017. № 861. С. 328–332.

3. Перун Т. Методологічні засади дослідження механізму забезпечення інформаційної безпеки в Україні. *Вісник Національного університету «Львівська політехніка»*. Серія: Юридичні науки. 2017. № 865. С. 303–307.

4. Перун Т. С. Принципи забезпечення інформаційної безпеки України в умовах євроінтеграції. *Eurasian Academic Research Journal*. 2017. № 11 (17). С. 108–114. (Вірменія).

5. Перун Т. Значення адміністративної відповідальності в системі заходів забезпечення інформаційної безпеки. *Право України*. 2017. № 10. С. 202–209.

6. Перун Т. С. Шляхи покращення взаємодії між Україною та ЄС у сфері забезпечення інформаційної безпеки. *Наукові записки Інституту законодавства Верховної Ради України*. 2018. № 5. С. 26–30.

які засвідчують апробацію матеріалів дисертації:

7. Перун Т. С. Адміністративна відповідальність в системі заходів забезпечення інформаційної безпеки. *ІТ-право: проблеми і перспективи розвитку в Україні*: збірник матеріалів ІІ Міжнародної науково-практичної конференції (Львів, 17 листопада 2017 р.) Львів, Національний університет «Львівська політехніка». 2017. С. 155–160.

8. Перун Т. С. Адміністративно-правова відповідальність за правопорушення у сфері інформаційної безпеки. *Адміністративне право і процес: проблеми та перспективи розвитку: тези* Всеукраїнської заочної науково-практичної конференції. (м. Львів, 30 березня 2018 р.). [у 2 ч.]. Київ: МП «Леся». Ч. 1 С. 166–170.

9. Перун Т. Провайдер як суб'єкт інформаційного права. *Політичні, соціальні, економічні, психологічні та правові механізми регулювання міграційних процесів у сучасних умовах:* матеріали Міжнародної заочної науково-практичної конференції. (м. Львів, 17 травня 2018 р.). Київ: МП «Леся». С. 82–84.

10. Перун Т. Інформаційна безпека країн ЄС: проблеми та перспективи правового регулювання. *Правові засади європейської та євроатлантичної інтеграції України: досягнення та перспективи*: матеріали учасників ІІ заочної науково-практичної конференції (Львів, 23 листопада 2018 р.). Львів, 2018. С. 140–143.

ВСТУП

Актуальність теми дослідження обумовлена соціальними, правовими та економічними чинниками, теоретичними та практичними проблемами адміністративно-правового регулювання та правозастосовної практики в інформаційній сфері. Реформування суспільного життя в Україні після Революції гідності торкнулося, в першу чергу, сфери адміністративного законодавства. Останнім часом значно змінилася ситуація в інформаційній сфері, істотно трансформувалися її окремі складові, але в цілому проблема забезпечення інформаційної безпеки зберігається, оскільки суспільство постійно зустрічається з новими викликами та загрозами, пов’язаними з військовою агресією Росії. Відповідно до цієї реальності держава шукає нові методи та засоби впливу на учасників відносин у сфері інформаційної безпеки. Ситуація в ній постійно змінюється, адже інституційні перетворення спрямовані на вдосконалення правових інститутів, що забезпечують реалізацію прав в інформаційній сфері, підвищення ефективності системи державного управління, розвиток людського капіталу та громадянського суспільства, стійке функціонування та розвиток національної економіки, подолання технологічного та інфраструктурного відставання в сфері застосування інформаційно-комунікаційних технологій.

Використання особливих форм і методів державного управління при забезпеченні інформаційної безпеки пояснюється необхідністю своєчасного реагування на виникаючі загрози політичного, економічного та військового характеру, оскільки в таких умовах використання звичайних традиційних правових механізмів не завжди призводить до очікуваного результату.

Держава є основним суб’єктом забезпечення інформаційної безпеки. Головну роль в ефективності забезпечення інформаційної безпеки має відіграти адміністративне право як право, яке регламентує управлінську діяльність суб'єктів забезпечення інформаційної безпеки. Норми адміністративного права забезпечують реалізацію механізму управління в різних сферах життєдіяльності, встановлюють відповідні правові режими, які повинні стати ефективним

інструментом державного управління в досліджуваній сфері.

У межах європейської інтеграції, головна мета якої полягає в корекції основних функцій держави, мають створюватися умови для розвитку інформаційних свобод, намічатися стратегічні орієнтири впровадження стандартів НАТО, повинна реалізовуватися політика ефективного державного управління з залученням нових організаційних структур і використання механізму реалізації норм адміністративного права суб'єктами забезпечення інформаційної безпеки.

Концептуальне конструювання системи забезпечення інформаційної безпеки України має певну складність у зв'язку з багатьма аспектами та передбачає розробку теоретико-методологічних питань і правового (зокрема, адміністративно-правового) механізму, основних напрямів, форм і методів реалізації відповідних нововведень. Основним елементом адміністративно-правового механізму забезпечення інформаційної безпеки є адміністративно-правовий режим. Сьогодні назріла необхідність дослідження адміністративно-правового механізму забезпечення інформаційної безпеки, від якого залежить ефективність реалізації адміністративно-правових заходів, в кінцевому підсумку – ступінь захищеності охоронюваних державних, громадських інтересів і інформаційних прав людини та громадянина.

Різні аспекти національної безпеки загалом та інформаційної безпеки зокрема, окремих її складових, питання адміністративно-правового регулювання та забезпечення інформаційної безпеки досліджували вчені-юристи В. Б. Авер’янов, О. Ф. Андрійко, О. А. Баранов, Л. Р. Біла, Ю. П. Битяк, Н. П. Бортник, К. В. Бондаренко, В. М. Брижко, В. М. Гаращук, Т. О. Гаврилюк, І. С. Грищенко, Є. В. Додін, Д. Г. Заброда, В. В. Зуй, Ю. М. Дмитренко, О. М. Музичук, В. К. Колпаков, Т. О. Коломоєць, О. В. Кузьменко, В. К. Колпаков, Р. А. Калюжний, М. В. Ковалів, С. В. Ківалов, Д. М. Лук’янець, В. Л. Ортинський, О. І. Остапенко, І. Д. Пастух, С. В. Пєтков, А. І. Собакарь, Ю. С. Шемшученко, В. О. Шамрай та інші.

Окремі аспекти, які так чи інакше є інформаційною складовою доказів,

утворених із використанням інформаційно-комунікаційних технологій, з позиції теорії інформаційного права досліджували І. В. Арістова, В. М. Глушков, Р. Гровер, С. С. Єсімов, Д. Коен, П. Малі, А. І. Марущак, А. М. Мірошниченко, О. Ю. Тихомиров, Е. Шмидт і інші.

Теоретико-правову основу дисертаційного дослідження склали роботи вчених з теорії держави і права, конституційного та адміністративного права: Ж-Л. Бержеля, О. Ерліха, М. С. Кельмана, П. М. Рабіновича, П. Соммера, Е. Шмідт-Ассманна та інших.

Значні зміни організаційно-правових основ в цій сфері, зокрема, реформа органів виконавчої влади, прийняття Доктрини інформаційної безпеки України, новації в законодавчому регулюванні діяльності державних органів в сфері забезпечення інформаційної безпеки, вимагають подальшого наукового осмислення і аналізу. Однак розвиток теорії та практика адміністративно-правового режиму забезпечення інформаційної безпеки, на жаль, не відповідають вимогам ситуації, що склалася у зв'язку з веденням Російською Федерацією гібридної війни проти України, оскільки питання правового забезпечення інформаційної безпеки стали предметом наукового вивчення лише на початку XXI ст., коли інформаційна безпека стала розглядатися як органічна тріада: безпека особи, суспільства та держави.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація виконана в контексті наукових досліджень відповідно до пункту 3.4.2.5 «Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук» Національної академії наук України на 2019–2023 роки, пункту 9 розділу «Правове забезпечення інформаційної сфери України» Пріоритетних напрямів розвитку правової науки на 2016–2020 роки Національної академії правових наук України, пункту 9.1 «Реалізація державної політики та пріоритетних напрямів створення сучасної інформаційної інфраструктури України» Переліку пріоритетних напрямів наукового забезпечення діяльності органів внутрішніх справ України на період 2015–2019 роки, затвердженого наказом МВС України від 16 березня 2015 року

№ 275, та у межах науково-дослідної роботи кафедри адміністративного та інформаційного права Навчально-наукового Інституту права та психології Національного університету «Львівська політехніка»: «Адміністративно-правове забезпечення прав і свобод людини та громадянина в умовах розбудови правової держави» (державний реєстраційний номер 0116U004099).

Мета і завдання дослідження. *Метою* наукового дослідження є з'ясування і аналіз концептуальних та організаційно-правових основ адміністративно-правового забезпечення інформаційної безпеки органами державної влади та іншими уповноваженими органами, вироблення на цій основі пропозицій і рекомендацій, які сприятимуть підвищенню ефективності забезпечення інформаційної безпеки.

Для досягнення поставленої мети сформульовано такі *завдання*:

– розглянути інформаційну безпеку як систему суспільних відносин і об'єкт правової охорони;

– проаналізувати вихідні методологічні засади дослідження інформаційної безпеки;

– узагальнити нормативно-правове забезпечення інформаційної безпеки в Україні;

– розкрити поняття та принципи побудови механізму правового регулювання забезпечення інформаційної безпеки;

– здійснити аналіз адміністративно-правового регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки;

– охарактеризувати систему суб'єктів забезпечення інформаційної безпеки;

– визначити особливості адміністративно-правового режиму інформаційної безпеки;

– показати шляхи підвищення ефективності адміністративно-правового забезпечення інформаційної безпеки в Україні.

Об'єктом дослідження є сукупність суспільних відносин, що

складаються в процесі реалізації адміністративно-правового механізму забезпечення інформаційної безпеки.

Предмет дослідження становлять правові норми, які регламентують адміністративно-правовий механізм забезпечення інформаційної безпеки.

Методи дослідження. Методи дослідження. Методологічною основою дослідження виступає міждисциплінарний підхід, сукупність філософських, загальнонаукових (аналіз, синтез, індукція, дедукція, абстрагування, моделювання) та спеціально-наукових методів, які забезпечують об’єктивний аналіз досліджуваного предмета. За допомогою діалектичного методу пізнання здійснювалось дослідження та обґрунтування основних понять, які використовуються в роботі та вивченні правових явищ у контексті їхнього виникнення, функціонування, розвитку та взаємозв’язку (пп. 1.1, 1.2, 1.3). Порівняльний метод використовувався при дослідженні заходів адміністративно-правового забезпечення інформаційної безпеки (п. 2.1); історичний метод – для дослідження формування правових поглядів на поняття забезпечення інформаційної безпеки (пп. 1.1, 2.2); системно-структурний метод дав змогу визначити завдання та принципи діяльності суб'єктів забезпечення інформаційної безпеки щодо захисту прав і свобод людини та громадянина (пп. 1.1, 1.3, 2.2, 2.3, Розділ 3); спеціально-юридичний метод використовувався для визначення юридичної природи досліджуваних явищ та формулювання відповідних юридичних понять (пп. 1.3, Розділ 2); метод інтерпретації (тлумачення) використовувався для з’ясування змісту правових норм адміністративно-правового механізму забезпечення інформаційної безпеки (Розділи 2, 3), соціологічний метод – при проведенні анкетування респондентів, аналізі та узагальненні результатів анкетування (пп. 2.1; 2.2; Розділ 3).

Науково-теоретичним підґрунтям дисертації стали наукові розробки фахівців у галузі права, інформатики, інформаційно-комунікаційних технологій та інших сфер людської життєдіяльності.

Нормативно-правовою основою дослідження є Конституція України, закони України, укази Президента України, нормативно-правові акти Кабінету

Міністрів України, відомчі нормативно-правові акти, нормативно-правові акти Європейського Союзу, держав-членів ЄС, Європейського суду з прав людини, США, Японії.

Емпіричну базу дослідження становлять офіційні дані та матеріали правозастосовної практики органів державної влади, наділених повноваженнями в галузі забезпечення інформаційної безпеки, судова практика. У роботі використовувалися матеріали науково-практичних конференцій, дані періодичної преси, офіційних сайтів, статистичні дані, аналітичні матеріали, результати опитування 150 представників Національної поліції, Державної служби спеціального зв'язку та захисту інформації України, вищих навчальних закладів юридичного спрямування м. Львова.

Наукова новизна одержаних результатів полягає в тому, що дисертаційна робота є одним з перших досліджень адміністративно-правого механізму забезпечення інформаційної безпеки, яке проведено в Україні в умовах інформаційної війни, розв'язаної Росією проти України, розвитку інформаційного суспільства та асоціації України і ЄС, та містить аналіз доктрини та практики держав-членів ЄС з питань інформаційної безпеки. На підставі вивчення наукових джерел, практики Європейського суду з прав людини, законодавства проведено порівняльно-правове дослідження розвитку інформаційної безпеки та доктринальних підходів щодо адміністративно-правого механізму забезпечення інформаційної безпеки. Найсуттєвішими результатами дослідження, що зумовлюють новизну та визначають внесок автора у розробку зазначеної проблематики, є:

уперше:

– на основі системно-структурного аналізу законодавства України та Європейського Союзу з урахуванням стандартів НАТО у сфері інформаційної безпеки запропоновано поняття адміністративно-правого механізму забезпечення інформаційної безпеки;

– подана характеристика системи суб'єктів забезпечення інформаційної безпеки, позначених у Доктрині інформаційної безпеки України, як структурно-

функціональної моделі предметної діяльності, виходячи з оцінки правого регулювання окремих органів у зазначеній сфері;

– сформульовані науково обґрунтовані пропозиції щодо організації взаємодії та координації функціонування системи суб'єктів забезпечення інформаційної безпеки України з можливістю створення спеціального органу для координації діяльності державних та недержавних суб’єктів – власників критично важливої інформаційної інфраструктури в сфері забезпечення інформаційної безпеки;

– запропонована нова юридична конструкція адміністративно-правового режиму забезпечення інформаційної безпеки;

удосконалено:

– нормативно-правове забезпечення інформаційної безпеки в Україні;

– методологію аналізу засад дослідження інформаційної безпеки завдяки використанню методів програмно-цільового управління складними соціальними та технологічними системами в регулюванні процесів з чітко заданими цільовими параметрами забезпечення інформаційної безпеки, що характеризують поведінку функціональної системи суб'єктів забезпечення інформаційної безпеки в умовах високого навантаження зовнішнього середовища;

– аналіз адміністративно-правового регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки на підставі застосування теорії систем і системного підходу, представленої у формі функціональної моделі, елементи якої дозволяють виробляти теоретичну інтерпретацію методами аналогії структур;

набули подальшого розвитку:

– дослідження інформаційної безпеки як системи суспільних відносин і об'єкту правової охорони;

– поняття та принципи побудови механізму правового регулювання забезпечення інформаційної безпеки;

– характеристика системи суб’єктів забезпечення інформаційної безпеки;

– дослідження особливостей адміністративно-правового режиму

інформаційної безпеки;

– шляхи підвищення ефективності адміністративно-правового забезпечення інформаційної безпеки в Україні.

На підставі висновків запропоновано внести доповнення до законодавства України у сфері забезпечення інформаційної безпеки.

Практичне значення одержаних результатів дослідження визначено тим, що вони можуть бути використані у подальших дослідженнях із забезпечення інформаційної безпеки, у правозастосуванні та правотворчості, при розробці програм навчальних дисциплін і викладанні спеціальних курсів, покладені в основу методичних рекомендацій суб'єктам, які здійснюють діяльність у сфері забезпечення інформаційної безпеки:

– *у науково-дослідній сфері* – для подальшої розробки актуальних питань теорії забезпечення інформаційної безпеки, визначення шляхів адаптації чинного національного адміністративного законодавства до вимог Європейського Союзу;

– *у правотворчості* – для подальшого розвитку законодавства з питань забезпечення інформаційної безпеки *(Довідка підкомітету з питань державної інформаційної політики та інформаційної безпеки Комітету Верховної Ради України з питань свободи слова та інформаційної політики від 24.04.2019 р.)*;

– *у правозастосовній та практичній діяльності* – для підвищення ефективності практичної діяльності державних органів і інститутів громадянського суспільства щодо захисту інформаційних прав, свобод і законних інтересів фізичних і юридичних осіб *(Довідка Державної організації «Національний офіс інтелектуальної власності» №70/2019 від 24.04.2019 р.*;

– *у навчальному процесі* – під час проведення занять з навчальних дисциплін «Адміністративне право», «Інформаційне право» *(Довідка Національного університету «Львівська політехніка» від 09.09.2019 р.)*.

Особистий внесок здобувача. Сформульовані в дисертації положення, узагальнення, висновки, рекомендації, пропозиції обґрунтовані на підставі особистих досліджень автора в результаті опрацювання й аналізу наукових,

нормативних і статистичних джерел.

Апробація результатів дисертації. Основні ідеї положень дисертаційної роботи були апробовані на: міжнародній науково-практичній конференції «ІТ-право: проблеми і перспективи розвитку в Україні» (м. Львів, 17 листопада 2017 р.); Всеукраїнській науково-практичній конференції «Адміністративне право і процес: проблеми та перспективи розвитку» (м. Львів, 30 березня 2018 р.); Всеукраїнській науково-практичній конференції «Правові засади європейської та євроатлантичної інтеграції України: досягнення та перспективи» (м. Львів, 23 листопада 2018 р.).

Публікації. Основні положення та результати дисертації викладено в 6 наукових статтях у журналах, що входять до переліку фахових наукових видань України, 3 із них внесено до міжнародної наукометричної бази «Index Copernicus International», 1 стаття – у закордонному виданні, 4 тези виступів – на науково-практичних заходах.

Обсяг і структура дисертації. Структура й обсяг дисертаційної роботи обумовлені метою, завданнями та предметом дослідження. Дисертація складається з вступу, трьох розділів, що поділені на вісім підрозділів, висновків, списку використаних джерел та додатків. Повний обсяг дисертації становить 268 сторінок, із них 192 сторінки основного тексту. Список використаних джерел – 308 найменувань – 33 сторінки, додатки – 28 сторінок.

РОЗДІЛ 1

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, ОСОБИ ТА СУСПІЛЬСТВА ЯК ОБ'ЄКТ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ

1.1 Інформаційна безпека як система суспільних відносин і об'єкт правової охорони

Теорія розвитку інформаційного суспільства показує відносно невисокий ступень критичності досліджень щодо можливостей які відкриваються на основі використання інформаційних технологій. Це зумовлює приділенню недостатньої уваги до нових видів небезпеки, загроз, що виникають в суспільстві, в наслідок негативних ефектів застосування інформаційних технологій. Проблема інформаційної безпеки виникла на ґрунті глобального протиріччя між можливостями інформаційних технологій, с однієї сторони, и негативними ефектами, небезпеками, загрозами їх застосуванням в деструктивних цілях по відношенню до особи, суспільства, держави – з другої.

У даний час, у контексті реалізації Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони одним з головних стратегічних пріоритетів є розвиток інформаційного суспільства та впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя та в діяльність органів публічної влади [1].

Як зазначено в «Стратегії розвитку інформаційного суспільства в Україні» (прийнято від 15 травня 2013 року), метою формування та розвитку інформаційного суспільства в Україні є підвищення якості життя громадян, забезпечення конкурентоспроможності України, розвиток економічної, соціально-політичної, культурної та духовної сфер життя суспільства, вдосконалення системи державного управління на основі використання інформаційних і телекомунікаційних технологій [2].

У процесі досягнення цієї мети на перший план виходять питання, пов'язані із забезпеченням інформаційної безпеки, яка, як вказано у Аналітичній доповіді до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 році», є одним із пріоритетних напрямів забезпечення національної безпеки. Президент України звертає увагу на те, що надійна робота інформаційних ресурсів, систем управління та зв'язку має виключне значення для обороноздатності країни, для сталого розвитку економіки та соціальної сфери, для захисту суверенітету України в найширшому сенсі цього слова [3, с. 47-48]. При цьому відповідні відомства фіксують постійне зростання комп'ютерних атак на національні інформаційні ресурси, зростання злочинності в сфері використання інформаційних ресурсів і комп'ютерних систем.

Дані негативні тенденції є наслідком активних інформаційних процесів, що відбуваються в Україні і в світі, коли інформаційні відносини охоплюють весь спектр суспільного буття, виникають і існують у всіх сферах життєдіяльності.

Водночас, як зазначають дослідники, сьогодні тільки починає усвідомлюватися проблема «людина в інформаційному суспільстві», виникає розуміння того, що інтереси особистості в інформаційній сфері полягають у реалізації конституційних прав людини та громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного і інтелектуального розвитку та у захисті інформації, що забезпечує особисту безпеку.

У науковій літературі цілком виправданою є теза, згідно з якою стрімкий розвиток і широке використання інформаційно-комп'ютерних технологій привело до формування фундаментальної залежності критичних національних інфраструктур від стану їх захищеності в інформаційному плані, що знайшло відображення у Законі Україні від 5 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України» [4]. Крім того останнім часом інформація набуває нових властивостей, що визначають як її соціально-

економічну цінність, так і правовий зміст.

В першу чергу в даний час інформація усвідомлюється як важливий економічний ресурс. Використання інформаційних ресурсів, ефективна організація інформаційних процесів можуть істотно збільшити рентабельність багатьох видів продуктивної діяльності, сприяти вирішенню політичних, військово-політичних, соціально-економічних, культурно-просвітницьких і соціальних проблем. Інформація стає економічним товаром, що стимулює в усьому світі зростання нового сегменту національної економіки – інформаційних послуг.

Як будь-який товар інформація має власника, який володіє правом розпоряджатися інформацією на свій розсуд, а її несанкціоноване використання тягне за собою матеріальні втрати для її правовласника, несанкціоновані дії з інформацією стають підставою для настання шкоди для держави, громадян, суб'єктів господарювання.

При цьому в розвинених країнах інформація перетворилася в основний предмет праці. Тобто галузь виробництва, де фізична робота традиційно переважала, перейшла на інформаційні засади, відповідно інформація стає засобом виробництва, яке також вимагає відповідної правової захисту. Слід вказати і на те, що в останні десятиліття інформація набуває властивостей потужного засобу впливу на суспільно-політичні, ідеологічні та соціально-економічні процеси, стає свого роду зброєю, яке вимагає створення системи протидії, захисту інформаційних ресурсів, що належать державним органам, що становлять державну, лікарську, особисту і ніші види таємниць.

О. А. Нищеменко посилаючись на роботу «Національна безпека України: сутність, структура та напрямки реалізації» (О. Г. Данільян, О. П. Дзюбань, В. К. Пархоменко, Д. В. Дмитрієв) зазначає, що розвиток інформаційних засобів веде до можливості встановлення такого тотального контролю над людьми, якого ще не було в історії людства [5, с. 19].

У сучасних умовах інформація стає стратегічним ресурсом, правова зашита якого диктується необхідністю розвитку економіки, формування

громадянського суспільства, забезпечення безпеки держави та громадян. У зв'язку з цим, інформаційна безпека є найважливішою складовою національної безпеки в цілому, а проблема забезпечення інформаційної безпеки є надзвичайно актуальною.

У зв'язку з цим актуалізується проблема правового регулювання процесів, в яких інформація починає виступати як основа суспільних відносин, що виникають при реалізації інформаційних потреб держави, особи та суспільства, тобто при створенні, одержанні, обробці, накопиченні, зберіганні, пошуку, поширення та споживання інформації, при створенні та використанні інформаційних систем, інформаційних технологій і засобів інформаційної безпеки.

На нашу думку, методологічно вірним, з точки зору логіки наукового дослідження, буде аналіз поняття «інформаційна безпека» на рівні термінології. Про важливість термінологічного підходу до розгляду проблем у галузі інформаційної безпеки пишуть С. Ф. Гончар, Г. П. Леоненко, О. Ю. Юдін. Розбіжності у вживанні понять і термінів, їх нез'ясованість, не розмежованість за обсягом та значенням, як у наукових дослідженнях, так і у міжнародно-правових актах, свідчать про те, що осмислення основних понять, складових елементів системи забезпечення інформаційної безпеки критичної інфраструктури з їх багатогранними проявами та наслідками ще не завершено. Так, сьогодні провідні країни світу проходять шлях стандартизації термінології та підходів у сфері захисту критичної інфраструктури, зокрема, ці процеси активно відбуваються в Сполучених штатах Америки [6, с. 35]. На сьогоднішній день терміни починають відігравати важливу роль в юриспруденції, а для розкриття змісту досліджуваного поняття слід звернутися до аналізу поняття «інформація».

Доцільно зазначити, що складність визначення даного поняття полягає в тому, що кожна наука, має справу з інформацією пропонує свою дефініцію. Відзначимо, що у витоків інформатики як науки стояв Н. Вінер, який визначав інформацію як позначення змісту, отриманого з зовнішнього світу в процесі

нашого пристосування до нього і пристосування наших почуттів. Інформація є інформація, а не матерія і не енергія [7, с. 201]. Він стверджував, що процес отримання та використання інформації є процесом нашого пристосування до випадковостей зовнішнього середовища і нашої життєдіяльності в цьому середовищі. З даного визначення випливає, що самі по собі відомості ще не є інформацією до моменту ознайомлення, взаємодії та контакту з суб'єктом або адресатом.

У наступні десятиліття наука кібернетика уточнила поняття «інформації», в загальному визначивши її як відомості, отримані з зовнішнього світу, сприйняті та збережені в пам'яті, які можуть бути перероблені за допомогою інтелектуальної діяльності або з використанням спеціальних технічних пристроїв, передані різними комунікаційними каналами з метою інформування, стимулювання діяльності, формування поведінки.

Кібернетичний підхід до інформації вимагав того, щоб вона була осмислена на філософському рівні, оскільки саме філософія визначає методологічні основи будь-якої науки.

Видатний український вчений В. М. Глушков зазначає, як фізична субстанція інформація являє собою міру неоднорідності розподілу матерії та енергії в просторі та в часі, міру змін, якими супроводжуються всі процеси, що протікають в світі [8, с. 53].

У науковій літературі поняття «інформація» осмислювалось на рівні її комунікативної ознаки, як основна частина процесу комунікації.

Інформація є складним явищем, утворене, з одного боку, проявом властивості об'єктів живої природи (суб'єктів) відображати в формі психічних відчуттів рух об'єктів навколишнього світу (змістовна сторона інформації, відомості), а з іншого – проявом здатності деяких об'єктів живої природи передавати за допомогою повідомлень випробувані ними відчуття (образи) іншим об'єктам живої природи (представницька сторона інформації, повідомлення).

Наведені вище визначення відображають комунікативну сутність

інформації, проте в той же час вказують на її основу, тобто на об'єкт комунікації, яким є відомості, викладені у формі, що дає можливість їх передавати та сприймати.

Як вказують В. М. Варенко, І. В. Братусь, В. С. Дорошенко, Ю. Б. Смольніков, В. О. Юрченко, «відомості» складають змістовну сторону інформації, виконують ряд функцій, зокрема вони сприяють пізнанню навколишнього світу, забезпечують процес соціальної комунікації [9, с. 14].

В. Г. Іванов, С. М. Іванов, В. В. Карасюк під інформацією розуміються дані, що характеризують об'єкт пізнання і можуть бути виділені пізнає суб'єктом в тому чи іншому відображенні пізнаваного об'єкта. Термін «відомості» замінений на поняття «дані», які визначаються як змістовна сторона інформації, як властивість живого або комп'ютерного інтелекту описувати факти, образи, явища, процеси і забезпечувати передачу інформації.

З точки зору сучасних процесів інформатизації поняття «дані» більш точно відображає характер об'єктів інформаційних відносин, в структуру якого входять відомості, що є тими чи іншими фактами, що стосуються різних сфер людського буття [10, с.17].

Як вказують С. О. Телешун, І. В. Рейтерович, інформація являє собою відомості, що повідомляються однією особою іншій, про неї, на думку вченого, також можна говорити як про процес повідомлення цих відомостей. У широкому сенсі під інформацією автор розуміє будь-які відомості, які передаються на будь-яких засадах [11, с. 9]. Однак підкреслюючи, що сучасні реалії вимагають від нас здатності розрізняти завдання, які в недавньому минулому прийнято було вважати суміжними – інформацію та її використання. Виникає необхідність у відокремленні самої інформації і розгляді її у відриві від процесу передачі. Таке розуміння виходить за межі інформації як такої, і термін «інформація» при такому підході використовується умовно і навіть «помилково», маючи на увазі під собою нову групу складних інформаційних відносин. Таким чином, інформацію у відриві від процесу передачі справедливо було б назвати іншим, більш широким терміном.

Особливістю поняття «інформація» є його універсальність – воно використовується в усіх без винятку сферах людської діяльності, в той же час, визначення категорії «інформація», перш за все, залежить від конкретної галузі знань, в якій ведеться дослідження.

Виходячи з наведених вище визначень, ми можемо говорити про те, що з правової точки зору інформація – це дані, які є об'єктом комунікації, і посягання на інформацію слід розглядати в двох площинах: як посягання безпосередньо на інформацію і як посягання на можливості її безперешкодної передачі (комунікації).

Слід визнати, що в принципі будь-яка інформація створюється з метою її поширення та використання, тому розглядати інформацію у відриві від складного і різноманітного процесу її передачі та отримання, практично неможливо. Іншими словами сучасні уявлення про зміст поняття «інформація» також пов'язані зі здібностями оперувати відомостями, існує думка, що інформація є повідомлення, метою якого є передача відомостей і даних, щодо ідей, відкриттів про стан справ де-небудь, про стан чого-небудь .

Даний підхід має під собою цілком прагматичні підстави, оскільки інформація в статичному стані перестає володіти тим величезним масивом корисних якостей, якими вона наділена, будучи здатною до передачі. У такому випадку вона перетворюється в просто відомості або дані, чия цінність полягає лише в утриманні, яке вони несуть. Тому, видається, що під інформацією слід розуміти сукупність відомостей і даних, процес їх передачі та отримання, а також їх психічне сприйняття і оцінка.

З правової точки зору інформація є субстанцію, що має здатність трансформуватися в фактичні соціально-праві відносини з приводу володіння, розповсюдження, продажу та передачі відомостей, які підлягають правовому захисту і охорони. У даному випадку охороною слід вважати діяльність по створенню правових норм, спрямованих на захист інформації та інформаційних прав учасників процесів, пов'язаних з обігом інформації – держави, особи, підприємств, організацій, інститутів громадянського суспільства.

Захистом доцільно вважати процес застосування даних норм в практичну діяльність правозастосування.

Водночас, звертаючись до визначення терміна «інформаційна безпека», слід визнати, що в науковій літературі відсутня єдина думка щодо його змісту.

Українська наукова думка звернула увагу на проблеми інформаційної безпеки в 90-і роки XX століття у межах забезпечення національної безпеки держави, подолання технологічної та науково-технічної залежності України від зовнішніх джерел. Як зазначає О. Л. Гапеєва, у науковому доробку українських дослідників виокремлено праці, в яких розглянуто актуальні питання сьогодення в контексті забезпечення інформаційної безпеки, пов'язані із міграційними та євроінтеграційними аспектами [12, с. 40]. Останні два десятиліття характеризуються інтенсивним вивченням даної галузі. Науковим дослідженням притаманна многосторонність висвітлення питань інформаційної безпеки, в той же час відсутність єдиної наукової концепції інформаційної безпеки говорить про недостатній рівень соціально-філософської розробленості теми.

Загальна тематика досліджень використання інформаційних технологій, в науковій літературі представлена технологічним и гуманітарним напрямами рішення завдань інформаційної безпеки. На відміну від технологічного підходу, що розглядає програмно-технічну сторону процесу забезпечення інформаційної безпеки, гуманітарний розглядає інформаційну безпеку в якості міждисциплінарної галузі наукового знання, виділяючи юридичні, соціологічні и психологічні аспекти указаного феномена.

Дослідження проблем інформаційної безпеки гуманітарного характеру базуються на вивченні загальнометодологічних основ процесу інформаційної безпеки, закономірностей розвитку інформаційної сфери як системо утворюючого фактора життя суспільства, шліхів и способів використання інформаційної сфери для реалізації основних соціально-політичних завдань України – вступ до НАТО і Європейського Союзу.

Вивчення інформаційної безпеки як філософсько-методологічної

проблеми, підкреслює її аксіологічний аспект. Концептуальна модель єдності інформаційної безпеки на глобальному рівні представляє не суму складових інформаційної безпеки, а інформаційно-когнітивну форму, об'єднуючу можливості кожної з них. Головним елементом парадигми інформаційної безпеки виступає інформаційний гуманізм, гарантуючий захищеність об'єктів соціальної природи.

Як вказує В. С. Цимбалюк, А. В. Бабінська, під інформаційною безпекою України слід розуміти стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особи, суспільства та держави [13].

Схоже визначення поняттю «інформаційна безпека» пропонує О. А. Ніщименко, який вважає, що цей стан захищеності національних інтересів України в інформаційній сфері, що складаються з сукупності збалансованих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз, що відповідає принципу забезпечення національної безпеки в інформаційній сфері [5, с.19].

На думку Л. О. Кочубей, інформаційна безпека – це такий стан захищеності життєво важливих інтересів, а, отже, й інформаційної озброєності держави, суспільства, особистості, за якого жодні інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів [14, с. 221-222].

Інформаційна безпека є стан захищеності особи, суспільства, держави від інформації, що носить шкідливий або протиправний характер, від інформації, що надає негативний вплив на свідомість особи, що перешкоджає сталому розвитку особи, суспільства та держави. Інформаційна безпека забезпечує сталий розвиток особи, суспільства та держави стан захищеності інформаційної інфраструктури, включаючи комп'ютери і інформаційно-телекомунікаційну інфраструктуру, інформацію, що в них знаходиться.

Однак при цьому Г. М. Савчук вважає, що особливістю реалій України є

не сформованість і недостатня визначеність системи цінностей та інтересів суспільства, наявність низки протиріч між інтересами різних соціальних спільнот і професійних груп, що спричинює політичну та соціальну нестабільність. Внаслідок несформованості консенсусу в суспільстві щодо національних цілей, інтересів і цінностей, не забезпечується належна конструктивність у забезпеченні національної та інформаційної безпеки країни як «стану захищеності життєво важливих інтересів особистості, суспільства та держави від зовнішніх і внутрішніх загроз» [15]. Водночас, на нашу думку, звернення до поняття «стан захищеності», вважає цілком виправданим, якщо його немає, то немає і безпеки. У цьому сенсі мова йде про розуміння безпеки в правовому, охоронному аспекті.

У свою чергу С. С. Єсімов вказує, що суть інституту інформаційної безпеки в системі інформаційного права полягає в здійсненні правових, організаційних, технічних заходів, що забезпечують безпеку всіх складових інформаційно-комунікаційного комплексу держави, системи інформаційних ресурсів, інформаційно-комунікаційної інфраструктури, науково-технічного та виробничого комплексу інформаційної індустрії, ринку інформаційної продукції та послуг, системи масової інформаційної освіти, просвіти та підготовки професійних кадрів для інформаційної сфери. окремих організацій та кожної людини [16, с. 75].

Дані проблеми спостерігаються і в інших визначеннях. На нашу думку, розглядаючи інформаційну безпеку як об'єкт адміністративно-правової охорони, слід вказати на те, що вона є не тільки станом захищеності, а й системою суспільних відносин, які сприяють виникненню стану захищеності або безпеки.

Водночас, під інформаційною безпекою доцільно розуміти сукупність суспільних відносин, що складаються в процесі захисту конституційних прав і свобод від внутрішніх і зовнішніх загроз в інформаційній сфері.

При цьому слід вказати на те, що важливою ознакою інформаційної безпеки, як вважає Н. С. Мороз, є її динамічність, оскільки вона, в широкому

сенсі, являє собою забезпечення стабільності та розвитку інформаційної сфери, яка постійно змінюється через різноманіття потреб учасників інформаційних відносин [17, с. 136].

У зв'язку з останнім зауважимо, що більшість з наведених визначень хоча фіксують важливі, конститутивні ознаки інформаційної безпеки, однак розглядають її як стабільний, незмінне явище: «стан захищеності», «здатність захищати», «захищеність» тощо.

Для конкретизації поняття «інформаційна безпека», доцільно погодитися з думкою О. Г. Яреми та С. С. Єсімова, що принциповим є визначення інформаційної безпеки як самостійного правового утворення, оскільки має власну складну структуру, що охоплює інститут віднесення інформації до категорії з обмеженим доступом, інститут захисту інформації та ліцензування цієї діяльності, а також інститут відповідальності за правопорушення в інформаційній сфері. Структурна складність пояснюється предметною безліччю правовідносин, що виникають під час забезпечення захищеності інтересів особистості, суспільства та держави в інформаційній сфері [18, с. 247-248].

Дане визначення дає підстави для попереднього розгляду інформаційної безпеки саме як певної системи суспільних відносин, що виникають з приводу створення умов безпечної життєдіяльності держави, суспільства і особи в інформаційному середовищі. Фактично на суспільний характер інформаційної безпеки вказує Доктрина інформаційної безпеки України, яка, зазначає, що застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Інформаційна сфера, будучи системоутворюючим фактором життя суспільства, активно впливає на стан політичної, економічної, оборонної і інших складових безпеки України [19].

У контексті вирішення завдань правового регулювання системоутворюючий фактор життя об'єктивно вимагає захисту, яка здійснюється як інформаційного та адміністративного права, так і за

допомогою різних інших конструктивних галузей права: конституційного, цивільного, банківського, комерційного та інших.

Відповідно, адміністративно-правова охорона в інформаційному середовищі забезпечується за допомогою норм, які спрямовані на захист різних суб'єктів інформаційної безпеки, держави, суспільства, особи, хоча з погляду на дослідження І. О. Валюшко «Інформаційна безпека України в контексті російсько-українського конфлікту» та О. Г. Семенюка «Баланс життєво важливих інтересів особистості, суспільства та держави в інформаційній сфері» можна стверджують, що принцип балансу інтересів особи, суспільства та держави в інформаційній сфері законодавчо не визначений [20; 21, с. 67-68].

Якщо в чинному законодавстві справді не відображено баланс інтересів учасників інформаційних відносин, то в науковій літературі такий баланс в принципі визначено. На думку О. Д. Довганя, інтереси суспільства в інформаційній сфері полягають у забезпеченні інтересів особи в цій сфері, зміцненні демократії, створенні правової соціальної держави, досягненні та підтримці суспільної злагоди, в духовному оновленні України [22, с. 21].

Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розвитку національної інформаційної інфраструктури, для реалізації конституційних прав і свобод людини та громадянина в галузі отримання інформації та користування нею з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності України, політичної, економічної та соціальної стабільності, в безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

Інформаційна безпека це сталий стан інформаційного середовища, який забезпечує свою цілісність і захист об’єктів при наявності несприятливих внутрішніх та зовнішніх впливів на основі визначення соціальними суб’єктами своїх цінностей, потреб (життєво важливих інтересів) і цілей розвитку.

Інформаційна безпека в якості ключової складової національної безпеки охоплює напрями: забезпечення захисту інформаційного простору, що

підтримує справедливий розподіл благ і ресурсів; сприяння процесу переходу до стійкого розвитку світового інформаційного середовища, що формується; стан захищеності культурного генофонду людства в умовах глобалізації.

Що стосується інтересів особи в інформаційній сфері, то вони полягають в забезпеченні вільного доступу до відкритої інформації, в тому, щоб дана інформація була правдивою, не мала на меті негативний інформаційний вплив на особистість, не носила антигуманний, аморальний, екстремістський характер, щоб особиста, конфіденційна інформація громадян була належним чином захищена з використанням норм права, щоб система юридичних норм надійним чином гарантувала права громадян в інформаційній сфері.

Наведені вище підходи є підставою для того, щоб визначити інформаційну безпеку (в юридичному сенсі) як сукупність суспільних відносин, які регулюються системою правових норм, спрямованих на забезпечення національних інтересів держави та суспільства, на забезпечення законних інтересів особи та суб'єктів господарювання в інформаційній сфері, гарантують права людини та громадянина в інформаційній сфері, захист інформації від несанкціонованого доступу, знищення, блокування, модифікації, копіювання та неправомірного використання.

Дані відносини включають відносини з приводу: забезпечення доступу до інформаційних ресурсів; створення, використання та поширення інформації, обмеження доступу до інформації; безпечної життєдіяльності в інформаційному середовищі.

У межах першої групи забезпечується функціонування ефективних засобів інформаційної діяльності, у межах другої – забезпечується можливість суб'єктів отримувати доступ до необхідних інформаційних ресурсів, формується інформаційний ресурс, який відповідає потребам суб'єктів, третя група забезпечує функціонування інформації, що має режим таємницею, конфіденційною, четверта група відносин визначає стан громадської (публічної) безпеки, пов'язаної з використанням комп'ютерів і інформаційних технологій.

У свою чергу, як вказує А. М. Воронов, родовим об'єктом інформаційно-правового захисту в інформаційній сфері України є інформаційні права, свободи та законні інтереси громадян, суспільства та держави, а предметно-галузевим – правовідносини, що виникають у процесі реалізації прав громадянина, суспільства та держави на отримання, зберігання, поширення, користування інформацією та її захисту.

Прикладом тісної взаємодії інформаційної та громадської безпеки може служити приховування інформації, поширення неправдивої інформації, що веде до порушення громадського порядку, до порушення функціонування технічних, технологічних і екологічних систем, порушення функціонування органів державної влади та місцевого самоврядування, до проблем з безпекою особи в техногенному середовищі.

Якщо ж звернутися до Доктрину інформаційної безпеки України, в якій під інформаційною безпекою України розуміється стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особи, суспільства та держави, то можна зробити висновок, що основним вектором політики держави щодо забезпечення інформаційної безпеки є дотримання конституційних прав і свобод людини в інформаційній сфері.

Це означає, що аналіз нормативно-правового регулювання інформаційної безпеки та вдосконалення законодавчої бази необхідно починати з Конституції, яка має найвищу юридичну силу та містить значну кількість норм, що складають основу нормативно-правового регулювання інформаційної безпеки.

Проведений логіко-семантичний, догматико-юридичний та структурно-функціональний аналіз норм Конституції України, дозволяє виділити права та свободи людини, які так чи інакше пов'язані з інформацією:

1. Конституція України проголошує: «Кожен має право вільно збирати, зберігати, використовувати та поширювати інформацію будь-яким законним способом. (ч. 1 ст. 34) [23].

2. Кожен має право на недоторканність приватного життя, особисту та

сімейну таємницю (ч. 1 ст. 32 Конституції України), при цьому слід зазначити, що питання захисту прав і свобод людини та громадянина при обробці його персональних даних, в тому числі захист конституційних прав на недоторканність приватного життя, особисту та сімейну таємницю регулюються Законом України «Про захист персональних даних» [24];

3. Кожен має право на безпечне для життя та здоров'я довкілля та на відшкодування завданої порушенням цього права шкоди. Кожному гарантується право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення. Така інформація ніким не може бути засекречена (ст. 50 Конституції України).

4. Ст. 40 Конституції України встановлює, 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.

Дану конституційну норму можна вважати гарантією та передумовою громадського контролю за органами державної влади, місцевого самоврядування та громадськими недержавними структурами, що передбачає рівний доступ до державних інформаційних ресурсів, за винятком інформації, що відноситься до державної таємниці.

Відповідно до Законів України «Про доступ до публічної інформації», «Про внесення змін до деяких законів України щодо доступу до публічної інформації у формі відкритих даних» до основних принципів забезпечення доступу до інформації про діяльність державних органів і органів місцевого самоврядування належать: відкритість і доступність інформації про діяльність державних органів та органів місцевого самоврядування; достовірність інформації про діяльність державних органів і органів місцевого самоврядування та своєчасність її надання; свобода пошуку, отримання, передачі та поширення інформації про діяльність державних органів і органів місцевого самоврядування будь-яким законним способом; дотримання прав

громадян на недоторканність приватного життя, особисту і сімейну таємницю, захист їх честі і ділової репутації, права організацій на захист їх ділової репутації при наданні інформації про діяльність державних органів і органів місцевого самоврядування [25; 26].

5. Ст. 15 Конституції України забороняє цензуру та на законодавчому рівні визнає свободу масової інформації, що прямим чином пов'язано з правом на доступ до інформації, тому що її основна маса передається за допомогою засобів масової інформації, до яких, відповідно до закону «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення і радіомовлення», «Про Суспільне телебачення і радіомовлення України», відносяться періодичні видання, радіо, телевізійні, відео програми і інші форми періодичного поширення інформації [27; 28; 29].

Взаємодія та підтримку зворотного зв'язку громадян з державними органами слід вважати невід'ємною ланкою права на доступ до інформації. Інформаційні права та свободи громадян знаходяться в органічному зв'язку з обов'язками держави в інформаційній сфері. Обмеження права на доступ до інформації відповідно до ч. 2. ст. 34 Конституції України, може мати місце тільки в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Водночас Конституція України встановлює ряд принципових положень, що стосуються гарантій інформаційної безпеки:

1. Права і свободи людини і громадянина захищаються судом (ст. 55).

2. Кожен має право на повагу до його гідності (ч. 1 ст. 21).

3. Кожен має право на таємницю листування, телефонних переговорів, поштових, телеграфних та інших повідомлень. Обмеження цього права допускається лише на підставі судового рішення (ст. 31 Конституції України).

4. Не допускається збирання, зберігання, використання та поширення

конфіденційної інформації про особу без її згоди, крім випадків, визначених законом. (ч. 1 ст. 32 Конституції України).

5. Органи державної влади та органи місцевого самоврядування, установи і організації їх посадові особи зобов'язані забезпечити кожному можливість ознайомлення з документами і матеріалами, що безпосередньо зачіпають його права і свободи, відомостями про себе, якщо інше не передбачено законом (ч. 2 ст. 32 Конституції України).

6. Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації (ч. 3 ст. 32 Конституції України).

7. Інтелектуальна власність охороняється законом (ст. 54 Конституції).

8. В умовах воєнного та надзвичайного стану для забезпечення безпеки громадян і захисту конституційного ладу відповідно до конституційним законом можуть встановлюватися окремі обмеження прав і свобод із зазначенням терміну їх дії (ст. 64 Конституції України).

Таким чином, конституційне право на свободу отримання інформації є не тільки основою інформаційних відносин, а й гарантом прозорості, транспарентності та законності діяльності державної влади.

Розглянуті вище положення Конституції знайшли відображення в адміністративному праві, наприклад, стаття 212-3 «Порушення права на інформацію та права на звернення» Кодексу України про адміністративні правопорушення, встановлює відповідальність посадових осіб за відмову в наданні громадянину інформації, а також за надання громадянину неповної або завідомо неправдивої інформації [30].

Дане визначення співвідноситься з положеннями Конституції України, де в ст. 3 зазначено, що людина, її права і свободи є найвищою цінністю. Визнання, дотримання і захист прав і свобод людини та громадянина є обов'язок держави.

Можна сказати, що інформаційна безпека є складною конституційно-правову конструкцію, що визначається: складною соціальною та правовою природою, заснованою на різноманітті інформаційних відносин в суспільстві; диференціацією суб'єктів інформаційних відносин, що мають свої інтереси, права і обов'язки в цій сфері; об'єктивним характером інформаційних відносин, які визначають розвиток світової цивілізації та системи міжнародного права. Для забезпечення інформаційної безпеки використовується, весь історично накопичений досвід, як адаптивна відповідь на вплив різноманітних умов середовища, який відповідає новітнім тенденціям розвитку інформаційних і телекомунікаційних технологій. Всі системні механізми формування та використання інформаційного потенціалу, їх типологія, провідні чинники управління, адаптивні можливості інформаційних систем залежать від умов конкурентного середовища, яка є для нормативно-правого регулювання головним фактором динамізму, що визначає динаміку розвитку техніко-технологічних і правових засад інформаційної безпеки.

Важливим завданням забезпечення інформаційної безпеки є забезпечення збалансованості інтересів особи, суспільства і держави та їхньої ефективної співпраці в межах глобального інформаційного простору. Цей баланс повинен бути узгоджений з державною політикою у сфері безпеки загалом [31, с. 331].

Розглянув поняття інформаційної безпеки як системи суспільних відносин і об'єкта правової охорони доцільно зробити висновки.

В умовах реалізації Стратегії сталого розвитку «Україна – 2020», Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, Закону України «Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях» інформаційна безпека набуває пріоритетного значення в політичній, соціально-економічній, воєнно-технічній, юридичній і інших сферах життя суспільства та виступає системо утворюючим елементом системи національної безпеки в цілому [1; 32; 33].

У науці застосовуються два основні підходи до дослідження інформаційної безпеки – технологічний і гуманітарний. Їх відмінність полягає у використанні різних критеріїв безпеки. Технологічний підхід в якості основних критеріїв виділяє забезпечення конфіденційності, цілісності та доступності інформації. Гуманітарний підхід концентрується на захисті від інформаційних загроз, здатних привести до руйнування традиційних духовно-моральних цінностей суспільства, розмиттю ідентичності особи, дестабілізації політичної системи та втрати державного суверенітету, включаючи дослідження у галузі юриспруденції, соціології, психології інших наук. Комплексне дослідження інформаційної безпеки передбачає поєднання обох підходів.

У контексті інформаційної безпеки система суспільних відносин що впливає на об'єкт правової охорони розглядається як єдина цілісна сукупність різних категорій, в якій вони знаходяться в стані структурно-функціональних зв'язків між собою з метою забезпечення оптимальної діяльності у межах правових відносин, які за своєю природою є соціально-правовими цілями, що визначають особливості організації, законодавчого закріплення та реалізації системи юридичних засобів адміністративно-правового регулювання. Встановлення системи забезпечується відповідною системною правовою регламентацією в законодавстві, яка входить складовою частиною в систему юридичних засобів адміністративно-правового регулювання інформаційної сфери держави.

Розвиток інформаційних і комунікаційних технологій сприяє змінам у суспільних відношеннях, які у свою чергу здійснюють вплив на інститут прав людини. У цих умовах проходить формування нової групи прав людини – інформаційних, які обумовлені використанням інформації та інформаційних ресурсів. Більша частина інформаційних прав відноситься к основним правам, здійснення яких можливо з використанням інформаційних і комунікаційних технологій. Формулювання таких прав людини на міжнародному та конституційному рівнях є в достатній мірі загальними та не залежать від розвитку технологій. Для признання можливості їх здійснення з використанням

інформаційних і комунікаційних технологій внесення змін у такі формулювання, як правило, не треба. До числа інформаційних прав включаються не тільки права, які має в on-lane середовищі, але й нові права, характерні виключно для інформаційного середовища. Нові інформаційні права людини, зв’язані з інформацією про приватне життя, є компонентами уже признаних основних прав, таких як свобода виразу думки та право на недоторканість приватного життя. Водночас, інформаційні права отримають юридичне закріплення в якості основних прав. Розвиток інформаційних прав на сучасному етапі обумовлено різними національними моделями и юридичного закріплення, що відповідає відповідним правовим традиціям держав і рівню їх соціально-економічному розвитку. Це відрізняє правові засади забезпечення інформаційної безпеки в країнах Європейського Союзу, сталих демократій (США, Японія, Канада інші) та країнах з тоталітарними методами управління (Російська Федерація, країни СНД).

У практиці забезпечення інформаційної безпеки існують організаційні та правові форми втілення в життя приписів адміністративно-правових норм, об'єктивізації на практиці їх юридичного змісту. Вони визначають послідовність дій і операцій, що здійснюються всіма суб'єктами адміністративного права в встановлених законом процесуальних формах спрямованих на досягнення цілей адміністративно-правового регулювання інформаційних суспільних відносин, що дає можливість поєднати в змісті інформаційної безпеки два концептуальних уявлення про організаційно-правові форми управлінської діяльності у зазначеній сфері та процедурно-процесуальні форми реалізації права.

1.2 Вихідні методологічні засади дослідження інформаційної безпеки

Пошук сучасних підходів до інформаційної безпеки, перегляд і аналіз вже відомих, а також розробка нових моделей забезпечення інформаційної безпеки складають найважливіший етап у формуванні сучасної теорії безпеки держави.

Процес переосмислення центральних юридичних понять, у тому числі інформаційної безпеки, зумовлює формулювання та розробку основних теоретичних конструкцій і моделей правового регулювання інформаційної безпеки України.

Плюралізм підходів до інформаційної безпеки, різноманітність моделей її розуміння цілком адекватні сучасному розвитку гуманітарних наук і не є ознакою кризи або особливістю юриспруденції. Таке ж різноманіття позицій спостерігається і в питаннях про сенс і поняття суспільства, політики, влади в політології, соціології, культурології. У рамках юридичної науки до тепер не досягнуто хоча б приблизної подібності поглядів серед вчених з приводу визначення інформаційної безпеки. Це веде до відсутності продуманої та зваженої правової політики. Різницю дослідних інтерпретацій, що стосуються природи інформаційної безпеки, врівноважує єдність думок представників державної влади, які дотримуються європейського стандарту в оцінці соціальних явищ, у тому числі інформаційної безпеки.

Тому теоретико-методологічний аналіз процесу розуміння інформаційної безпеки неминуче зачіпає питання його методології, розробка якої традиційно вважається пріоритетною для теорії права.

Існує два основних теоретичних підходи до природи розуміння інформаційної безпеки. Одні автори (Д. А. Ловцов інші) дають визначення розумінню інформаційної безпеки, розглядаючи її як особливий спосіб соціальної діяльності, спрямований на пізнання загальних закономірностей функціонування суспільства, представлення отриманих відомостей у формі наукового знання, впровадження наявних теорій і концепцій у практичну діяльність, яка здійснюється в специфічній формі із застосуванням спеціального (науково-правового) інструментарію пізнання (методу) [34, с. 95]. Другий підхід (В. В. Антонюк) дозволяє розглядати інформаційну безпеку як явище суспільного життя, а не тільки як науковий пошук істини [35, с. 23]. Широкий підхід до поняття інформаційної безпеки включає в себе два зазначених погляди: інформаційна безпека трактується як система знань і

уявлень про розвиток правових явищ. У межах широкого підходу можна виділити науково-теоретичне, професійно-практичне та буденно-повсякденне розуміння інформаційної безпеки.

У контексті дослідження А.Ю. Нашинець-Наумової «Інформаційна безпека: питання правового регулювання», від розуміння інформаційної безпеки, як юридичної концепції соціальної реальності, залежить методологія, тому що вчення про сутність – це вчення про метод його вивчення [36, с. 9-11].

Проблеми забезпечення інформаційної безпеки України органічно пов'язані з політичними, економічними, соціальними, державно-правовими реформами, які проводяться в країні, з проблемами формування громадянського суспільства, демократії, що вимагає системного їх осмислення в контексті Стратегії національної безпеки України та закону України «Про основні засади забезпечення кібербезпеки України» (набрав чинності 9 травня 2018 року) [4; 37].

У зв'язку з цим виникають завдання щодо подальшого розвитку норм законодавства, діючих у сфері забезпечення інформаційної безпеки, з урахуванням критичного перегляду національного та зарубіжного досвіду, але головне – наукового обґрунтування напрямів забезпечення інформаційної безпеки України як сукупності адміністративно-правових засобів, що відображають систему стратегічних і тактичних заходів протидії загрозам інформаційній безпеці.

Ці принципово важливі міркування дозволяють додати проблемі забезпечення інформаційної безпеки України загальнонауковий характер. Його розробка передбачає координацію зусиль вчених і фахівців різних галузей знань з метою отримання науково-обґрунтованих і практично значущих результатів як основи конструювання адміністративно-правових засад діяльності органів державної влади, місцевого самоврядування, громадських організацій (об'єднань) щодо забезпечення інформаційної безпеки.

На формування теоретичних підстав методологічних засад дослідження поняття та змісту інформаційної безпеки зробили істотний вплив

фундаментальні наукові праці з загальної теорії права, філософії права, соціології, історії, конституційного права, кримінології, роботи відомих учених-адміністративістів, у тому числі фахівців в галузі державного управління: В. Б. Авер'янов, І. В. Арістова, Є. О. Архипова, О. А. Баранов, В. Л. Бурячок, Д. О. Біленська, В. І. Гурковський, Є. В. Жуков, Л. П. Коваленко, В. А. Ліпкан, І. В. Мукомела, О. В. Рибальський, І. М. Сопілко, О. М. Селезньова, В. В. Ткаченко, О. О. Тихомиров і інших [38-54]. У відповідь на соціально-економічні, культурологічні і інтелектуальні виклики сучасності теорія безпеки та інформаційної безпеки, як її відгалуження, потребують сьогодні об'єктивної ревізії та якісного наукового оновлення.

Основою понятійного комплексу «інформаційна безпека» є загальнотеоретичне вчення про безпеку, як фундаментальну проблему юридичної науки, що носить виражений міждисциплінарний характер і що дає вихід на концепти спеціального правозастосування.

Теорія безпеки являє собою досить розроблену доктрину [55, с. 12]. Водночас, окремі питання досліджуються в зв'язку з галузевою спеціалізацією та проблематикою й вивчені порівняно меншою мірою. Винятком є, мабуть, концепція національної безпеки, що характеризується високим ступенем інструменталізації свого теоретико-методологічного апарату, що підтверджується дослідженнями В. А. Ліпкана, В. Ортинського та інших [47; 48; 56 с. 7].

Необхідно констатувати, що інформаційна безпека, як розділ теорії безпеки, в даний час у вітчизняній юридичній науці слабо висвітлена. Методологічно домінуюче питання про парадигму інформаційної безпеки, яка структурує науково-теоретичну та практичну інформацію про досліджуваний об'єкт, залишається дискусійним, так як питання ґенези та розвитку структури елементів інформаційної безпеки, їх систематичної класифікації та типології, оптимальної системної організації і ефективного функціонування в умовах практики правозастосування, гармонізації структурно-елементних зв'язків, прогнозу змін структури та її елементів сьогоднішня юриспруденція не знає.

Необхідно знайти науково зважене вирішення питання про парадигму інформаційної безпеки як методологічно пріоритетної проблеми загальної теорії безпеки.

На думку О. П. Дзьобаня, О. Ю. Панфілова, Р. А. Чемчекаленка предметом системного дослідження інформаційної безпеки виступає виявлення типів зв’язків і, передусім, системотворчих зв’язків цілісності, виокремлення об’єктивної структури даного системного утворення та її характеру [57, с. 178].

Це особливо важливо в період реалізації Законів України «Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях». «Про основні засади забезпечення кібербезпеки України» та Доктрини інформаційної безпеки України для досліджень, де загальнонаукові засоби пізнання виконують евристичні функції, за допомогою яких будується система нових наукових знань про ту чи іншу сферу безпеки; забезпечення її комунікаційних зв'язків з іншими видами безпеки; трансформація понятійного апарату однієї сфери безпеки в іншу, що розширює можливості інтерпретації результатів досліджень [4; 19; 33].

Структура сучасного знання про безпеку характеризується не стільки сукупністю окремих фактів, теорій і методів їх вивчення, скільки комплексним підходом до дослідження «стикових», що припускають використання наукового інструментарію різних сфер безпеки в ході дослідження комплексних проблем, пов'язаних, наприклад, із засобами забезпечення інформаційної безпеки на регіональному, або в цілому, на державному рівні, що зумовлено внутрішнім взаємозв'язком, тобто взаємопроникненням і взаємовпливом різних методів пізнання та загальної методологічної домінанти. Реалізація вищеназваного розширює можливості використання системного, структурно-функціонального, інформаційного, логічного, модельного, ймовірнісного і інших загальнонаукових методів у формуванні відповідного понятійного апарату.

Використовуючи підходи М. Кельмана щодо методології, у цьому зв'язку виникають питання, з одного боку, про використання загальних знань про

безпеку при дослідженні соціальних проблем, вивчення яких в логіко-гносеологічних аспектах може призвести до отримання як нового, так і до поглиблення раніше отриманого знання, а, з іншого – при виробленні та прийнятті управлінських рішень з проблем забезпечення безпеки [58, с. 42-43]. Водночас доцільно погодитися з А. Качинським, що всебічне вивчення закономірностей виникнення суспільно небезпечних факторів і їхнього впливу на природу, суспільство і людину в структурі загальнонаукового знання переоцінити важко, оскільки результатів залежить соціальна оцінка і активна державна політика в галузі забезпечення інформаційної безпеки [59, с. 13-14].

Стає ясним, що до числа подібних проблем соціальної практики з повною підставою слід віднести проблему інформаційної безпеки, теоретичне та прикладне рішення якої передбачає, передусім, досить широке, загальнонаукове осмислення в формально-логічній системі суджень:

- по-перше, теоретико-прикладне рішення проблеми забезпечення інформаційної безпеки має чітку спрямованість на вироблення та реалізацію наукових методів управління соціальною практикою у сфері організації забезпечення інформаційної безпеки;

- по-друге, науковий інструментарій дослідження проблеми забезпечення інформаційної безпеки передбачає обов'язковий перехід від суто теоретичних конструкцій до аналізу емпіричного матеріалу, а далі на рівень загальнонаукового осмислення, що фіксує загальне наукове знання «безпека» в органічній єдності зі специфічним знанням «інформаційна безпека»;

- по-третє, у сфері теоретико-методологічного забезпечення інформаційної безпеки відбувається синтез природничих, технічних і гуманітарних знань, які включають в себе загальні положення всіх елементів соціальних систем з метою їх збереження, нормального функціонування та розвитку.

Як зазначає І. П. Арістова розглядаючи методологію науки «інформаційне право», перша гносеологічна засада: вчений, який займається дослідженнями у сфері інформаційного права, має враховувати, зокрема,

існування однієї із закономірностей розвитку науки в цілому – взаємодію та взаємопов'язаність усіх галузей науки. Звертаємо увагу на важливість взаємодії усіх галузей юридичної науки, оскільки це дозволяє досліджувати предмет однієї із галузей юридичної науки (наприклад, науки «інформаційне право») за допомогою прийомів і методів інших юридичних наук [60].

У даному випадку важливо взяти до уваги вимогу міждисциплінарного методу пізнання, що дозволяє отримати та використовувати результати прикладного значення з метою вдосконалення практичної діяльності. Звідси випливає, що гносеологічне трактування поняття «інформаційна безпека», розкриваючи притаманні ознаки та характеристики, може розглядатися лише в певному, предметному ракурсі (щодо особи, суспільства, держави).

З огляду на дослідження О. Д. Довганя, Т. Ю. Ткачука, правове забезпечення інформаційної безпеки можна визначити як цілісну систему правового регулювання суспільних відносин, має власний предмет правового регулювання [61, с. 79]. Концептуальне конструювання сучасної системи забезпечення інформаційної безпеки містить певну складність в силу своєї багатоаспектності та передбачає розробку як теоретико-методологічних питань, так і адміністративно-правового механізму, основних напрямів, форм і методів реалізації відповідних нововведень. Тут важливо дотримати поєднання теоретичних і прикладних аспектів вивчення проблеми адміністративно-правового забезпечення інформаційної безпеки так, щоб на основі встановлення її ролі, функціонального значення та місця в загальній структурі проблем забезпечення національної безпеки виробити і уточнити відповідні понятійні категорії, обґрунтувати пропозиції щодо вдосконалення законодавства та практику його застосування.

На наш погляд, необхідно враховувати і той фактор, що з моменту прийняття основоположних нормативних актів у сфері забезпечення безпеки: Стратегії національної безпеки України (2015 рік), Стратегію кібербезпеки України (2016 рік) і Доктрини інформаційної безпеки України (2016 рік) минув певний проміжок часу [62]. Для оцінки загроз інформаційній безпеці у світовій

практиці використовують спеціальну систему моніторингу, яка може ефективно працювати, застосовуючи відповідні відправні показники системи індикаторів, які необхідно закріпити у законодавчому порядку або на рівні постанови Кабінету Міністрів України, що передбачено Указом Президента України від 26.05.2015 № 287/2015 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», так як індикатори за зазначеним напрямом не включено до Вагових коефіцієнтів складників інтегрального індексу національної безпеки, як це пропонує представник Національний інститут стратегічних досліджень С. Л. Гнатюк [63; 64, с. 12]. У зв'язку з цим потребують конкретизації: загрози інформаційній безпеці, система суб'єктів, які в комплексі забезпечують інформаційну безпеку.

При розгляді проблеми організації забезпечення інформаційної безпеки набуває значення її структурна класифікація, яка відносно умовна і будується відповідно до певних цілей і завдань. У зазначеному аспекті доцільно розділити інформаційну безпеку залежно від джерел загрози на два типи – безпеку технічного характеру, що зумовлено технологією інформаційних і комунікаційних процесів, та безпеку, яку зумовлюють соціальні чинники.

Сьогодні, в умовах, як зазначає Т. Ю. Ткачук, стратегічне інформаційне протистояння становить небезпечний компонент гібридної війни, розгорнутої Росією проти України, межа між двома складовими вельми розмита. Причому головною загрозою інформаційній безпеці нашої держави сьогодні залишається загроза впливу ворога на інформаційну інфраструктуру, інформаційні ресурси, на суспільство, свідомість і підсвідомість особистості з метою нав’язати власну систему цінностей у життєво важливих сферах суспільної й державної діяльності [65, с. 185]. Однак, такий розподіл видається дуже доцільним і корисним з практичної точки зору, оскільки дозволяє чітко класифікувати ті чи інші концептуальні підходи до вирішення проблем забезпечення інформаційної безпеки в цілому. Крім того, такий розподіл необхідній для усвідомлення того, що при забезпеченні інформаційної безпеки технічного характеру потрібні

зовсім інші методи, форми та способи, ніж при забезпеченні інформаційної безпеки, яку зумовлюють соціальні чинники.

На даний час загрози інформаційній безпеці носять соціальний характер і зосереджені у внутрішньополітичній, економічній, соціальній, екологічній, інформаційній та духовній сферах життєдіяльності нашого суспільства. Як зазначалося вище, інформаційна безпека є складовою, органічною частиною національної безпеки. Звідси випливає, що збіг окремих видів загроз для них цілком виправданий. Це стосується тероризму, корупції тощо. Дані фактори несуть загрозу національній безпеці, в той же час вони становлять небезпеку для інформаційної безпеки в цілому.

Необхідно відзначити, що в юридичній літературі висловлюються різні трактування такого ключового поняття, як забезпечення інформаційної безпеки. Ми виходимо з того, що забезпечення інформаційної безпеки являє собою складний соціально-правовий механізм, під яким слід розуміти формування та проведення державної політики щодо створення та підтримки необхідного рівня захищеності об'єктів безпеки за допомогою здійснення заходів нормативно-правового, організаційного, управлінського і іншого характеру, заходів, адекватних загрозам життєво важливим інтересам особи, суспільства та держави у інформаційній сфері.

Основна мета цієї політики полягає у створенні, на базі відповідних концептуальних положень, й підтримці належного рівня функціонування організаційно-правового механізму забезпечення інформаційної безпеки, яка не обмежується лише правоохоронної сферою державного управління, а охоплює досить широку сукупність адміністративних, економічних, правових, організаційних і інших заходів з попередження та припинення загроз інформаційної безпеки та ліквідації наслідків їх проявів.

Тут необхідно зазначити, що забезпечення інформаційної безпеки – це діяльність не тільки держави, а й усього суспільства та кожного громадянина зокрема, спрямована на захист життєво важливих інтересів особи, суспільства та держави, і їх практичну реалізацію.

Політика забезпечення інформаційної безпеки – це діяльність політичного керівництва країни з визначення цілей і постановки принципових завдань по захисту життєво важливих інтересів особи, суспільства та держави у інформаційній сфері та вироблення форм, методів і способів досягнення цих цілей. Політика забезпечення інформаційної безпеки здійснюється на принципах дотримання та захисту прав і свобод людини та громадянина, законності, дотримання балансу інтересів особи, суспільства та держави, взаємної відповідальності особи, суспільства та держави за підтримання належного рівня функціонування механізму забезпечення інформаційної безпеки; системності та комплексності застосування органами державної влади, органами місцевого самоврядування політичних, організаційних, соціально-економічних, інформаційних, правових і інших заходів забезпечення інформаційної безпеки; пріоритет попереджувальних заходів з метою забезпечення безпеки; взаємодія органів державної влади з громадськими об'єднаннями, міжнародними організаціями та громадянами з метою забезпечення інформаційної безпеки.

Рішення теоретико-методологічних питань формування та реалізації державної правової політики, у межах якої розробляється правотворча стратегія у сфері інформаційної безпеки, що обумовлює характер процесу та результату застосування норм адміністративного права, має принципове значення для вироблення механізмів підвищення ефективності правомірного здійснення людиною, громадянином, об'єднанням громадян і державними органами свого власного статусу в юридично окреслених межах норм адміністративного права.

Адміністративно-правове забезпечення інформаційної безпеки прелставляє здійснювану у межах єдиної державної політики в галузі забезпечення інформаційної безпеки діяльність уповноважених суб'єктів, спрямовану на формування адміністративно-правової основи забезпечення інформаційної безпеки, на закріплення в ній системи адміністративно-правових засобів (адміністративно-правових норм, правовідносин, індивідуальних приписів та ін.), за допомогою яких досягається результативний, нормативно-

організаційний вплив на суспільні відносини з метою їх упорядкування, охорони, розвитку згідно суспільних потреб забезпечення інформаційної безпеки країни, створення та підтримки необхідного рівня захищеності об'єктів критично важливої інформаційної інфраструктури держави [66].

Порівняльний аналіз науково-теоретичних підходів до визначення понять «інформаційна безпека як стан», «забезпечення інформаційної безпеки як процес» (Т. Ю. Ткачук. Теоретичний дискурс пошуку основних складових системи інформаційної безпеки держави [67, с. 47]), практики їх нормативного закріплення в національному законодавстві, використання в міждержавних угодах країн Європейського Союзу, у контексті адаптації національного законодавства до вимог ЄС, показав, що використання даних термінів обумовлено потребами реалізації прогностичної функції права щодо суспільних відносин, рівень правового регулювання яких не володіє достатнім ступенем нормативності; створення правової основи діяльності суб'єктів у досить нових, мінливих сферах суспільних відносин; встановлення правового статусу суб'єктів, які реалізують свої повноваження у цій сфері; правового регулювання, що вимагає особливого поєднання правових засобів в процесі здійснення для досягнення максимального регулюючого впливу.

З урахуванням того, що Україна в даний час виступає частиною світового співтовариства, приймає на себе зобов'язання з дотримання нормативів європейського законодавства, проблема регулювання інформаційної безпеки, в аспекті самостійності регуляторної моделі адміністративного права, за визначенням німецького дослідника Е. Шмідт-Ассманна, набуває практичне значення [68, с. 24].

Основою для визначення поняття адміністративного права, у зазначеному аспекті, в Європі на сьогоднішній день є прецедент Європейського суду у справі Доймеланд (Deumeland) проти Федеративної Республіки Німеччини, розглянутий Європейським Судом 29 травня 1986 року. Зазначений прецедент Європейського Суду дозволяє визначити адміністративне право як частину системи права, що представляє особливу відокремлену групу правових норм,

зміст яких не може визначатися та змінюватися угодою учасників правовідносин, дотримання приписів що гарантується системою державного захисту постраждалої сторони [69, с. 56].

У згаданому контексті доцільно розглядати адміністративно-правове регулювання інформаційної безпеки. Аналіз тенденцій розвитку адміністративно-правового регулювання інформаційної безпеки дозволяє зробити висновок, що крім об'єктивних причин (розвиток суспільних відносин) на його динаміку істотний вплив робить юридична техніка. При цьому доцільно відрізняти розвиток нормативного регулювання інформаційної безпеки у власному розумінні (виникнення нових явищ у сфері публічно-правового регулювання) і техніко-юридичні феномени, що представляють собою, як зазначав Р. фон Иеринг, в ряді випадків результати невірної оцінки природи адміністративного права в процесі правотворчості [70, с. 203].

Розвиток правого регулювання інформаційної безпеки в Україні визначають у даний час дві основні тенденції. По-перше, спостерігається трансформація ролі держави, яка розширює свою участь у суспільних зв'язках як організатор залучаючи органи місцевого самоврядування та інститути громадянського суспільства [71]. По-друге, необхідно відзначити процес формування правосуб'єктності нових учасників публічно-правових зв'язків (квазі суб’єктів) у сфері інформаційної безпеки в контексті діяльності структур НАТО і країн-членів Європейського Союзу та Закону України «Про національну безпеку України» [72].

Особливий характер учасників суспільних відносин у сфері забезпечення інформаційної безпеки, сам факт наділення їх компетенцією необхідно враховувати в процесі правотворчої практики, вдосконалюючи техніко-юридичні прийоми визначення правосуб'єктності державних органів з погляду на досвід Німеччини [73].

Динаміка об'єктів нормативного регулювання інформаційної безпеки викликана технічними причинами, в силу яких відносини з приводу окремих явищ регулюються з використанням адміністративно-правових методів без

урахування специфіки соціальних зв'язків у відповідній сфері. Для сучасного нормативного регулювання інформаційної безпеки характерна тенденція децентралізації правотворчих центрів, формування системи відносно автономної правової регуляції суспільних відносин.

Співвідношення відомчої нормотворчості може бути описано тільки в категоріях взаємодії та взаємозв'язку, природа цих утворень в системі інформаційної безпеки не передбачає протиріч і взаємного проникнення у питання тактики застосування адміністративно-запобіжних засобів, засобів адміністративного припинення, адміністративно-профілактичних засобів правоохоронних органів і адміністративно-правового регулювання організаційно-технологічної діяльності державний та недержавних суб'єктів забезпечення інформаційної безпеки.

У даному випадку доцільно погодитися з О. Гавриловим та О. Дзюбенко, що проблема організаційно-методологічних підстав дослідження відомчої нормотворчості щодо інформаційної безпеки, як частини загальної теорії правозастосування, може бути розкрита тільки через ретельне вивчення процесів взаємодії, які протікають в умовах взаємного обміну і взаємопроникнення змісту їх науково-аналітичних апаратів, в системному аспекті щодо універсальності загального та індивідуального напрямків аналізу такого багатовимірного об'єкту, як інформаційна безпека [74; с. 27-28; 75].

Відповідно, проблема ефективності права як одного з основних регуляторів суспільних відносин, постійно знаходиться в центрі уваги правознавців, і її рішення завжди ставиться в залежність від ефективності методів правових досліджень та величини методологічного потенціалу власного юридичного інструментарію наукового освоєння об'єктивної дійсності у сфері інформаційної безпеки, як категорії техніко-економічної.

Питання про науково-теоретичне відтворення, що базується на міцній методологічній базі і якісних гносеологічних установках, що стоять сьогодні перед науковою спільнотою, набуває особливої ваги. У зазначеному контексті доцільно розглянути застосування порівняльно-правового методу наукового

дослідження адміністративно-правового регулювання інформаційної безпеки.

У міжнародних договорах у інформаційній галузі сфера безпеки є найважливішою. Необхідність посилення безпеки призвело до прийняття Загального регламенту захисту даних (англ. General Data Protection Regulation, GDPR; Regulation (EU) 2016/679). Директиви (ЄС) 2016/680 Європейського Парламенту і Ради від 27.04.2016 «Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами в цілях запобігання, розслідування, виявлення або переслідування злочинця злочину або виконання кримінальних покарань, а також про вільне переміщення таких даних, і скасування Рамкового рішення Ради 2008/977/ПВД»; Директиви (ЄС) 2016/681 Європейського Парламенту і Ради від 27.04.2016 «Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину» [76, с. 45]. Відносна схожість правових систем держав-членів Європейського Союзу (без врахування Великої Британії) на перше місце ставить нормативний спосіб проведення порівняльно-правових досліджень в галузі забезпечення інформаційної безпеки, при якому порівнюються подібні правові норми, інститути, законодавчі акти. Однак по мірі зменшення відмінностей між правовими системами України та держав ЄС, їх більшої інтеграції з іншими правовими системами країн, які є лідерами розвитку інформаційних технологій і систему (США, Японія) підвищується роль функціонального способу порівняння, при якому досліджуються правові засоби та способи; рішення подібних або однакових правових проблем у визначеній сфері.

Порівняльно-правовий аналіз адміністративно-правового забезпечення інформаційної безпеки в державах Європейського Союзу відтворює:

- спільність теоретико-методологічних підходів до формування національних законодавчих і інших нормативно-правових актів у сфері забезпечення інформаційної безпеки шляхом використання таких категорій, як «інформаційна безпека», «нормативні документи», «єдині принципи»;

- розвиненість національних адміністративно-правових засад,

забезпечення безпеки, включення у них нормативно-правових актів різної юридичної сили (від конституційних, міжнародно-правових до відомчих);

- міжгалузевий характер правового регулювання суспільних відносин у сфері забезпечення інформаційної безпеки, які переважно носить публічно-правовий характер.

Зазначене дає змогу використовувати досвід правового регулювання інформаційної безпеки у Німеччині (з врахуванням особливостей федеративного устрою), Великій Британії. Водночас спільність нормативно-правового регулювання діяльності з забезпечення інформаційної безпеки в країнах Європейського Союзу, в аспекті діяльності НАТО, дає можливість використати досвід Литви, Латвії і Естонії – членів Європейського Союзу та НАТО, де нормативно-правова база інформаційної безпеки, до вступу в НАТО, формувалась на однакових засадах з Україною [77].

Використання досвіду нормативного регулювання у сфері інформаційної безпеки країн різних нормативно-правових систем обумовлено необхідністю підвищення ефективності забезпечення інформаційної безпеки при одночасному зменшенні витрат на фінансування системи забезпечення та відповідає генеральній лінії зовнішньої політики України щодо вступу до Європейського Союзу та НАТО [78].

Розвиток кожної держави в даний час неможливий поза міжнародного контексту. Важливим фактором, що визначає напрями та хід розвитку людства стала глобалізація, яка охопила практично всі сфери людського життя. В активну фазу юридична інтеграція і інтернаціоналізація вступили після уніфікації моделей господарювання в різних країнах, переходу до ринкових відносин, становлення інституту приватної власності. Більш того, глобалізація права почалася саме завдяки зростанню потреби в захисті прав людини, і тому про правову глобалізації слід говорити, насамперед, як про глобалізацію у сфері безпеки, у тому числі інформаційної.

У найзагальнішому вигляді правова глобалізація у сфері інформаційної безпеки являє собою процес створення єдиних юридичних норм, на основі яких

будуть розвиватися відносини не тільки між країнами, а й між фізичними та юридичними особами різних держав.

Правова глобалізація сфери інформаційної безпеки повинна розглядатися як загальносвітова тенденція до зближення правових систем щодо вироблення єдиної основи для функціонування суспільних відносин у юридичній площині. Для цього необхідний єдиний юридичний інструментарій, на роль якого все частіше обираються правові інститути Європейського Союзу та США, а на теренах Співдружності незалежних держав – правові інститути Російської Федерації (за виключенням Молдови) – Модельний інформаційний кодекс для держав-учасниць СНД, Рекомендації щодо удосконалення та гармонізації національного законодавства держав-учасниць СНД у сфері забезпечення інформаційної безпеки» (23.11.2012), модельний закон «Про інформацію, інформатизацію та забезпечення інформаційної безпеки» (28.11.2014), прийняті Міжпарламентською Асамблеєю СНД [79; с. 5].

Тенденції розвитку сучасного права, обумовлені глобалізаційними процесами, досліджені Т. Чубко. [80, с. 27-28].

Правова глобалізація у сфері інформаційної безпеки характеризується кількома важливими особливостями. По-перше, розмежування кордонів між приватним і публічним, збіг і взаємозумовленість локальних і централізованих засад, залежність процесів, що проходять, і змін в праві.

По-друге, глобалізація та право, що регулює інформаційну безпеку, відчувають взаємозалежний вплив один на одного. У науці даються суперечливі оцінки впливу. В одному випадку вказується незначний вплив процесів глобалізації на право, відзначається лише необхідність невеликих корекцій у праві із збереженням основи та самостійності правової системи.

По-третє, не можна не помітити, що властиві конкретній правовій системі особливості перестають втрачати свій унікальний статус. Вчені давно помітили конвергенцію правових систем. Процес зближення країн, які раніше відносились до різних правових сімей, не дозволяє робити висновки про одні лише корекції в праві. Національні правові системи відчувають значний вплив

одна на другу завдяки прагненню до уніфікації правил поведінки.

По-четверте, відбувається формування спеціалізованих судів. У подальшому, можливе формування спеціальних міжнародних судів, рішення яких будуть набувати переважний, в порівнянні з постановами національних судів, характер.

По-п'яте, правова глобалізація у сфері, що досліджується, пов'язана з розширенням сфери правового регулювання одних відносин і необхідністю обмежувати державне панування в інших.

По-шосте, з'являються нові галузі права, ускладнюються взаємозв'язки між ними, критерії їх розмежування, що призводить до думок про формування єдиного права та правового простору, нових правових інститутів і норм.

По-сьоме, правова глобалізація у сфері інформаційної безпеки характеризується уніфікацією процесуального законодавства. Єдині правила щодо складової інформаційної безпеки – безпеки технічного характеру необхідні в умовах розвитку суспільних відносин, ускладнених участю іноземних юридичних і фізичних осіб.

По-восьме, зближення правових систем в умовах глобалізації правового забезпечення інформаційної безпеки проявляється у сфері визнання ролі, значення та місця окремих джерел права. Як відомо, країнам романо-германської правової сім'ї не властиве таке джерело, як судовий прецедент. Водночас у сучасному світі спостерігається тенденція посилення ролі судової влади та велике значення набувають акти судів.

Основним аспектом у питаннях забезпечення інформаційної безпеки в європейському адміністративному праві виступають правозахисні відношення, які виникають з природи прав людини. У вітчизняній юридичній науці дослідження правозахисних відносин здійснюються в контексті: як елемент правової системи суспільства; як предмет правозахисного регулювання; як природно-правове відношення. З точки зору інтересів людини щодо інформаційної безпеки слід визнати, що природно-правовий підхід у пізнанні правозахисних відносин відрізняється найбільшою наукоємністю та

практичною значимістю.

Основна специфіка природно-правового підходу щодо безпеки полягає у фіксуванні в правозахисних відносинах загально правової закономірності, згідно з якою в них, як в юридичному зв'язку, відбувається реальна взаємодія права природного та права позитивного [81, с. 397-398]. Головною ідеєю виступає теза про інтегративну природу правозахисних відносин, яка надається їм здатністю права людини на захист закону, як права природного, що примусово інтегрується з позитивно-правовими засадами правозахисних відносин, що, згідно з Конституцією України, виражається в програмуванні цим правом сенсу, змісту та застосування законів, діяльності законодавчої та виконавчої влади, місцевого самоврядування [82, с. 10-11].

Реалізація концепції природно-правового підходу передбачає обґрунтування спеціальної методології дослідження правозахисних відносин, що дозволяє: виявити відмінності юридичних і матеріальних прав людини як прояв загально-правової закономірності, відповідно з якою юридичні права людини захищаються, а матеріальні охороняються; визначити роль категорії «інформаційна безпека» в якості вихідної, базової для дослідження практики захисту та охорони прав людини в їх єдності та спільно із засобами свого забезпечення; виявити, що правозахисні відносини, будучи формою реалізації правозахисних гарантій людини та правозахисних обов’язків держави, її органів і посадових осіб, ні інструментально, ні функціонально не розраховані на втілення в них каральних санкцій, і навпаки, охоронні правовідносини, що припускають реалізацію собою штрафних санкцій, виявляються непристосованими для здійснення захисних заходів, які, хоча й уособлюють собою правовий примус, але не містять в собі карально-правового потенціалу.

Важливим результатом використання спеціальної методології дослідження правозахисних відносин є висновок про наявність в суб'єктивній структурі кожного права людини, в тому числі і права людини, на захист у інформаційній сфері, можливості індивіда використовувати організаційні та методологічні принципи, що гарантує виконання всіх інших правочинів. У

структурі права людини на захист закону ця можливість, не змінюючи природи самого права, виступає реальною правовою основою виникнення правоохоронних відносин з відносин правозахисних, чим забезпечується діалектична зв'язаність відносин правозахисних з відносинами правоохоронними. Виникнення правозахисних відносин у сфері інформаційної безпеки – юридична закономірність, що має під собою строго певні передумови, формування яких є, в той же час, і початком складання системи їх правового регулювання.

Як вказує М. С. Кельман розглядаючи методологія дослідження як наукове пізнання, методологія будь-якого теоретико-правового дослідження має трирівневу структуру (дослідницькі підходи, методи та прийоми), у дослідженнях необхідно використовувати методологічні дослідницькі підходи – основані на висновках світоглядних ідей, які в межах тієї чи іншої наукової парадигми визначають для науковця особливості виявлення, добору та систематизації досліджуваних фактів, а також їх інтерпретації й оцінки. Завдяки цим дослідницьким підходам уможливлюється пізнання правових явищ та їхніх властивостей [83, с. 201].

Специфічна природа методології дослідження інформаційної безпеки полягає в інтеграції наукових знань про способи та засоби пізнання правової реальності, закономірностей її розвитку та їх адекватного відображення у формуванні понятійного апарату. Інтегративний підхід – це взаємозв'язок основних структурних елементів адміністративно-правової науки: об'єкта наукового пізнання (правова реальність), предмета наукового пізнання (закономірності розвитку), принципів і методів наукового дослідження (способи пізнання), правил і прийомів правового пізнання (засоби пізнання), категоріального та понятійного апарату. Основним елементом методології є система спеціальних юридичних методів: системного, синергетичного, герменевтичного, історико-правового, порівняльно-правового та формально-юридичного.

Узагальнюючи, доцільно відмітити, що з позиції методології юридичної

науки, парадигма інформаційної безпеки має структуру яку утворюють елементи: методологія правозастосування, законодавство України, систематика адміністративного права, норми адміністративного права, адміністративно-правові відносини, юридична кваліфікація адміністративно-правових відносин, тлумачення норм права, механізм застосування закону, державна правова політика в галузі інформаційної безпеки, культура і етика застосування законодавства, яке встановлює обмеження прав і свобод людини та громадянина, стратегія та тактика діяльності суб'єктів забезпечення інформаційної безпеки, ефективність застосування законодавства, право-застосовна експертиза актів відомчого нормативно-правового забезпечення інформаційної безпеки. Кожен з названих елементів парадигми інформаційної безпеки може бути представлений у самодостатньому вигляді оригінального спеціально-юридичного вчення.

Юридична методологія відіграє принципову роль у розвитку наших уявлень про інформаційну безпеку, його структуру та елементи, вдосконалення механізму впливу права на суспільні відносини з метою гармонізації соціального середовища та зміцнення безпеки в різних прикладних аспектах. Поступове проникнення в сутність правових явищ детермінує планомірне ускладнення пізнавального процесу, посилює його методологічну силу на різних стадіях суспільно-політичного та економічного розвитку держави. Гносеологічний досвід освоєння правової дійсності показує, що для розвитку інформаційної безпеки, як сегменту правового життя особи, суспільства та держави істотне значення мають не тільки позитивні результати наукових досліджень, а й шляхи, які стимулюють пошук істини та призводять до таких результатів.

Отже, під час проведення дослідження правових аспектів механізму інформаційного забезпечення не треба обмежуватися лише власними методами правознавства, потрібно використовувати широкий арсенал сучасної наукової методології. Зокрема, доцільно застосовувати діалектичний, структурно-функціональний, системно-структурний, порівняльно-правовий, історичний та

інші методи наукового пізнання, які дають змогу всебічно дослідити механізми інформаційного забезпечення та реалізувати можливості порівняльно-правового, конкретно-соціологічного, історичного та логічного аналізів. Таке комплексне застосування методів уможливлює досліджувати проблеми у єдності їх соціального змісту і юридичної форми, здійснювати системний аналіз вказаних питань [84, с. 306].

Аналіз розгляду вихідних методологічних засад поняття та змісту інформаційної безпеки дозволили зробити наступні висновки:

- вихідні методологічні засади дослідження поняття та змісту інформаційної безпеки базується на системі спеціальних юридичних методів: системного, синергетичного, герменевтичного історико-правового, порівняльно-правового та формально-юридичного. Герменевтичний підхід дає можливість розширити кордони предметного поля інформаційної безпеки, синергетичний метод дозволить розглянути захист безпеки як складне функціональне явище, діалектичний метод дозволить розкрити процес забезпечення інформаційної безпеки в єдності с ціннісною свідомості суспільства;

- методологія дослідження інформаційної безпеки полягає в інтеграції наукових знань щодо способів і засобів пізнання правової реальності, закономірностей її розвитку, адекватного відображення у понятійному апараті;

- з позиції методології права парадигма інформаційної безпеки має структуру, яку утворюють: методологія правозастосування, законодавство України, систематика адміністративного права, норми адміністративного права, адміністративно-правові відносини, юридична кваліфікація адміністративно-правових відносин, тлумачення норм права, механізм застосування закону, державна правова політика в галузі інформаційної безпеки, культура і етика застосування законодавства, яке встановлює обмеження прав і свобод людини та громадянина, стратегія та тактика діяльності суб’єктів забезпечення інформаційної безпеки, ефективність застосування законодавства, експертиза актів відомчого нормативно-правового забезпечення інформаційної безпеки.

1.3 Нормативно-правове забезпечення інформаційної безпеки в Україні

Розвиток нормативно-правового забезпечення інформаційної безпеки в Україні обумовлюється виникненням якісно нових соціальних явищ, пов'язаних з інформацією, відповідно, збільшеним увагою законодавця до упорядкування цієї галузі суспільних відносин. Сьогодні все більше збільшується значення інформації в самих різних соціальних процесах. Активне використання засобів обробки та передачі інформації, розвиток нових технологій викликає суттєві зміни в економічній, політичній та інших сферах суспільного життя. Багатьма дослідниками ставиться питання про формування нового інформаційного типу суспільства, що йде на зміну індустріальному суспільству.

Вкрай важливою є необхідність створення ефективної системи забезпечення прав і свобод громадян та соціальних інститутів на вільне отримання, поширення і використання інформації та знання як найважливішої умови демократичного розвитку, щоб запобігти самостійному розвиткові та формуванню неконтрольованого інформаційного суспільства в Україні. Право має відповідати на всі виклики та загрози інформаційного суспільства [85, с. 2]. Природним наслідком стало збільшення інтересу до юридичних аспектів забезпечення безпеки в інформаційній сфері – інформаційної безпеки, що у певній мірі зумовлено інформаційною війною яку проводить Росії [86]. При цьому важливо відзначити не ослаблення, а, навпаки, посилення ролі права в нових умовах.

Слід погодитися з О.О. Золотар, що на сучасному етапі наука має в розпорядженні такі теоретичні надбання, на базі яких здійснюється технологізація інформаційної боротьби, тобто відповідні державні та недержавні структури, що причетні до такої діяльності, здійснюють розробку і апробацію нових інформаційних технологій, прийомів, методів здійснення психологічного впливу, технічних засобів необхідних для такої діяльності. Подібні зрушення не могли не відбитися на зростанні ефективності

застосування інформаційних технологій, яке може призводити до кардинальних змін в суспільній, економічній, політичній та іншій сферах окремої крани [87, с. 144]. Водночас, діалектика взаємозалежності права та інформації, показує, що право не втрачає основного призначення щодо регулювання відносини, пов’язаних з інформацією в процесах інформаційного забезпечення всіх інших соціальних відносин. Право регулює і одночасно відчуває вплив інформаційного середовища, змінюючись, виявляє нові об'єкти регулювання, трансформуючи методи свого впливу на суспільні відносини.

Всі ці фактори в сукупності зумовили виникнення наукового інтересу до проблем правового забезпечення інформаційної безпеки, систематизації законодавства в даній сфері, оцінці ефективності існуючого юридичного інструментарію, який використовується з метою регулювання захисту інформації, інформаційних прав і свобод громадян, прав і законних інтересів юридичних осіб, суспільства, держави, вироблення певної спільної концепції місця норм, що регулюють відносини, пов'язані із забезпеченням інформаційної безпеки в системі національного права. Розширення меж використання у законодавстві нового евристичного інструментарію, призначення якого обумовлюється філософськими та природничими трактуваннями сутнісних та системно-структурних властивостей сфери правового регулювання, дозволяє розкрити необмежений потенціал кожного досліджуваного феномена в органічному поєднанні як його статичних, так і, головним чином, динамічних характеристик [88, с. 12].

Вивчення названих обставин дозволяє стверджувати, що в основі формування нового структурного утворення в системі права, спрямованого на забезпечення правового захисту інтересів суб'єктів інформаційної сфери, лежать такі передумови:

- фактори та тенденції розвитку інформаційного суспільства, заснованого на масовому використанні обчислювальних засобів і інформаційних технологій, зростанні економічної та соціальної значущості інформації. У суспільстві виникає новий вид правовідносин – інформаційні, що складаються з приводу

споживання благ інформаційного характеру та потребують правового регулювання. Однак поряд з проявом інформаційних благ складається тенденція до наростання конфліктів інтересів з приводу інформаційних ресурсів, загострюються протиріччя між учасниками інформаційних процесів, виникають загрози життєво важливим інтересам особи, суспільства та держави. Відповідно виникає потреба в захисті від загроз життєво важливих інтересів особи, суспільства та держави, забезпеченні їх безпеки;

- відокремлення нового предмета правового регулювання – відносин, пов'язаних із забезпеченням стану захищеності найбільш значущих інтересів особи, суспільства та держави в інформаційній сфері від внутрішніх і зовнішніх загроз. Дані відносини є різновид інформаційних правовідносин і виникають в процесі діяльності забезпечення інформаційної безпеки;

- фактори теоретико-методологічного характеру що складають тенденцію до затребуваності з боку суспільства розвитку правової науки в галузі правового забезпечення інформаційної безпеки, що відбилося в роботах ряду вчених, які обґрунтовують наявність галузі інформаційного права (І. В. Арістова, Т. В. Аверочкіна, Л. В. Борець, Т. В. Бачинський, В. Д. Гавловський, В. В. Гриценко, О. О. Золотар, В. Ю. Нашинець-Наумова, Р. А. Калюжний, Т. А. Кобзєва, Б. А. Кормич, Т. А. Костецька, О. О. Кульчій, В. М. Куліш, А. І. Марущак, П. В. Мельник, Р. І. Радейко, О. П. Федотов, О. І. Харитонова, В. С. Шапіро, М. Я. Швець і інші [89-100]) і його структурних елементів, включаючи правове забезпечення інформаційної безпеки. Названі передумови взаємопов'язані та розглядаються як стійкі тенденції інституційного типу, а формування підгалузі правового забезпечення інформаційної безпеки носить закономірний характер. Процес виникнення в системі права нового структурного елементу (правового забезпечення інформаційної безпеки) носить об'єктивний характер. Нове правова утворення в структурі національного права має сукупність ознак підгалузі: відокремлений предмет правового регулювання; логічно пов'язану структуру та правовим режимом; комплексне використання галузевих методів правового регулювання;

високу ступень спеціалізації і інтеграції правових інститутів, що входять до його складу, кожен з яких в свою чергу також має структуру (субінстітути). Норми, що входять до складу даної підгалузі пов'язані єдністю мети правового регулювання – забезпечення інформаційної безпеки, що виражається в стані захищеності та балансі життєво важливих інтересів особи, суспільства та держави.

Підгалузь правового забезпечення інформаційної безпеки є частина системи інформаційного права, що обумовлено єдністю комплексної природи підгалузі правового забезпечення інформаційної безпеки та комплексною природою інформаційного права, включенням правовідносин, пов'язаних із забезпеченням інформаційної безпеки, до складу галузевих інформаційних правовідносин. Підгалузь правового забезпечення інформаційної безпеки є самостійним нормативним утворенням, що складається з системи норм інформаційного права, норм інших галузей права, що регулюють однорідні суспільні відносини, що виникають з приводу захисту інформації конфіденційного характеру, ліцензування діяльності по захисту інформації, встановлюють відповідальність за інформаційні правопорушення. Структурна складність підгалузі пояснюється предметною безліччю правовідносин, що виникають в ході забезпечення захищеності інтересів особи, суспільства та держави в інформаційній сфері.

Під нормативно-правовим регулюванням забезпечення інформаційної безпеки доцільно розуміти форму владного правового впливу на суспільні інформаційні відносини, що здійснюється державою з метою їх упорядкування, закріплення та забезпечення. Дане визначення співпадає з визначенням нормативно-правового регулюванням інформаційної безпеки даної Ю. Є. Максименко у дослідженні «Теоретико-правові засади забезпечення інформаційної безпеки України» [101, с.118]. Але підтримуємо думку О. О. Золотар, що оскільки інформаційна безпека є невід’ємною властивістю її об’єктів, то говорити про регулювання інформаційної безпеки немає підстав. Правове регулювання може розглядатись лише як складова забезпечення

інформаційної безпеки [91, с. 178-179]. Це обумовлює необхідність закріплення функції забезпечення інформаційної безпеки в Основному законі держави.

Стаття 17 Конституції України говорить: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [23].

С. О. Лисенко зазначає, що вплив сучасних реалій на систему управління забезпечення інформаційної безпеки формує систему конституційних засад, які будуть, в майбутньому, гарантом сучасного та законного їх регулювання. При цьому створення відповідних засад має адекватно реагувати на виклики кожного етапу розвитку інформаційного суспільства. Інформаційна революція, глобалізаційні інформаційні процеси, широкий спектр нових негативних інформаційних чинників перетворили інформаційну безпеку на категоричний імператив сучасності, як важливу сферу права та сферу адміністративно-правового регулювання. Систематизація норм інформаційної безпеки повинна відбуватись згідно з переліченими конституційними засадами, повністю позбавляючись складних процедур, зайвих перепон та найбільш узгодженою системою норм [102, с. 160].

Цілеспрямоване управління інформаційною сферою є найважливішим фактором оптимізації державного управління включає формування та поширення різних видів інформаційних впливів, управління інформаційними потоками та ресурсами, розвитком інформаційно-комунікаційної інфраструктури та ринку інформаційної продукції, послуг і технологій.

Державна політика забезпечення інформаційної безпеки повинна базуватися на наукових і методологічних розробках, систематизованих і об'єднаних в єдину концепцію. Вона може бути представлена як сукупність національних цілей, інтересів і цінностей; стратегії та тактики управлінських рішень і методів їх реалізації, що розробляються та реалізуються державною владою для регулювання та вдосконалення безпосередньо процесів інформаційної взаємодії в усіх сферах життєдіяльності суспільства та держави,

процесів (в широкому сенсі) технологічного забезпечення такої взаємодії. Метою політики забезпечення інформаційної безпеки України має стати формування відкритого інформаційного суспільства, як простору цілісної держави, інтегрувального в світовий інформаційний простір з урахуванням національних особливостей і інтересів при забезпеченні інформаційної безпеки на внутрішньодержавному та міжнародному рівнях. Необхідною умовою ефективної реалізації політики забезпечення інформаційної безпеки є розробка організаційних і технологічних заходів щодо захисту систем державного управління на державному та регіональному рівнях від несанкціонованого впливу на ці системи з метою заподіяння шкоди життєво важливим інтересам особи, суспільства та держави.

Д. О. Хом'яков розглядаючи нормативно-правове регулювання інформаційної безпеки України пише: «Під час створення сучасної та ефективної системи забезпечення інформаційної безпеки істотного значення набуває наявність відповідної нормативно-правової бази, без якої неможливо охопити усі сфери життєдіяльності суспільства в рамках єдиного правового поля, розробити загальнонаціональну концепцію розвитку держави й ефективно реалізовувати політику національної безпеки в інформаційній сфері [103, с. 183]. У 2013 роду Кабінет Міністрів України прийняв прийнято Стратегії розвитку інформаційного суспільства в Україні де інформаційна безпека віднесена до принципу розвитку інформаційного суспільства [2].

Дослідження питань прогнозування розвитку інформаційного законодавства з інформаційної безпеки набуває особливої актуальності з огляду на розширення практики використання програмно-цільових методів, методів стратегічного планування та прогнозування в публічному управлінні. Прикладом є видання в Україні актів стратегічного характеру, що визначають основні загальнодержавні напрями соціально-економічного розвитку та передбачають розробку прогнозів розвитку законодавства.

Необхідно відзначити, що з моменту появи нових загроз інформаційній безпеці внаслідок агресії Російської Федерації прийнято Стратегію сталого

розвитку «Україна-2020» де визначили загальні напрями реформування національної безпеки, Стратегію національної безпеки України де питанням інформаційної безпеки приділено значну увагу, у тому числі розвиток нормативно-правої бази, Стратегію кібербезпеки України, яка передбачає розвиток техніко-технологічних засобів забезпечення інформаційної безпеки [32; 37; 62; 104].

Дослідження правових стратегій як джерела розвитку інформаційного права доцільно здійснювати на основі соціологічної методології із застосуванням елементів формально-юридичного та управлінського підходів. Поняття «правова стратегія» (далі – стратегія) є багатозначним [105]. В основному значенні стратегія постає як деталізований план діяльності, здійснюваної з метою зміни існуючого права і процесів, що відбуваються в правовому житті, відповідно до заздалегідь сконструйованої ідеальної моделі, що відбиває певний стан чинного права та правової практики. При цьому мається на увазі, що зміна, яка виступає метою стратегії, є незворотною, спрямованою та закономірною якісною зміною чинного права і інших компонентів правової системи суспільства, тобто їх розвитком.

Як джерела розвитку права стратегії є: змістовним джерелом; джерелом, що носять програмний характер і створюють організаційні передумови для розвитку чинного права та правової практики; джерелом-умовою, що сприяють розвитку права, але не детермінують його. Інтенсивність впливу, що чиниться стратегіями на розвиток права, при інших рівних умовах збільшується в разі їх формального закріплення в офіційно визнаних державою джерелах перш за все, нормативно-правових актах, наприклад, Закони України: Про Національну програму інформатизації, Про Концепцію Національної програми інформатизації, Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки [106; 107; 108].

Стратегії як джерела розвитку права є якісно неоднорідними. Їх властивості варіюються в залежності від об'єктів, на зміну яких націлена їх реалізація; в залежності від суб'єктів, що конструюють і реалізують стратегії; в

залежності від передбачуваних засобів їх реалізації та інших обставин. Разом з тим, характер і значимість впливу, що чиниться стратегіями на розвиток права, залежать не тільки від їх якісних особливостей і форм існування, але і від властивостей середовища, в якій відбувається їх реалізація.

Характер магістральних напрямів і засобів реалізації стратегій в інформаційному праві істотно позначається на інтенсивності впливу, що чиниться на розвиток правого забезпечення інформаційної безпеки як в цілому, так і в окремих компонентах. Зокрема, існує залежність між прагненням державно-владного суб'єкта врахувати при конструюванні стратегії наявний правовий інструментарій, який потенційно може бути використаний при її здійсненні, і зниженням інтенсивності впливу, що чиниться реалізацією даної стратегії на розвиток права.

Умовою гармонізації сфери забезпечення інформаційної безпеки як однієї з основних сфер дії права є формування такої моделі взаємовідносин між людиною та державою, яка, з одного боку, забезпечить розрізнення особистісно-значущих потреб на рівні соціально-значущих інтересів, з іншого боку, буде враховувати социоцентризм масової правосвідомості.

Вивчення стратегій як джерело розвитку нормативно-правого забезпечення інформаційної безпеки, організуючого функціонування механізму правового регулювання, свідчить про те, що, з одного боку, стратегії відіграють важливу роль в оптимізації механізму правового регулювання шляхом його реформування, з іншого боку, вони не є універсальним інструментом такого реформування. Реальні можливості стратегій у вирішенні завдань, пов'язаних з функціонуванням механізму правого регулювання інформаційної безпеки, багато в чому визначаються характеристиками самих складових механізму, що підлягають реформуванню на основі стратегічного планування. Розуміння структурно-змістовних властивостей складових механізму дозволяє правильно визначити об'єкти стратегічного впливу, а, значить забезпечити максимальну ефективність.

Європейський досвід реформування системи забезпечення інформаційної

безпеки свідчить про те, що реалізація стратегічного підходу в перетворенні функціонально відокремлених підсистем, що входять в механізм правового регулювання, може бути найбільш успішною за умови, що стратегічним плануванням буде охоплена реорганізація саме тих складових таких підсистем, які організовані за принципом систем інформаційного типу, на основі нормативно-правових актів виданих на виконання положень стратегій. Як зазначає Т. Ю. Ткачук розглядаючи інформаційну безпеку в законодавстві європейських країн: «Варто констатувати, що країни ЄС мають «у певному сенсі злагоджену систему захисту інформації» [109, с. 146]

Доктрини в сфері інформаційної безпеки, що реалізуються державою, виступають засобами рішення, перш за все, політичних, а не правових задач, що обумовлюється не вадами проведеної політики, а об'єктивно існуючими закономірностями та тенденціями розвитку права.

Доктрина інформаційної безпеки України визначає національні інтереси в інформаційній сфері: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів; життєво важливі інтереси суспільства і держави [19]. Зміни, що відбуваються в сфері інформаційної безпеки особи, свідчать про те, що вибір реалізованих доктрин не є довільним ні з точки зору її цільової спрямованості, ні з точки зору засобів, використовуваних для її реалізації. Сфера інформаційної безпеки особи є відображенням сутнісних характеристик права. У зв'язку з цим закономірним виявляється те, що цільову спрямованість визначає гуманізація, базова для сфери інформаційної безпеки особи, що характеризує змістовними змінами, які відбуваються в перш за все в європейському праві. Юридизації, яка виступає тенденцією розвитку форм інформаційного права, визначає засоби, за допомогою яких відбувається здійснення гуманізації інформаційної безпеки особи.

Реалізація Доктрини інформаційної безпеки України в контексті

гуманізації не може бути забезпечена в умовах подальшої формалізації діяльності ні за допомогою перебудови системи суб'єктів, що реалізують інформаційну політику і забезпечують інформаційну безпеку, ні за допомогою зміни процесуального законодавства, ні за допомогою створення нових, додаткових гарантій забезпечення та захисту прав людини в сфері правосуддя, без зміни нормативно-правової бази технічної складової. Указаний підхід обґрунтовано у аналітичній записці Національного інституту стратегічних досліджень при Президенті України «Проблеми впровадження сучасних стандартів інформаційної безпеки в умовах становлення національної системи кібербезпеки України» (2018 р.) [64].

Т. В. Тарасенко відзначає, що визначення основних принципів державної інформаційної політики, розподіл повноважень і відповідальності державних органів у забезпеченні інформаційної безпеки значно посилюють позиції України в інформаційному протистоянні та створюють, за умови прийняття у руслі Доктрини інформаційної безпеки відповідного законодавства, необхідну основу для ефективного подолання інформаційних загроз у нинішній гібридній війні [110].

Особливості розвитку інформаційної сфери свідчать про те, що існують об'єктивні передумови для зниження ефективності стратегічного планування та реалізації Доктрини інформаційної безпеки України. До числа таких передумов, насамперед, відноситься суперечливість розвитку національного права внаслідок нерівномірної адаптації правової бази інформаційної безпеки до вимог Європейського Союзу та НАТО [111, с. 188].

Дослідження нормативно-правового забезпечення інформаційної безпеки знайшли відображення у монографіях українських вчених: О. О. Золотар «Інформаційна безпека людини:теорія і практика» (2018 р.), А. Ю. Нашинець-Наумової «Інформаційна безпека: питання правового регулювання» (2017 р.), О. А. Баранова «Правове забезпечення інформаційної сфери: теорія, методологія і практика (2014 р.), О. О. Тихомирова «Забезпечення інформаційної безпеки як функція сучасної держави», О. А. Заярний «Правове

забезпечення розвитку інформаційної сфери України: адміністративно-деліктний аспект» (2018 р.) і інших [36; 41; 57; 91; 112].

Монографічні дослідження забезпечення інформаційної безпеки України здійснювались і до 2014 року, однак, з погляду на думки авторів аналітичної доповіді Національного інституту стратегічних досліджень при Президентів України «Активні заходи» СРСР проти США: пролог до гібридної війни» Д. В. Дубова, А .В. Баровської, В. П. Горбуліна; Т .О. Ісакової, І. О. Коваля, державна політика в сфері інформаційної безпеки суттєвим чином змінилася, відповідно перед державою постали нові завдання які потребують нового нормативно-правого регулювання [113; 114; 115]. Тому, у дисертаційній роботі ми приділимо уваги тим аспектам, які на нашу думку, не відображено у наукових дослідженнях з 2014 року.

Соціальна цінність права визначається його здатністю ефективно реалізовувати властиві йому функції. Проблеми, пов'язані з характеристикою права в його дії, є актуальними для нормативно-правового забезпечення інформаційної безпеки. Дія права передбачає не тільки нормування (встановлення норм, пред'явлення вимог тощо), воно не вичерпується наданням прав і покладанням обов'язків, моделюванням відносин. Про ефективне функціонування права можна вести мову тільки тоді, коли нормативні встановлення знаходять реальне здійснення на практиці.

Особливістю нормативно-правого забезпечення інформаційної безпеки в Україні, країнах-членах Європейського Союзу є те, що в більшості законодавчих актів, на нашу думку, виступають в якості правого гарантування. Вказаний висновок можна зробити на підставі дослідження В. Г. Пилипчука, та І. М. Дороніна, які вважають, що правовий режим безпеки складається з великої групи однорідних суспільних відносин, які становлять окрему, відносно самостійну сферу суспільного життя, що є предметом підгалузі права. Для правового режиму в такому контексті характерною є наявність особливої цілісної системи регулятивного впливу, яка характеризується специфічними прийомами регулювання, особливим порядком виникнення та формування

змісту прав і обов’язків, їх реалізації, дією єдиних принципів, загальних положень, які поширюються на сукупність правових норм [116, с. 66]. Це зумовлює наявність зв'язку правового гарантування з гарантуванням, здійснюваним державою за допомогою технічних, економічних, політичних, ідеологічних і інших засобів. У контексті техніко-технологічного напряму дослідження інформаційної безпеки гарантіям, відмінним від правових, традиційно приділяється увага в правових дослідженнях, так, як вважається, що реалізація технічних, економічних, політичних, ідеологічних та інших гарантій здійснює вплив на ефективність правового гарантування. В інформаційному праві значення для оптимізації правового гарантування має вдосконалення діючих нормативно-правових актів, що визначають правові гарантії та порядок їх реалізації.

Правове гарантування за своєю природою є органічною складовою дії права, проте в правовому гарантуванні потребує не будь-яке правовідношення. У забезпеченні ефективної дії нормативно-правого регулювання забезпечення інформаційної безпеки роль правового гарантування дійсно принципово значима тільки тоді, коли мова йде про захист базових правових цінностей. Поряд з універсальними рисами, властивими правовому гарантування інформаційної безпеки за природою, йому властива культурно-історична специфіка, обумовлена інформаційними правами людини [117, с. 20].

Особливості правового гарантування інформаційної безпеки в суспільствах демократичного (країні-члени Європейського Союзу, США. Японія, Канада і інші демократичні правові країни) та тоталітарного типу (країни Євразійського економічного союзу – Російська Федерація, Білорусія, Казахстан, Киргизія, Таджикистан) обумовлюються відмінностями в характерному для масової правосвідомості уявлення про співвідносини значущості приватноправових і публічно-правових інтересів. У суспільствах демократичного типу правове гарантування орієнтоване, перш за все, на забезпечення реалізації значимих, у контексті права, інтересів, в суспільствах тоталітарного типу – на підтримку сформованої системи відносин. У

суспільствах демократичного типу базовою правовою цінністю і основним об'єктом гарантування виступають права та свободи людини, в суспільствах тоталітарного типу – порядок.

Відповідно основним завданням нормативно-правого регулювання забезпечення інформаційної безпеки у Європі і інших правових країнах є захист прав і свобод людини, суспільства та держави, у країнах Євразійського економічного союзу, країнах з тоталітарним режимом, – забезпечення існуючого порядку. У якості прикладу доцільно вказати на підручник з інформаційного права, які вийшли у світ і інші матеріали з даного питання [118-122]. Це є суттєвою відмінністю правових засобів, що використовуються в Україні та Російській Федерації з метою нормативно-правого регулювання забезпечення інформаційної безпеки.

Другою суттєвою відмінністю нормативно-правого регулювання забезпечення інформаційної безпеки в Україні та Російській Федерації є застосування держано-приватного партнерства на засадах впровадження європейського досвіду. В аналітичній записці Національного інституту стратегічних досліджень при Президенті України «Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні» (грудень 2017 р.) зазначено, Закон України «Про основні засади забезпечення кібербезпеки України» та Стратегія кібербезпеки України заклали основи національного галузевого законодавства і визначили ключові вектори його подальшого розвитку відповідно до європейських демократичних практик. В обох документах значущу увагу приділено питанню правового регулювання державно-приватного партнерства (у Законі застосовується форма «державно-приватна взаємодія») у забезпеченні кібербезпеки як складової інформаційної безпеки [123, с. 2].

Доцільність запровадження державно-приватного партнерства відображена у аналітичних записках Національного інституту стратегічних досліджень при Президенті України: Досвід Німеччини у функціонуванні платформ державно-приватного партнерства в сфері кібербезпеки (травень 2018

р.), Державно-приватне партнерство в кібербезпековій сфері: досвід республіки Польща (березень 2018 р.), Нормативно-правові та організаційні засади державно-приватного партнерства США у сфері кібербезпеки (лютий 2018 р.), Державно-приватне партнерство у сфері кібербезпеки: кейс Німеччини (січень 2018 р.) [124-127]. Це питання заслуговує найпильнішої уваги, як і питання про базові принципи правового забезпечення інформаційної безпеки [128, с. 112].

Водночас, у Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» (у редакції від 19 квітня 2014 року) державно-приватне партнерство у контексті інформаційної безпеки не зазначено, що вимагає внесення змін і доповнень до нормативно-правого акту. На даний аспект звернута увага респондентів у ході соціологічного опитування (*Додатки Б, В*) [129]. Відповідно у Законах України «Про державно-приватне партнерство», «Про Державну службу спеціального зв'язку та захисту інформації України» не має терміну «державно-приватна взаємодія», що вимагає внесення змін і доповнень (Додатки Д, Ж) [130].

У соціальній системі забезпечення інформаційної безпеки України сформувалися системи інформаційної безпеки телекомунікаційних мереж і систем, що складаються з різних за структурою техніко-технологічних систем де застосовуються інформаційно-комунікаційні технології різних поколінь. Ці мережі та системи у більшості відносяться до об'єктів критично важливої інформаційної інфраструктури [131].

Зазначений стан потребує суттєвого реформування на що вказує Концепції створення державної системи захисту критичної інфраструктури [132]. У даному випадку для забезпечення належного рівня інформаційної безпеки доцільно більш повно використовувати можливості нормативно-правого регулювання у технічній сфері. Закони України «Про стандартизацію», «Про метрологію та метрологічну діяльність», «Про технічні регламенти та оцінку відповідності» дають можливість врахувати великий спектр зовнішніх умов, але один стандарт повинен бути визначальним, приймаючи загальні для всієї системи інженерно-технічні рішення [133-135].

Розвиток стандартизації інформаційної безпеки це не послідовна зміна однієї техніко-технологічної системи та нормативно-правого регулювання забезпечення інформаційної безпеки іншою, а розвиток системи забезпечення в умовах розвитку інформаційних технологій і систем, зміни зовнішніх загроз, впровадження міжнародних стандартів у галузі що досліджується. При цьому умови середовища можуть сприяти прискореному впровадженню певних категорій стандартів, прийнятих міжнародними профільними організаціями, та не сприяти розвитку систем забезпечення інформаційної безпеки на об’єктах критичної інформаційної інфраструктури, що не є державною власністю. У таких умовах доцільно внесення змін і доповнень у Закон України «Про телекомунікації» щодо впровадження державно-приватного партнерства для забезпечення інформаційної безпеки телекомунікаційних систем і інших об’єктів критичної інформаційної інфраструктури (*Додаток Е*) [136].

Суспільні відносини, що виникають у межах розробки та включення обов'язкових нормативних вимог до технічних регламентів інформаційної безпеки визначені джерелами інформаційного права та нормами технічного регулювання. Але, як зазначає С. О. Гнатюк, на практиці це виражається в тому, що критерії, що характеризують інформаційні системи в якості інформаційно безпечної, відсутні, і навіть більше того – відсутні нормативні передумови для їх створення [64, с. 3]. Зазначені критерії повинні встановлюватися державою, так як ринкові інструменти саморегулювання в цій галузі неефективні, і, внаслідок цього, не застосовуються. Ліквідація цього бар'єру може бути досягнута за допомогою застосування комплексного впливу інформаційних норм і норм технічного регулювання.

Подібне рішення означеної проблеми зумовлена не тільки потенціалом системи інформаційного права, а й природою технічного регулювання. Використання технічного регулювання в якості одного з інструментів інформаційного права дозволяє збагатити не тільки технічні регламенти інформаційної безпеки їх норм, а й збагатити теорію інформаційного права. З цією метою для більш точного визначення співвідношення перерахованих

понять застосуємо інструментарій технічного регулювання, у межах якого категорія інформаційної безпеки розглядається в якості базової, тобто передбачає наявність показників, що перевищують за своєю суттю показники технічні критерії безпеки.

Це тісно пов'язано з встановленої в Доктрині інформаційної безпеки України необхідністю технологічного переозброєння та поступового виведення з експлуатації підприємств із застарілим обладнанням, оснащення підприємств сучасним обладнанням, підтримку виробництва вітчизняних засобів технічного захисту інформації.. Ці вимоги Доктрини інформаційної безпеки України відносяться до об'єктів віднесених до критично важливої інформаційної інфраструктури не залежно від форми власності.

Зв'язок технічного регулювання з інститутом інформаційної безпеки, підтверджується посиланнями, зазначеними в серії стандартів ISO/IEC 27000 (ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT)., яка основну увагу приділяє на менеджменту інформаційної безпеки, але в той же час доводить, що інформаційна безпека має комплексний характер і досягається не тільки впливом інструментів технічного регулювання, а й у межах нормативно-правого регулювання забезпечення [137].

Система технічного регулювання в Європейському Союзі за рахунок можливості різного рівня імплементації вимог директив в національне законодавство є гнучкою, але при цьому необхідно враховувати, що рівень інформаційної безпеки може коливатися в залежності від зобов'язань, прийнятих кожною країною. Водночас, не можна не враховувати, що загальний рівень інформаційної безпеки не відповідати критеріям НАТО.

Обидві системи (одна – рамкова ЄС, друга – жорстко централізована НАТО) показують один і той же результат при використанні різних моделей технічного регулювання, вертикально організовану систему (що включає вимоги інформаційної безпеки та охорони критичної інформаційної інфраструктури), коли приймається один основоположний нормативно-

правовий акт, що регламентує всю систему технічного регулювання (від загальних принципів до тих вимог, які можуть знаходити своє відображення в технічних регламентах). Всі технічні регламенти, прийняті у межах цієї системи, повинні повністю відповідати загальному нормативно-правовому акту. Можна зробити висновок, що обидві системи припускають і навіть беруть можливість включення в технічні регламенти (або директиви) вимоги, спрямовані на забезпечення інформаційної безпеки за рахунок обмеження певних інформаційних свобод в мережі Інтернет, але обов'язковими умовами при цьому будуть їх обґрунтованість, умови перевірки та неможливість їх використання для маніпулювання інформаційними потоками та психологічного тиску, зазіхати на охоронюваний законом інтерес заснований на нормах і принципах інформаційного права, гарантоване правовою забороною втручання сторонніх осіб у сферу приватних інтересів, правовою можливістю зацікавленої особи реалізувати свій інтерес усіма способами, які прямо не заборонені законом.

План заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони передбачає ряд заходів спрямованих на удосконалення нормативно-правого забезпечення інформаційної безпеки серед яких: удосконалення законодавства про захист персональних даних з метою приведення його у відповідність з Регламентом (ЄС) 2016/679 (пункт 11); сприяння розвитку національної команди реагування на комп’ютерні надзвичайні події (CERT) (пункт 41); уточнення положень щодо комп’ютерних програм (пункт 78), уточнення положень законодавства щодо охорони баз даних відповідно до положень Угоди про асоціацію (пункт 82), уточнення положень законодавства щодо забезпечення належного правового захисту проти осіб, які свідомо здійснюють без дозволу видалення або зміну будь-якої електронної інформації про управління правами та розповсюдження, ввезення для розповсюдження, передачу в ефір об’єктів авторського права і суміжних прав (пункт 105) і інші [138].

Розглянув нормативно-правове забезпечення інформаційної безпеки в Україні доцільно зробити наступні висновки.

Нормативно-правове забезпечення інформаційної безпеки включає процеси: розробки; реалізації; саморегулювання. Кожному із зазначених елементів необхідний достатній набір засобів нормативно-правового та іншого характеру. Нормативно-правове забезпечення інформаційної безпеки в цілому, так і на елементному рівні характеризується науковістю, системністю та має багато аспектів. Нормативно-правове забезпечення є науково обґрунтована, послідовна система правових і інших засобів, за допомогою яких громадянське суспільство та держава здійснює вплив на інформаційні відносини (реалізація інформаційної безпеки, саморегулювання) і відносини, безпосередньо пов'язані з розробкою інформаційної безпеки, виходячи з черговості завдань і переслідуваних цілей, що виникають перед суспільством.

Нормативно-правове забезпечення є більш широким поняттям порівняно з нормативно-правовим регулюванням. Перше представляє собою не тільки регулювання за допомогою нормативно-правових актів, а й включає сукупність взаємопов'язаних елементів соціально-економічного та правового саморегулювання. Слід співвідносити «нормативно-правове регулювання» та «нормативно-правове забезпечення» як частина і ціле.

Модернізація системи інформаційної безпеки та досягнення стабільного інформаційного середовища, стійкого економічного зростання можливі при впровадженні нормативно-правового забезпечення інноваційного характеру (що забезпечує якісне зростання ефективності управлінських процесів і створення інституційних і законодавчих умов для впровадження нововведень в інформаційну політику), що враховує поточний потенціал розвитку України.

У ході трансформації інформаційної безпеки (від мінімального стану загроз до відкритої інформаційної війни) інформаційні відносини в Україні регулювалися за допомогою законів, підзаконних і судових актів, договорів. Закон має пріоритетне значення, однак, найчастіше в силу низької ефективності, в якості основної правової форми регулювання життя суспільства

та економіки виступають акти органів виконавчої влади, а роль договору в процесах саморегулювання зменшена. У зв'язку з цим виникає необхідність розробки та реалізації ефективної програми нормативно-правового забезпечення інформаційної безпеки.

З розвитком інтеграційних відносин, входженням України в європейський інформаційний простів, інформаційною агресією Російської Федерації пріоритетне значення набувають міжнародні акти. Політика інформаційної війни встановлює нові правила взаємодії. Законодавство, адміністративні правила, техніка та практика державного регулювання інформаційної безпеки повинні бути виведені на рівень стандартів Організації Північноатлантичного договору НАТО і Європейського Союзу з урахуванням національних особливостей інформаційної інфраструктури.

Подальші напрями нормативно-правового забезпечення інформаційної безпеки будуть визначатися завданнями щодо сприяння поступального та сталого розвитку держави, єдиного економічного простору у межах територіальної цілісності України та входження в економічний простір країн-членів ЄС, викликам з якими стикається Україна на геополітичному просторі.

Основними принципами розвитку нормативно-правового забезпечення інститутів, що створюють умови для підвищення ефективності інформаційної безпеки держави, повинні стати: прозорість і надійність засобів правового захисту інформаційних прав особи, суспільства та держави; державна підтримка інститутів громадянського суспільства для збільшення його ініціативності в розвитку нормативно-правової бази забезпечення інформаційної безпеки; законодавче закріплення реального врахування думки суб'єктів інформаційної діяльності при будь-яких змінах в законодавстві; переважне використання приватноправових засобів та засобів вироблених суб’єктами інформаційної діяльності у порядку саморегуляції щодо захисту інформаційних інтересів, спрямованих на забезпечення правопорядку в інформаційній сфері не стільки за рахунок превентивних обмежень, скільки за рахунок невідворотності швидкого реагування щодо відповідальності та

компенсації в повній мірі будь-якої заподіяної шкоди законним правам і інтересам фізичним та юридичним особам; підвищення відкритості механізмів, що забезпечують реалізацію інформаційних прав всіх осіб, що беруть участь в інформаційній діяльності, незалежно від форми власності; створення системи необхідних і достатніх правових процедур державного і громадського контролю реалізації інформаційної безпеки.

Висновки до розділу 1

Розглянув теоретико-правові засади забезпечення інформаційної безпеки в Україні доцільно зробити висновки.

Поняття «інформаційна безпека» має дефініції в різних нормативно-правових актах. Така множинність визначень заважає коректному застосуванню законодавчих положень і свідчить про необхідність формування законодавчого тезауруса визначень в галузі інформаційного права. Водночас, завдання та мета інформаційної безпеки істотно змінилися та набули нових властивостей і якості, що вимагають переосмислення і перегляду правових відносин, сформованих раніше в інформаційній сфері. З метою ефективного впровадження та реалізації, вдосконалення правового режиму інформаційної безпеки в умовах розвитку інформаційного суспільства і агресії Російської Федерації обґрунтовується науковий підхід, який передбачає, що під інформаційною безпекою слід розуміти стан захищеності інформаційних ресурсів, базах даних інформації, інформаційних технологій і технічних засобів, що реалізують певні технологічні дії за допомогою інформаційних процесів, призначених для збору, обробки, зберігання та передачі інформації, необхідної для реалізації прав, обов'язків і законних інтересів суб'єктів інформаційної діяльності, особи, суспільства та держави в інформаційному просторі від впливу на них особливого виду загроз, які виступають в формі цілеспрямованої або стихійної діяльності в інформаційному середовищі.

Інформаційну безпеку слід розглядати як систему суспільних відносин,

що виражає зв'язок між інтересами особи, суспільства та держави в сфері інформації та правовим забезпеченням їх захисту, охоплює стан захищеності особи, суспільства та держави в інформаційному просторі, інформаційних ресурсів держави, інформації і інформаційних ресурсів, інформаційно-телекомунікаційної інфраструктури від можливих внутрішніх і зовнішніх загроз. Нормативно-правова природа інформаційної безпеки забезпечує її функціонування як інституційної організаційної та правової системи регулювання правовідносин які є частиною системи суспільних відносин, обумовлені змістом економічних, техніко-технологічних, політичних, правових та культурних зв'язків, які характеризують суспільну та державну системи.

Інформаційна безпека виступає в якості об’єкта правової захисту. Правові засоби забезпечення інформаційної безпеки є провідним фактором захисту національних інтересів в даній сфері, а їх застосування визначається: оптимізацією балансу відносин між правом суб'єктів інформаційних відносин на отримання інформації та правом на встановлення обмежень даних відносин з боку інших осіб щодо відомостей, володарями яких вони є; розробкою та реалізацією правових заходів захисту інформації, доступ до якої повинен обмежуватися правовими підставами в процесі захисту інформаційних ресурсів. Правове забезпечення ліквідації загроз і ризиків у сфері інформаційної безпеки є основним фактором структурування, формування, розглядається як законотворча діяльність, спрямована на запобігання нанесення шкоди інтересам особи, суспільства та держави в інформаційній сфері. Сукупність потенційних загроз інформаційній безпеці поширюється на сферу конституційних права і свобод громадян, духовне життя суспільства, інформаційну інфраструктуру та інформаційну ресурси.

У даний час необхідно говорити про функціонування системи забезпечення інформаційної безпеки, що складалася протягом усього періоду існування незалежної української держави, в першу чергу через зміцнення національної безпеки, як про механізм, що перетворює прийняту державою стратегію в галузі забезпечення інформаційної безпеки в скоординовану

діяльність органів публічної влади, інститутів громадянського суспільства та громадян на основі чинного законодавства.

Методологія дослідження інформаційної безпеки полягає в інтеграції наукових знань щодо способів і засобів пізнання правової реальності, закономірностей її розвитку, адекватного відображення у понятійному апараті. У науці склалося два напрями дослідження інформаційної безпеки технологічний та гуманітарний, що охоплює правове забезпечення при якому правова основа інформаційної безпеки України розглядається через призму галузей права, що дозволяє виокремити юридичну складову проблем для створення універсальних правових механізмів забезпечення інформаційної безпеки. Вихідні методологічні засади дослідження поняття та змісту інформаційної безпеки базується на системі загальнонаукових і спеціальних юридичних методів: системного, синергетичного, герменевтичного, історико-правового, порівняльно-правового та формально-юридичного і інших. Системний метод дає можливість розглянути інформаційну безпеку її техніко-технологічну та гуманітарну складові з позиції теорії систем. Герменевтичний підхід дає можливість розширити кордони предметного поля інформаційної безпеки, синергетичний метод дозволить розглянути захист безпеки як складне функціональне явище, історико-правовий і порівняльно-правовий метод дозволить розкрити процес забезпечення інформаційної безпеки в єдності с ціннісною свідомістю суспільства.

З позиції методології права парадигма інформаційної безпеки має структуру, яку утворюють: методологія правозастосування, законодавство України, систематика адміністративного права, норми адміністративного права, адміністративно-правові відносини, юридична кваліфікація адміністративно-правових відносин, тлумачення норм права, механізм застосування закону, державна правова політика в галузі інформаційної безпеки, культура і етика застосування законодавства, яке встановлює обмеження прав і свобод людини та громадянина, стратегія та тактика діяльності суб’єктів забезпечення інформаційної безпеки, ефективність застосування законодавства, експертиза

актів відомчого нормативно-правового забезпечення інформаційної безпеки.

Під нормативно-правовим регулюванням забезпечення інформаційної безпеки доцільно розуміти форму владного правового впливу на суспільні інформаційні відносини, що здійснюється державою з метою їх упорядкування, закріплення та забезпечення. Нормативно-правове забезпечення є науково обґрунтована, послідовна система правових і інших засобів, за допомогою яких громадянське суспільство та держава здійснює вплив на інформаційні відносини (реалізація інформаційної безпеки, саморегулювання) і відносини, безпосередньо пов'язані з розробкою інформаційної безпеки, виходячи з черговості завдань і переслідуваних цілей, що виникають перед суспільством.

Нормативно-правове регулюванням забезпечення інформаційної безпеки представляє різновид публічно-правового регулювання, що має на меті забезпечення публічних інтересів в інформаційній сфері, яке поєднує застосування конституційного, фінансового, адміністративного, інформаційного і інших публічно-правових методів регулювання суспільних відносин на основі норм адміністративного права.

Під адміністративно-правовим регулюванням забезпечення інформаційної безпеки розуміється цілеспрямований вплив на інформаційні відносини в сфері державного управління системою адміністративно-правових засобів регулювання, закріплених в нормах чинного законодавства, що визначають напрями забезпечення інформаційної безпеки в різних сферах життєдіяльності держави, суспільства і особи. Модель оптимізації адміністративно-правового регулювання забезпечення інформаційної безпеки, маючи визначені конструктивні принципи і елементи представляє єдиний комплекс форм і методів впливу на зазначені відносини у вигляді адміністративно-правової моделі правого регулювання.

З урахуванням того, що інформаційна безпека є об'єктом комплексного правового регулювання різних галузей права, сутність, специфіка і основні напрями та державне регулювання та державне управлінням в сфері забезпечення інформаційної безпеки здійснюється адміністративно-правовим

методом. Інформаційна безпека як адміністративно-правова категорія розглядається як системи заходів державного регулювання на основі збереження стійкого стану інформаційної сфери держави до різного виду загроз, яка, використовуючи систему адміністративно-правових методів, гарантує захист прав і законних інтересів об'єктів інформаційної безпеки.

Правова основа забезпечення інформаційної безпеки в теоретичному сенсі це сукупність різних за юридичною силою права норм, що відносяться до різних галузей і відбивають сутність процесів, що відбуваються в сфері забезпечення інформаційної безпеки, складаючи єдину систему, що сприяє вдосконаленню механізму правового забезпечення інформаційної безпеки направленого на підтримання балансу інтересів особи, суспільства та держави в інформаційній сфері за рахунок вдосконалення законодавчих засад.

РОЗДІЛ 2

СТРУКТУРА МЕХАНІЗМУ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

2.1 Поняття та принципи побудови механізму правового регулювання забезпечення інформаційної безпеки

Адміністративно-правове забезпечення інформаційної безпеки полягає в виконавчо-розпорядчої діяльності органів державної влади та місцевого самоврядування з забезпечення виконання загальнообов'язкових умов та вимог безпеки, що пов'язано з безпосереднім втручанням в адміністративно-господарську, організаційно-розпорядчу і іншу діяльність фізичних і юридичних осіб, організаційно не підлеглих даними органам, врегульованою нормами адміністративного права, здійснювана в цілях охорони та захисту законних інтересів учасників відносин, що виникають у сфері забезпечення інформаційної безпеки. Забезпечення безпеки, що включає в себе різноякісні елементи, об'єктивно повинна здійснюватися різними способами завдяки механізму правого регулювання.

Поняття механізму правового регулювання пов'язане з правовим регулюванням, яке представляє собою форму впливу права на суспільні відносини за допомогою системи спеціальних юридичних засобів. С. С. Алексєєв підкреслював, що право як регулятор – це не тільки одна з найважливіших проблем теорії права, розглянутого в якості інституційного нормативного утворення. Перед нами проблема ширшого наукового значення. Тут відкривається перспектива нового підходу до права в цілому. Такого підходу, який невідомий догматичної юриспруденції, виходить за її межі, характеризується тим, що право розглядається в дії, в русі, згідно закладеним в ньому потенцій і закономірностям, що дозволяє побачити найбільш істотні сторони логіки права. Категорією, через яку реалізується така наукова

перспектива, є поняття «правове регулювання» [139, с. 347].

Механізм правового регулювання також є категорією теорії права, яка повинна відображати момент «руху правової форми», спосіб її функціонування і систему юридичних засобів впливу, які в сукупності складають механізм правового регулювання. Як видно, сутність і зміст механізму правового регулювання пов'язані з поняттям правового регулювання. Їх зв'язок є вихідним при дослідженні механізму правового регулювання. У зв'язку з цим деякі автори розглядають механізм правового регулювання як «технологічну схему» правового регулювання.

Наприклад, К. І. Валігура вважає, що механізм правового регулювання є певною теоретико-методологічною категорією, яка дозволяє виявити місце, «субординацію», функції, правові засоби, які застосовуються в процесі правового регулювання на різних стадіях, і надає можливість уявити у взаємозв’язку всі правові засоби, на основі яких відбувається правове регулювання [140, с. 21]. Знаючи механізм можна уявити, які ланки пройде процес втілення норми права в життя, які зупинки та збої можуть статися в цьому процесі. Відповідно можна запропонувати науково обґрунтований план підвищення ефективності правового регулювання за рахунок зміцнення основних ланок. При цьому склад і структура механізму правового регулювання як складна система, що складається з правових засобів, суб'єктів, які здійснюють правове регулювання чи правову діяльність, є дискусійними.

У методологічному плані важливо, щоб механізм дозволяв відповісти на питання, за допомогою яких інструментів, засобів право надає регулюючу дію на ті чи інші суспільні відносини.

С. С. Алексєєв висловлював думку про те, що механізм правового регулювання дозволяє зібрати разом явища правової дійсності (норми, правовідносини, юридичні акти та ін.), Окреслити їх як цілісність (це досягається, в тому числі, за допомогою поняття «правова система»), уявити в працюючому вигляді, висвітлити специфічні функції, які виконують ті чи інші юридичні явища в правовій системі, показати їх зв'язок між собою, взаємодія

[139, с. 364].

На думку О. М. Куракіна, оскільки, механізм правового регулювання, з одного боку, функціонує в одному системному утворенні – суспільстві, а з іншого – він сам є системою елементів, доведено про наявність двох рівнів його функцій: зовнішніх (загально соціального характеру, що визначають зміст загально регулятивного впливу на суспільство) та внутрішніх (напрями правового впливу на конкретні суспільні відносини) [141, с. 364].

Процес створення механізму правового регулювання ґрунтується на правовій культурі, правосвідомості суб'єктів права, встановлених і закріплених правових принципах, що становлять разом з самим механізмом правового регулювання комплекс заходів (механізм правового впливу), який часто називають головним засобом науково обґрунтованого та соціального управління.

Управління покликане забезпечувати ефективність практичної діяльності суб'єктів, тобто створювати умови для досягнення поставленої мети найбільш економними та прогресивними засобами. Це планомірний і поетапний процес, в якому на перший план висувається організуючі засади, що складається в результаті немайнових акцій учасників даних соціальних зв'язків.

Управління суспільними відносинами, що виникають в інформаційній сфері, це найбільш складний процес, що визначає специфіку правового впливу на ці відносини. З одного боку, воно забезпечується державою (конституційний постулат), але з іншого боку, жорсткі приписи можуть погубити ініціативу суб'єктів, тим самим загальмувати процес економічного розвитку суспільства.

Інформаційне середовище, незважаючи на наявність об'єктивно властивих йому недоліків і необхідність державного регулювання, є все ж саморегульованою системою, яка передбачає вільну, активну діяльність суб'єктів підприємництва в інформаційній сфері.

Регулюючий вплив держави має не порушувати нормальні ринкові зв'язку, а створювати умови для розвитку механізмів саморегуляції, використовуючи при цьому економічні методи і інструменти впливу.

Важливою складовою цього процесу є постійний моніторинг його ефективності та миттєве реагування на найменші збої в керованій системі.

Таким чином, під механізмом правового регулювання розуміється система правових засобів, що використовуються для управління суспільними відносинами. Під терміном «система» (від грецького σύστημχ – тобто складене з частин з'єднання) в філософському сенсі розуміють ціле, утворене шляхом об'єднання закономірно пов'язаних один з одним предметів, явищ тощо [142]. Останні є її елементами, складовими частинами. При цьому якості системи як самостійного цілого ніколи не зводяться до якостей елементів, що утворюють систему Оскільки елементи об'єднуються в систему, підкоряючись об'єктивним закономірностям, між ними виникають стійкі зв'язки, що формують внутрішню форму, тобто структуру системи. Таким чином, будь-яка система складається з елементів і системоутворюючих зв'язків [143, с. 26-27].

Склад елементів механізму правового регулювання є спірним: різними дослідниками називаються різні елементи. Невизначеність складу механізму правового регулювання повинна бути усунена, враховуючи, що набір правових засобів, що використовуються методи та способи правового регулювання в кінцевому підсумку визначають правову природу механізму правового регулювання.

Деякі дослідники відносять до числа основних елементів механізму правового регулювання: норми права; правовідносини; акти реалізації; акти застосування права [144, с. 76].

Інший, інституційний, підхід застосовується в роботах С. С. Алексєєва, який виділяв наступні три основних ланки в механізмі правового регулювання: юридичні норми, правові відносини, акти реалізації прав і обов'язків; факультативне ланка – індивідуальні приписи та акти застосування права [139, с. 364–365].

Ще одним свідченням неоднозначності підходу вчених-юристів до змісту механізму правового регулювання є позиція О. В. Стукаленка та В. І. Осадчого. Зміст першої і останньої ланки доповнюють юридичними засобами

нормативного характеру і юридичними засобами реалізації права [145, с. 21].

Представляється можливим не погодитися з думкою тих авторів, які виключають юридичні факти з механізму правового регулювання. Юридичний факт є тим елементом, що пов'язує норму права з конкретною фізичною подією. Без юридичних фактів механізм правового регулювання не «запрацює».

На думку О. Я. Кархут, нормативно-правова регламентація суспільних відносин знаходить своє відображення в такому елементі механізму правового регулювання як правова норма [146, с. 8]. З огляду на різноманіття джерел вираження норм права в інформаційних правовідносинах, вважаємо за можливе погодитися з правовою позицією Ю. В. Кривицького, який запропонували розширити перший елемент механізму правового регулювання, включивши в нього не тільки норми права, що містяться в законодавстві, але також спеціалізовані норми права і інші норми [147, с. 10].

Доцільно погодитися з пропозицією дослідників про використання поняття «юридичні засоби» в складі термінів, які розкривають зміст механізму правового регулювання. Завдяки такому підходу в першу стадію механізму правового регулювання допустимо включити не тільки правові норми, а й інші засоби нормативного характеру, в тому числі засоби саморегулювання, правила та стандарти, що обґрунтовано в побудові ефективного механізму правового регулювання інформаційної безпеки. За допомогою норм, що містяться в законодавстві, законодавець створює напрям розвитку суспільних відносин, а в інформаційних відносинах, які опосередковують інформаційний обіг, визначає своєрідні рамки для подальшого саморегулювання відносин суб'єктів підприємницької діяльності [139, с. 364-365]. Крім того, важливою функцією правових норм є стимулювання розвитку одних суспільних відносин і стримування (можливо виключення) інших. Елементи правової політики держави закріплені в диспозиції норм.

Ряд учених не згодні з думкою про виділення юридичних фактів в самостійну ланку механізму правового регулювання. На думку Л. О. Шапенко, юридичні факти не просто беруть участь у формуванні законодавства та

практики його застосування, а значної мірою задають їм необхідний вимір та впливають на їх ефективність входять в усі стадії механізму правового регулювання [148, с. 224].

Доцільно погодитися з точкою зору про юридичний факт як істотному елементі правового механізму.

С. Л. Саржан зазначає, що юридичний факт з позиції національної та державної безпеки в рамках адміністративно-правової науки та конституційного права це державно-владна діяльність компетентних органів держави щодо внесення правових актів як важливого засобу державного управління суспільством чи події, або певні обставини, що визначені в нормах права, і обумовлюють виникнення, зміну чи припинення правовідносин у сфері національної безпеки та правоохоронної діяльності. Це положення може бути первинним, вихідним або визначальним при похідних темах дослідження шляхів формування системи національної безпеки (одним з елементом якої є інформаційна безпека, прим. Т. П.) та її удосконалення [149, с. 33].

Правовідносини – один з основних елементів механізму правового регулювання, покликаний втілити ідеальну модель, передбачену нормою, в реальну поведінку суб'єктів. З їх допомогою механізм приводиться в рух, виникає правовий зв'язок між учасниками через конкретизацію і єдність суб'єктивних прав і юридичних обов'язків.

У цілому засоби, що використовуються для регулювання відносин, що виникають в інформаційному середовищі, різноманітні та включають не тільки традиційні правові, а й економічні, технологічні, інформаційні, технічні засоби, які в процесі реалізації норм права набувають правову форму та стають взаємопов'язаними елементами механізму, спрямованого на стимулювання, стримування або виключення відповідних суспільних відносин.

На нашу думку, набір засобів правового регулювання в інформаційній сфері не може бути обраний довільно він зумовлений потребами розвитку громадянського і інформаційного суспільства та ринкової економіки.

З урахуванням наведеного вище аналізу правової літератури з теорії права

вважаємо за можливе визначити наступні елементи механізму правового регулювання: засоби нормативного характеру; акти індивідуальної регулювання. юридичні факти; правовідносини.

Зазначені елементи механізму правового регулювання пов'язані єдиною метою, яку ставить законодавець, видаючи норми права (системоутворюючий зв'язок). Крім того, правова мета є також критерієм забезпечення ефективності правового регулювання. Будучи складовою частиною процесу формування права, мета, як правило, фіксується в нормативно-правових актах безпосередньо або через принципи, обґрунтовуючи необхідність самої пропонованої моделі. Мета в праві, офіційний орієнтир законодавця.

Проблему суті механізму правового регулювання не можна розглядати окремо від проблеми сутності права та правового регулювання. З даного питання в правовій науці сформульовані протилежні точки зору.

Б. А. Кістяківський у науковому дослідженні «Філософія і соціологія права» зазначає, що думка одних вчених засноване на визначенні права як явища природного порядку, інша розглядає право як телеологічне явище, сутність якого визначає ціль (Р. фон Иеринг, Р. Штаммлер і ін.). Прихильники телеологічного концепції досліджували мета права як регулятор «всіх юридичних конструкцій». Р. фон Иеринг в своєму основному науковому трактаті «Ціль в праві» вказував, що «ціль є творець всього права», але визначав її не в праві, а поза правом. Р. Штаммлер, погоджуючись з телеологічним підходом до визначення сутності права, пропонував шукати мета не поза правом, а в самому право, причому «шукати ту ціль або, вірніше, ті цілі, які діють в праві і визначають саме його єство» [150, с. 391].

С. С. Алексєєв процес формування права (процес створення правової норми і процес правотворчості як завершальний етап формування права) розглядав окремо від процесу правового регулювання та, отже, не включав його в механізм. [151, с. 306].

Але, на наш погляд, те, що ціль, зазначена в диспозиції норми, норми-принципу, норми звичаєвого права є відбита в юридичних нормах частина

більш широкого поняття «юридична ціль», яка включає ціль в юридичній практиці, представляє суб'єктивні орієнтири конкретних учасників діяльності з реалізації права.

Т. І. Тарахоніч зазначає, що цілі права, поряд з цим і правового регулювання є ідеальним виразом об’єктивної закономірності, ідеальної сили, яка спонукає до певної поведінки людей [152, с. 29]. Постановка цілі правового регулювання складний процес, в результаті якого будується ідеальна правова модель, покликана зробити юридичне перетворення дійсності, зміну існуючих суспільних відносин. Існування та реалізація цілі можливі тільки в зв'язку із засобом. Саме в засобі реалізації ціль отримує визначеність і конкретність. Тому визначення специфічно правової цілі передбачає виявлення специфічного засобу реалізації.

М. В. Старинський, зазначає, що між цілями і засобами існує взаємозв’язок та своєрідна взаємодія. З одного боку, ціль визначає використовувані засоби. З іншого – засоби, впливаючи на досягнутий результат, визначають реалістичність чи утопічність цілей, коректують її основні параметри, в тому числі, це може відбуватись і до відмови від тих ідеалів, що виявились на сьогодні недосяжними. [153, с. 34].

У певному сенсі ціль правового регулювання визначається правовою політикою держави. Ю. О. Ващук вказує, що правова політика це системна публічна владна імперативна діяльність держави в сфері правового регулювання суспільних відносин, яка відповідає принципам права спирається за необхідності на державний примус і знаходить своє закріплення в формах об’єктивного (позитивного права [154, с.70]. Правова політика є комплекс ідей, заходів, завдань, цілей, програм, методів, установок, що реалізуються у сфері дії права і за допомогою права, будується з урахуванням міжнародних правових принципів і стандартів.

Правова політика реалізується за допомогою права, через його норми і використовує можливість досягнення цілей за допомогою застосування примусових заходів до осіб, які не враховує правову політику держави у

діяльності та порушують вимоги правових норм,.

На даний момент основні завдання правової політики у сфері інформаційної безпеки поки не реалізовані: відсутні деякі важливі нормативно-правові акти або, навпаки, окремі відносини занадто за регульовані. Це означає, що правова основа послідовного та визначального вибору, для побудови механізму правового регулювання, відповідної системи засобів стійкого розвитку демократії та інформаційного суспільства поки не сформована.

Перевагою правової політики є те, що в її формуванні та здійсненні прямо або побічно беруть участь всі зацікавлені суб'єкти. У процесі формування цілей і принципів різноманітні інтереси повинні бути виявлені в результаті діалогу та враховані за допомогою пошуку компромісних варіантів рішень. Крім того, правова політика нероздільна в часі, в просторі, по колу осіб, по суті.

Є. В. Курінний вказує, що забезпечення державної (правової) політики, яка фактично є тією консолідуючою категорією, що за певних умов може сприяти необхідній гармонізації відносин між людиною, суспільством та державою/ На користь пропонованої новації також виступає те, що переважна більшість суспільних відносин, що виникають під час формування нормативно-правового закріплення та реалізації державної політики, мають адміністративно-правову природу та регулюються за участю органів виконавчої влади, охоплюються усі різновиди публічно-владної діяльності, що мають адміністративно-правову регламентацію [155, с. 49].

Правова політика визначає ідеологію, ціль і принципи, які потім в процесі управління відповідними суспільними відносинами реалізуються в застосуванні правових і неправових, але здатних придбати правову форму, засобів, які необхідні для побудови механізму правового регулювання.

Сполучені в систему, послідовно реалізовані засоби стають елементами механізму правового регулювання, який веде до досягнення відповідного, поставленого ціллю, результату, тобто упорядкованих, що розвиваються в напрямі, визначеному правовою політикою, суспільних відносин.

Ціль в праві, офіційний орієнтир законодавця, відображена в юридичних

нормах, є частиною більш широкого поняття «юридична ціль», що включає також і мету в юридичній практиці, що представляє собою суб'єктивні орієнтири конкретних учасників діяльності з реалізації права.

Постановка цілі правового регулювання це складний процес, в результаті якого будується ідеальна правова модель, покликана зробити юридичні перетворення дійсності, зміни існуючих суспільних відносин. Існування та реалізація цілі можливі тільки в зв'язку із засобом.

Узагальнюючи викладене, зазначимо, що постановка мети правового регулювання це процес, результатом якого є побудова ідеальної правової моделі, що здійснює юридичні перетворення дійсності, зміну існуючих суспільних відносин.

В умовах ринкової економіки процес визначення цілі обумовлений різною направленістю інтересів суспільства, держави, суб'єктів підприємницької діяльності, інших суб'єктів інформаційних правовідносин, що в подальшому ускладнює структуру механізму правового регулювання.

Конфлікт інтересів важливо передбачити на стадії вироблення ідеальної правової моделі, щоб в подальшому включати правові засоби, необхідні для досягнення відповідного результату. Крім того, слід враховувати постійні зміни суміжних з регульованими відносин та передбачити побудова для них нових механізмів правового регулювання. Це, в свою чергу, створює передумови до зміни всієї системи правового регулювання відносин, які опосередковують досліджувані. В іншому випадку, при несвоєчасному реагуванні на зміни, що відбуваються, велика ймовірність отримати результат, протилежний цілі правового регулювання.

Під механізмом правового регулювання в літературі розуміється система правових засобів, підпорядкованих досягненню визначеної мети управління суспільними відносинами. Зазначений висновок повинен послужити основою для побудови механізму правового регулювання адміністративно-правового забезпечення інформаційної безпеки так, як О. В. Стукаленко пише, що механізм правового регулювання – це родова категорія, яка включає і категорію

механізм адміністративно-правового регулювання [145, с. 21].

Визначення цілі в інформаційній безпеці ускладнене різною направленістю інтересів держави, суб'єктів підприємницької діяльності та споживачів інформаційних послуг. У соціальних мережах протиріччя особливо очевидні та вимагають продуманого підходу до їх пом'якшення на стадії визначення цілі й вибору відповідних засобів.

Складність структури інформаційної системи країни та неконтрольована зовнішня інформаційна ситуація стимулюють державу до постійної зміни підходів регулювання, про що свідчить перехід до механізму проведення цілеспрямованої інформаційної політики, створення суб'єктами її проведення.

Таким чином, проблеми, що виникають на стадії визначення цілі, в подальшому ускладнюють структуру механізму правового регулювання, вимагають особливого підходу до вибору необхідних засобів.

Можливий конфлікт публічних і приватних інтересів важливо передбачити на стадії вироблення ідеальної правової моделі, для того щоб в подальшому нівелювати її включенням тих правових засобів, які необхідні для досягнення відповідного результату. В іншому випадку норми права не засвоюються та не переводяться в цілі та мотиви поведінки суб'єктів, а нормативні вимоги дотримуються лише зовні (формально), що уповільнює розвиток національних інформаційних ресурсів і негативно відбивається на всій інформаційній сфері суспільства.

При побудові механізму правового регулювання провідна роль належить цільовим суб'єкту. Правове регулювання як юридичне явище – це система дій та операцій, які здійснюються органами державної влади у встановлених процесуальних формах за допомогою певних методів та з використанням при цьому юридичних засобів, спрямованих на встановлення та реалізацію певних моделей суспільного розвитку [156, с. 22].

Механізму правового регулювання забезпечення інформаційної безпеки повинен визначати концептуальні підходи до правового регулювання та побудови механізму, і, отже, направляти учасників на досягнення результату.

Для цього суб'єкта, який визначає ціль, необхідно забезпечити можливістю «піднятися» над системою, зберегти його незалежність. Він зобов'язаний здійснювати постійний моніторинг стану внутрішнього взаємодії в керованій системі, вирішувати проблеми її зіткнення з іншими суміжними системами, ініціювати та враховувати зміни в правовому регулюванні.

Однак при дослідженні механізму правового регулювання забезпечення інформаційної безпеки, правових засобів, що використовуються в якості його елементів, особливостей їх взаємодії, методів регулювання, виникають сумніви в пріоритетності його публічно-правової природи. Участь спеціальних державних органів у відносинах пов'язаних з інформаційною безпекою за методом координації, а не субординації ефективно при стимулюванні ініціативи суб'єктів підприємницької діяльності. Це має визначальне значення щодо інформаційної безпеки об’єктів критичної інформаційної інфраструктури [66].

На підставі викладеного допустимо висновок, що під ціллю правового регулювання забезпечення інформаційної безпеки слід розуміти результат діяльності суб'єктів систем забезпечення інформаційної безпеки, який полягає в досягненні такого рівня їх взаємодії, який забезпечує дотримання всіх базових принципів в контексті прав людини в інформаційній сфері та кібербезпеки (у визначення даному у пункті 5 статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» [4]).

Досягнення цілі правового регулювання, який О. М. Куракін визначає, як це набір правових засобів, призначених для моделювання поведінки людей, опосередкованої юридичними категоріями (суб’єктивними правами та юридичними обов’язками),. повинно забезпечувати дотримання вимог безпеки та безперебійності роботи інформаційних систем, і захисту прав споживачів інформаційних послуг [157, с. 48].

Використання функціонального підходу до аналізу механізму правового регулювання забезпечення інформаційної безпеки дозволяє запропонувати систематизацію правових засобів, які є елементами даного правового

механізму. Правові засоби розділені на дві підсистеми: підсистема правових засобів створення системи інформаційної безпеки; підсистема правових засобів функціонування системи інформаційної безпеки.

В першу підсистему включені дві групи правових засобів: правові засоби створення систем інформаційної безпеки; засоби технічного супроводу, що набувають форми норм права.

У другу підсистему повинні бути включені дві групи правових засобів: правові засоби організації діяльності систем інформаційної безпеки; правові засоби, що забезпечують безперервність функціонування систем інформаційної безпеки.

Серед правових засобів механізму правового регулювання забезпечення інформаційної безпеки основна роль належить нормам права, закріпленим у законодавчих актах.

Світовий досвід свідчить про те, що успішній реалізації проектів з розвитку національних систем інформаційної безпеки сприяло створення правової бази, яка має наступні важливі характеристики. По-перше, це логічність, тобто відсутність взаємовиключних і суперечливих норм. По-друге, в них відображена перспективність, одночасно враховано накопичений досвід і передбачені можливі інновації. По-третє, відсутність дискримінації окремих учасників інформаційних відносин, виваженість, пропорційність проблем, які можуть виникнути в разі відсутності регулювання.

Крім норм права, серед яких значне місце належить нормам, виробленим державою, до числа засобів нормативного характеру слід віднести також принципи правового регулювання, різні норми саморегулювання, розроблені громадськими, науковими і виробничими об'єднаннями, міжнародними організаціями, норми «м'якого» права, які надають саме серйозний вплив на законотворчу діяльність в інформаційній сфері.

З урахуванням зазначених особливостей правового регулювання забезпечення інформаційної безпеки допустимо представити наступну сукупність елементів механізму правового регулювання:

- засоби нормативного характеру, що включають норми права, що містяться в законодавстві, норми-принципи, норми «м'якого права», норми саморегулювання власників інформаційних систем, звичаї, правила безпеки систем;

- акти індивідуальної регулювання (інструкції, правила, договори, судові рішення у спорах, що виникають із інформаційних правовідносин);

- юридичні факти як підстави виникнення інформаційних захисних правовідносин;

- правовідносини, що виникають в інформаційній сфері пов'язаної з критичної інформаційною інфраструктурою.

Дослідження зазначених елементів механізму правового регулювання інформаційної безпеки неможливо без аналізу економічної основи регулювання суспільних відносин в інформаційній сфері. Практично всі засоби правового регулювання в інформаційній сфері та в інформаційній безпеці за базисом – економічні, лише придбавши правову форму, вони стають елементами механізму правового регулювання.

Складна система взаємовідносин суб'єктів, вільних в прояві підприємливості та ініціативи, не повинна бути порушена, тому що побудована вона на основі принципів, які відповідають потребам розвитку інформаційного суспільства та інформаційному обігу в інформаційній економіці і інформаційному суспільстві [158].

Отже, при побудові механізму правового регулювання забезпечення інформаційної безпеки перед законодавцем постало складне завдання органічно поєднати публічну ціль забезпечення ефективного, безперебійного та безпечного функціонування інформаційних систем і приватноправові засоби стимулювання розвитку. Така комбінація цілей і принципів виникає в приватній інформаційній системі, де основними функціями держави є спостереження, а в разі виявлення збоїв – стимулююча або стримуюча участь. Все це свідчить про побудову механізму правового регулювання відносин, що виникають в контексті забезпечення інформаційної безпеки в інформаційній сфері, з

використанням приватноправових засобів. Приватноправовий характер механізму правового регулювання інформаційної безпеки безпосередньо пов'язаний з особливостями норм інформаційного права, однак на практиці це проявляється в абстрактній статичній сукупності правил поведінки. У свою чергу, правовий механізм інформаційної безпеки є спосіб перетворення норм адміністративного права в конкретні правовідносини, є його динамічною складовою критерієм ефективності що вимагає, як вважає голова комітету спілки адвокатів України О. М. Вольвак, забезпечення реалізації положень Декларації про державний суверенітет України та Конституції України в контексті реалізації принципу гуманізму [159, с. 25].

Щодо приватноправового характеру механізму правового регулювання забезпечення інформаційної безпеки, то припущення зроблено на основі аналізу чинного законодавства та інших правових актів, що регулюють функціонування системи забезпечення інформаційної безпеки в Україні, зокрема, Законів України «Про національну безпеку», «Про основні засади забезпечення кібербезпеки України», Стратегії національної безпеки України, Стратегії кібербезпеки України, Доктрини інформаційної безпеки України і інші та поглядів О. В. Кохановської на приватноправове розуміння інформаційних відносин в Україні [4; 19; 36; 62; 72; 160].

Доцільно відзначити, що підхід до вказаної проблеми є дискусійним, але в контексті забезпечення інформаційної безпеки, поки що не знайшов відображення у науковій літературі.

Реалізація цілі правового регулювання інформаційної безпеки може бути досягнута тільки шляхом дотримання всіх базових принципів інформаційного права. Досягнення зазначених принципів має з'єднати різноспрямовані інтереси всіх учасників інформаційних відносин, зібрати відповідно до поставленої цілі правові засоби, що сприяють її досягненню, для того щоб побудувати ефективний механізм правового регулювання забезпечення інформаційної безпеки.

І. Д. Ваньчук пише, що для забезпечення стабільності системи правового

регулювання необхідно забезпечити здійснення її функціонування відповідно до чітко визначених принципів правового регулювання [161, с. 10].

Принципи інформаційного права повинні забезпечувати гармонійну взаємодію різних суб'єктів: власників інформаційних ресурсів і інформаційних систем, держави та споживачів інформаційних послуг, (за висловом Я. О. Лазора, інформаційна система – це організований комплекс організаційно-технічних заходів (сукупність підприємств, підрозділів і фахівців), а також безпосередньо інформаційних технологій і інформаційних ресурсів, призначених для забезпечення функціонування інформаційних процесів, зокрема забезпечення створення, поширення, використання, систематизації, збереження і знищення інформації [162].)

Однак для правильного формування цілі правового регулювання та адекватного вибору конкретних правових засобів необхідні принципи іншого роду. Назвемо їх принципами побудови механізму забезпечення інформаційної безпеки.

Дані принципи грають роль орієнтирів для вирішення конкретних практичних завдань правового регулювання забезпечення інформаційної безпеки, наприклад, для підготовки проектів нормативно-правових актів в галузі інформаційної безпеки. Вони повинні правильно формувати структуру правового механізму забезпечення інформаційної безпеки та зміст кожного елемента правового засобу, що входить в нього.

В основі системи принципів правового механізму забезпечення інформаційної безпеки повинні лежати базові права людини, що мають загальну природу та з'єднують воєдино всі інтереси учасників інформаційних відносин. Вони повинні служити засобами досягнення цілі правового регулювання, яка знаходить загальне вираження в принципах інформаційного права.

Принципи правового механізму забезпечення інформаційної безпеки покликані впорядкувати і оптимізувати застосуванні технічних засобів, тобто це принципи, які повинні забезпечити баланс інтересів власників

інформаційних систем, їх користувачів і держави. До числа базових принципів правового механізму забезпечення інформаційної безпеки, на нашу думку, відносяться: принцип економічної ефективності; принцип використання правових засобів відповідно до мети правового регулювання; принцип пріоритетного використання приватноправових засобів; принцип використання публічно-правових засобів виключно для цілей управління інформаційними системами в умовах хакерських атак і інших реальних загроз. М. В. Вейтас і М. І. Лукашенко вказують, що незважаючи на позитивні зрушення у сфері законодавчої роботи над проблемою кібертероризму, вітчизняне законодавство потребує активного удосконалення та подальшого забезпечення механізмів результативної реалізації розроблених положень [163, с. 12]

Принципи формування механізму правового регулювання забезпечення інформаційної безпеки не тотожні принципам інформаційного права. Вони є засобом досягнення цілі правового регулювання забезпечення інформаційної безпеки, а принципи інформаційного права є зовнішнім виразом мети правового регулювання.

Відповідно до зазначених вище принципів повинні бути розроблені нормативні та інші правові акти, документи реалізації права, що опосередковують техніко-технологічну сферу та мають забезпечити реалізацію цілі правового регулювання забезпечення інформаційної безпеки у контексті технологічного напряму дослідження інформаційної безпеки.

Розумні вимоги до авторизації постачальників інформаційних послуг, які передбачають створення засобів, що повинні включати умови про обов'язкову присутність юридичних або фізичних осіб в якості керуючого та відповідального не повинні ускладнювати структуру інформаційної систем, необґрунтовано збільшуючи витрати на забезпечення інформаційної безпеки. Вимоги повинні бути встановлені щодо регулювання відповідальності, розподілу функцій і відповідальності (виключаючи її «розмивання») в процесі інформаційної діяльності, в тому числі між власниками інформаційних систем і споживачами.

Важливим завданням названих принципів є створення умов і вимог до розвитку технічної інфраструктури та програмних засобів забезпечення їх вільного використання власниками інформаційних систем. Вони повинні сприяти підвищенню технічної безпеки, а в разі збоїв та інших порушень, застосування відповідальності, що дозволяє розумно розподілити збитки, у тому числі відповідальності організаторів технічної інфраструктури. Особливо слід відзначити важливість умов і вимог, що дозволяють втілити принципи інформаційного права, зокрема принципу безперервності та забезпечення інформаційної безпеки в режимі реального часу.

Відсутність закріплених принципів, вимог та умов, сформованих в результаті дослідження інтересів всіх учасників інформаційних відносин, аналізу зарубіжного досвіду та Доктрини інформаційної безпеки України, може негативно вплинути в кінцевому підсумку на розвиток правовідносин у сфері забезпечення інформаційної безпеки, і на процес формування правозастосовної практики.

Навпаки, наявність принципів побудови правового механізму забезпечення інформаційної безпеки дозволило б гармонізувати захисні правовідносини, знайти правильний напрям удосконалення регулювання забезпечення інформаційної безпеки в мінливій глобальній ситуації та в умовах інформаційної агресії Російської Федерації, в результаті побудувати ефективний і універсальний правовий механізм.

Р. І. Благута розглядаючи значення ефективного механізму правового регулювання для розвитку правової держави вказує, що доводиться констатувати, що великою проблемою є відсутність системних науково обґрунтованих методик оцінки ефективності механізму правового регулювання, підвищення якості його компонентів і внутрішніх зв’язків. Окремо слід наголосити на необхідності установлення переліку необхідних умов досягнення ефективного механізму правового регулювання [164, с. 5].

Підводячи підсумок вищевикладеного у контексті дослідження поняття та принципів побудови механізму правового регулювання забезпечення

інформаційної безпеки можна зробити такі висновки.

Конструювання механізму правового регулювання інформаційної безпеки має здійснюватися відповідно до цілі правового регулювання. Мета правового регулювання, будучи частиною управлінського процесу та результатом правової політики в даній сфері, передбачає об'єднання відповідних правових засобів для досягнення необхідного правового результату, визначаючи при цьому вибір засобів і природу механізму.

Ціль правового регулювання інформаційної безпеки залежить від правової політики держави в інформаційній сфері. Вона визначається суб'єктами, що здійснюють нормативно-правове регулювання інформаційної безпеки з урахуванням свободи розсуду та розвитку приватної ініціативи юридичних і фізичних осіб власників інформаційних систем.

Вирішальну роль у формуванні цілі національного правового регулювання забезпечення інформаційної безпеки, що мають транснаціональний характер, грають цілі, передбачені в актах міжнародних та наднаціональних організацій, в тому числі Європейського Союзу і Організації Північноатлантичного договору – НАТО (англ. North Atlantic Treaty Organization – NATO). Мета правового регулювання, поставлена відповідно до принципів розвитку інформаційного суспільства, для досягнення необхідного результату вимагає органічного поєднання публічно-правових та приватноправових засобів в структурі механізму правового регулювання. Це дозволить врахувати підприємницький характер інформаційної діяльності та інформаційної безпеки.

Державні інформаційні системи взаємодіють з інформаційними системами інститутів громадянського суспільства, що також мають свої цілі, принципи та механізми правового регулювання, на основі системи засобів, переважно приватноправового характеру. Ефективність взаємодії всіх систем залежить від високого ступеня уніфікації правового регулювання і побудови механізмів з використанням подібних правових засобів. Таким чином, можна припустити, що всі взаємодіючі інформаційні системи функціонують за

допомогою механізмів правового регулювання, що мають однакову структуру і комплексну об'єднану публічно-правову і приватноправову природу.

Специфіка адміністративно-правового методу регулювання відносин у сфері забезпечення інформаційної безпеки в механізмі їх правового забезпечення, спрямованого на реалізацію публічних інтересів в забезпеченні інформаційної безпеки, представляє застосування владного впливу з боку уповноважених суб'єктів держави на поведінку та волю суб'єктів, що базується на імперативній основі, в поєднанні із засобами приватноправового характеру.

Елементами механізму правового регулювання забезпечення інформаційної безпеки є: засоби нормативного характеру, що включають норми права, що містяться в законодавстві, норми-принципи, норми «м'якого права», норми саморегулювання власників інформаційних систем, звичаї, правила інформаційної безпеки інформаційних систем; етичні кодекси та правила: юридичні факти як підстави виникнення інформаційних правовідносин в сфері інформаційної безпеки; правовідносини, що виникають в системах забезпечення інформаційної безпеки (зобов'язальні, контрольні, наглядові та корпоративні правовідносини); акти застосування і реалізації права (в тому числі судові рішення).

Система принципів адміністративно-правового регулювання діяльності щодо забезпечення інформаційної безпеки, заснована на конституційних принципах суспільно-економічного устрою держави, виходячи з яких, вироблені і розкриті загально принципи діяльності: пріоритет центрального рівня регулювання, єдність і цілісність організаційно-правового регулювання, публічність і стимулюючий вплив діяльності щодо забезпечення інформаційної безпеки. Принципи інформаційного права та принципи побудови правового механізму забезпечення інформаційної безпеки співвідносяться як ціль та засіб її досягнення. До числа базових принципів побудови правового механізму забезпечення інформаційної безпеки відносяться: принцип економічної ефективності; принцип використання правових засобів відповідно до мети правового регулювання; принцип пріоритетного використання

приватноправових засобів; принцип використання публічно-правових засобів виключно для цілей антикризового управління інформаційними системами.

2.2 Адміністративно-правове регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки

Сьогодні стратегічне управління державою є фундаментальна умова забезпечення інформаційної безпеки, яка є важливою характеристикою життєздатності країни. Очевидним є ефект правової взаємопов'язаності в адміністративних відносинах в межах міждержавних об'єднань Європейського союзу, Світової організації торгівлі (англ. World Trade Organization, WTO), Організації Північноатлантичного союзу (НАТО) і ін.

С. М. Подзігун зазначає, що доцільно погодитися з науковцем в тому, що стратегічне управління дає змогу досягти таких основних результатів: створити системний потенціал для досягнення цілей; сформувати оптимальну структуру, яка уможливить забезпечення чутливості до змін зовнішнього середовища та відповідну адаптацію [165, с. 413].

Стратегічне управління інформаційною безпекою передбачає: визначення принципів, формування структури, розробку вимог до аналізу та концепції стратегічного управління; проведення стратегічного аналізу (аудиту) стану інформаційної безпеки з використанням сучасних підходів і аналітичних технологій; формування сприятливих умов реалізації Доктрини інформаційної безпеки України та Стратегії кібербезпеки України, проведення моніторингу конкретних досягнутих результатів; вдосконалення методів і методології розробки нормативно-правових актів, у тому числі відомчих з врахуванням особливостей національної інформаційної інфраструктури при підготовці управлінських рішень.

Як зазначає С. Л. Гнатюк, все це робить даний сегмент правового регулювання й державного управління на перетині двох важливих проблематик

однією з чутливих зон, де проблеми формування та реалізації державної політика легко можуть спричинити виникнення суттєвих дисбалансів у розвитку країни, включаючи значне зростання корупційних ризиків [64, с. 16].

Слід погодитися з думкою О. І. Яременко про те, що у сучасних умовах інформаційна сфера набула стратегічного значення, що активізувало процеси її державного управління. Специфічна природа та структура інформаційної сфери, в основі якої є інформація в процесі обігу в суспільстві і державі, обумовлює високий рівень її складності як об’єкта державного управління. Одним з ефективних заходів у цьому напрямі є вдосконалення системи органів державного управління інформаційною сферою [166, с. 15].

Для того, щоб проаналізувати специфіку інформаційної безпеки як об'єкта адміністративно-правового регулювання, необхідно визначитися із співвідношенням понять «державне управління» та «державне регулювання».

Цілі державного регулювання та державного управління завжди змінюються адекватно цілям держави. Одночасно змінюються засоби досягнення, за допомогою яких можливе підвищення соціальної цінності та дієвості правових інститутів. При визначенні стратегічних цілей правового регулювання необхідно виходити з того, що такі повинні відображати місце та роль правового регулювання в системі соціального регулювання; враховувати можливості правового регулювання та спиратися на вимоги, що пред'являються до правового регулювання. Державне регулювання зводиться до того, щоб створити та забезпечити достатні умови для успішного функціонування суспільства та державної адміністрації. Ефективність державного управління залежить, в першу чергу, від відповідності його структури функцій заданим державним регулюванням. Результативність державного втручання істотною мірою залежить від того, хто, коли та в який спосіб застосовує ті чи інші методи державного регулювання [167, с. 2].

Державне управління необхідно при реалізації державних функцій; важливо лише правильно визначити міру цього державного управління в системі правового регулювання.

В. Б. Авер’янов зазначає, що за характером вплив на об'єкти управління з метою досягнення певних результатів, тобто реалізації встановлених цілей та завдань управлінського впливу. При цьому регулювання охоплює порівняно з управлінням ширшу сферу організаційної діяльності. Управління означає цілеспрямований вплив саме на об'єкти управління, використання методів, що передбачають підпорядкування цих об'єктів управлінському впливу з боку суб'єкта управління. Регулювання ж пов'язане не стільки з впливом на об'єкти управління, скільки на оточуюче середовище. Воно передбачає високий ступінь альтернативності поведінки керованих об'єктів [168, с. 65].

Державне регулювання це встановлення та забезпечення державою загальних правил поведінки суб'єктів суспільних відносин і коригування їх в залежності від зміни умов. Державне управління, за своєю сутністю, є організуючий і регулюючий вплив держави на поведінку суб'єктів суспільних відносин. Державне управління дуже складне, багатогранне суспільне явище, характер, можливості та дія якого визначаються людьми.

В. Б. Авер’янов вважає, що держава залишається важливим фактором суспільного розвитку, на неї падає основний обсяг справ з управління.

Сутність державного управління В. В. Грохольский розглядає з позицій взаємозв'язку понять «держава» і «управління». Сутність державного управління проявляється, перш за все, через таку атрибутивну ознаку, як вплив органів держави на суспільні відносини та зв'язки. Державне управління за сутністю є соціальним і охоплює усі сфери соціального життя, здійснюється системою спеціально визначених органів державної влади і управління, які наділені певними владними повноваженнями, їх рішення є обов’язковими для виконання як у добровільному так і примусовому порядку [169, с. 31].

Цю ж точку зору поділяв Ю. О. Куц, який писав, що «державне управління» як дефініція – це управління, що здійснюється в загальнодержавному масштабі спеціальним суб’єктом – органами державної влади. Таке управління, будучи механізмом реалізації державної влади, і є власне процесом реалізації політичної влади. У цьому аспекті простежується

певне співвідношення влади й управління [170, с. 8]. Управління, в тому числі державне, доцільно розуміти, як цілеспрямований вплив, що спирається на пізнання об'єктивних закономірностей керуючої системи для оптимального досягнення поставлених цілей, це цілеспрямований вплив держави, її органів на суспільну систему в цілому або на окремі сфери на основі пізнання та використання властивих суспільству об'єктивних закономірностей розвитку.

Дослідники державного управління з точки зору «діяльності» мають на увазі та концентрують увагу тільки на суб'єкті управління, при цьому з поля зору значною мірою йдуть керовані об'єкти. Прихильники другого підходу, коли мова про державне управління йде як про «вплив», при дослідженні суті явища більше концентруються на самому об'єкті управлінського впливу.

При визначенні оцінки державного регулювання, співвіднесенні його змісту з фактичним рівнем розвитку держави та суспільства необхідно оцінювати: комплексний характер регулювання; циклічний характер регулювання як процес формування цілей, концепцій, прогнозів, моделей, форм правового впливу; багаторівневий характер регулювання, включаючи міжнародні та національні регулятори; принципи регулювання випереджаючого «відображення», варіативності, реалізації цілей в нових правових станах; типологію регулюючих режимів. Лише при дотриманні цих умов можна говорити про формування теорії правового регулювання.

Вивчення правового регулювання будь-якого соціального процесу має важливе практичне та теоретичне значення, що дозволяє визначитися зі змістом даного явища. Необхідно відзначити, що в науці теорії держави та права немає єдиної думки з питання визначення поняття «правове регулювання».

Наприклад, В. М. Соловйов вказує, що сутністю правого регулювання державного управління є нормативне закріплення доцільних правил поведінки [171, с. 32] правове регулювання є механізм, який зводився до того, щоб визначити коло суспільних відносин, що підлягає врегулюванню нормами права, вибрати тип, метод, спосіб регламентації зазначених відносин.

В. Б. Авер'янов, В. Н. Денисов, О. В. Зайчук, В. П. Нагребельний,

О. М. Костенко, І. О. Кресіна, В. Ф. Погорілко, Н. М. Пархоменко, В. Ф. Сіренко, В. І. Семчик, І. Б. Усенко, В. В. Цветков, Я. М. Шевченко, Ю. С. Шемшученко вважають, що існує два підходи до визначення державного управління: в широкому і вузькому значеннях. У широкому значенні державне управління являє собою регулюючу діяльність держави в цілому (діяльність представницьких органів влади, виконавчих органів державної влади, прокуратури, судів тощо). У вузькому розумінні державне управління є, перш за все, адміністративною діяльністю, тобто діяльністю виконавчих органів державної влади на центральному та на регіональному рівнях [166, с.. 56].

Державне управління забезпеченням інформаційної безпекою в широкому сенсі це різновид соціального управління, здійснюваного шляхом цілеспрямованого, організуючого та розпорядчого впливу держави на сферу інформаційної безпеки з метою стійкого розвитку інформаційної сфери. Державне управління забезпеченням інформаційної безпекою в широкому розумінні являє собою регулюючу діяльність у зазначеній сфері органів публічної влади, прокуратури, судів державних і місцевих органів і інших суб'єктів забезпечення інформаційної безпеки.

В. Р. Котковський зазначає, що більшість обов’язків розподілена між різними рівнями публічного управління, співпраця потрібна на різних етапах виконання функцій місцевими та центральними органами влади [172, с. 14].

Як зазначають О. П. Дзьобань, Є. М. Мануйлов, що інформаційна безпека – одна з гострих соціокультурних проблем сучасного суспільства, яка має системний характер і торкається діяльності основних інститутів і підсистем; у контекст її впливу потрапляють ключові соціокультурні процеси, що відбуваються в суспільстві [173, с. 79-80].

У межах дослідження державного управління та регулювання забезпеченням інформаційної безпеки, не можна не згадати адміністративно-правові моделі управління. У науковій літературі не так багато досліджень, присвячених аналізу зміни адміністративно-правових моделей управління, в основному в роботах вказується на дві основні моделі адміністративного права,

які різняться між собою з точки зору принципів правового регулювання, вимог до змісту правового регулювання, меж судового контролю діяльності державної адміністрації.

Узагальнюючи дослідження Фред С. Луненбурга та Беверлі Дж. Ірбі «Розвиток адміністративної думки: історичний огляд» (Fred C. Lunenburg, Beverly J. Irby) Development of Administrative Thought: A Historical Overview) доцільно відзначити дві моделі [174].

Перша модель – закрита характерна для держав авторитарного політичного режиму, зокрема, ознаки цієї моделі є в адміністративному праві Російської Федерації (відсутність адміністративного суду). Основний акцент робиться на керованості системи державної адміністрації, забезпечення виконання прийнятих управлінських рішень, незалежно від змісту цих рішень. Діяльність органів виконавчої влади регулюється виключно шляхом формального закріплення повноважень. Зміст діяльності залишається поза досяжністю правового регулювання. Ціль реалізації владних повноважень, визначається політичною владою, залишається поза межами судового контролю державною адміністрацією. Ця адміністративно-правова модель має риси: державне управління розглядається як інструмент для досягнення цілей управління, в той час як цілі управління визначаються правлячою партією або елітою, а не інтересами суспільного блага і без урахування прав громадян; форми звітності та контролю існують, але використовуються в основному для того, щоб переконатися, що управління дійсно направлено на цілі, визначені правлячою партією. Це внутрішній контроль адміністрування і управління при мінімальному або відсутньому контролі зовнішніх органів.

У контексті досліджень німецького вченого Е. Шмідт-Ассманн, друга модель адміністративно-правового управління є відкритою. Така модель характерна для демократичних держав, наприклад, країн Європейського Союзу [68]. Для моделі ефективність державного управління не представляє абсолютну цінність. Адміністративне право прагне встановити змістовні вимоги обґрунтованості реалізації владних повноважень державної

адміністрації. Цілі та завдання діяльності державної адміністрації закріплені нормативно та дозволяють виробляти правову, в першу чергу судову оцінку діяльності. Будь-який випадок реалізації владних повноважень може стати предметом судового аналізу на предмет того, чи були дії посадових осіб необхідними в конкретних умовах, чи обґрунтовані вони фактичною ситуацією. Наявність формальних примусових повноважень недостатня для оцінки правомірності фактично здійсненого примусу – повинна бути доведена його реальна обґрунтованість. У відкритій адміністративно-правовій моделі управління: державне управління в значній мірі спрямована на досягнення цілей правління, але з двома виразними рисами: цілі правління засновані на уявленнях про суспільне благо, визначеному через демократичні процедури; досягнення цілей правління коригується певними цінностями та принципами. Ці принципи, які виражені в ідеях транспарентності, законності, відкритості, прозорості, підзвітності, поваги до громадян, є стримуючі обмежувачі при досягненні цілей правління. Дана модель характеризується системою контролю адміністрування, здійснюваної інститутами громадянського суспільства допомогою методів, які відокремлені незалежні від влади.

Замість ситуації, при якій виконавча влада була центральною точкою управління, вона залишається однією з центральних точок, але не єдиною. Виконавча влада і адміністрація грають ключову роль в забезпеченні ефективного правління, але це не безмежна і нічим не стримувана роль. У інших державно-владних і самоврядних інститутів і механізмів є свої власні функції, при виконанні яких вони не підзвітні виконавчої влади. Права матеріального та процесуального характеру охороняються мережею процедур і інститутів, таких як адміністративно-процесуальний кодекс, суди, інститут уповноваженого з прав людини. Процедури та доктрини даної моделі приймають інший характер і служать цілям, відмінним від цілей закритої моделі. У відкритої моделі доктрини і процедури пов'язані з забезпеченням і підтримкою упорядкованого та системного адміністрування.

Модель адміністративно-правового регулювання забезпечення

інформаційної безпеки України вписується у відкриту модель, усталену в науці, так як має на меті захист, перш за все, інформаційних інтересів держави, суспільства і особи де особливо помітний вплив інтегральних політико-економічних, соціально-культурних і науково-технічних факторів, які проявляють себе у вигляді певних тенденцій [175, с. 151].

В. О. Криволапчук вказує, що одним із підтверджень суттєвої зміни правового становища сторін адміністративно-правових відносин у результаті трансформації методу адміністративного права є модель правового регулювання спрямована на подальшу демократизацію взаємовідносин між державою та людиною на засадах непорушності її природних та інших основних прав і свобод [176, с. 190-191].

Загальною ознакою відкритої моделі, у контексті інформаційної безпеки, щодо застосування адміністративних заходів є встановлення адміністративно-правового режиму інформаційної безпеки, що має свою специфіку, яка відображає динаміки державного управління в умовах глобалізації та інформатизації держави. За словами Ю. В. Нестеряк: «Основними напрямами реалізації державної інформаційної політики слід визначити: створення політико-правових, економічних, організаційних та матеріально-технічних умов для формування сучасної моделі інформаційної політики; підвищення ефективності використання всіх видів інформаційних ресурсів і управління елементами інформаційно-комунікаційної інфраструктури; державну підтримку виробництва і поширення вітчизняної інформаційної продукції; забезпечення розвитку і захисту вітчизняної інформаційної сфери на підставі пріоритету прав і свобод людини та громадянина, її потреб та інтересів» [177, с. 70].

Наука адміністративного права Європейського Союзу розробляє питання організації та функціонування виконавчої влади, бачачи в ній ядро механізму державного управління, що супроводжується масштабним вивченням інструментів і засобів управління з метою проведення адміністративних реформи, спрямованих на подолання корупції, децентралізацію і аутсорсинг.

З погляду на дослідження вчених К. І. Бєлякова, І. М. Дороніна,

І. Б. Жиляєва, А. І. Семенченка, А. В. Тарасюка Т. Ю. .Ткачука, В. М. Фурашева, державне регулювання інформаційної безпеки, на нашу думку, охоплює: загальне нормативне регулювання інформаційної сфери ат інформаційної безпеки; програмно-установчі способи регулювання інформаційної безпеки (цільові програми); засоби регулювання у сфері інформаційної безпеки (ліцензування, сертифікація, акредитація); нормативно-кількісні і якісні засоби регулювання у сфері техніко-технологічної складової інформаційної безпеки (квоти, стандарти, ціни); засоби підтримки та стимулювання діяльності господарюючих суб'єктів у сфері інформаційної безпеки (дотації, кредити, пільги); контрольні та наглядові методи регулювання інформаційної безпеки (облік, перевірки, санкції) [178-182]. Державне регулювання інформаційної безпеки доцільно класифікувати за формою на інформаційне, правове та організаційне.

Крім нормативної форми адміністративно-правового регулювання інформаційної безпеки, дана діяльність здійснюється у вигляді індивідуальних, тобто персоніфікованих, адміністративно-правових актів. Серед індивідуальних правових актів, що регулюють діяльність господарських суб'єктів, ми можемо назвати класичні для адміністративного права акти, що містять конкретні приписи та заборони щодо певної особи (наприклад, накладення штрафу), та и диспозитивні форми правового регулювання (наприклад, укладання органом влади договору з фізичною або юридичною особою). Дані акти приймаються на центральному рівні та на місцевому рівні органів влади і мають яскраво виражену правозастосовну природу. Характерним прикладом таких актів на центральному та на місцевому рівні є акти, що стосуються створення, реорганізації та припинення дії конкретних підприємств з надання послуг з інформаційної безпеки, хоча коректніше їх було би віднести до актів змішаного (нормативно-індивідуального) характеру. Як приклад правозастосовного акту в сфері інформаційної безпеки можна назвати статут Державного підприємства «Державний центр інформаційної безпеки» Державної служби спеціального зв'язку та захисту інформації України [183].

На думку С. С. Єсімова та С. Я. Мельник, інформаційна сфера є системою, яка охоплює: інформацію, інформаційну інфраструктуру, суб'єкти, що здійснюють збір, формування, поширення та використання інформації, а також сукупність норм, котрі регулюють суспільні відносини, які виникають. Через зростання ролі інформації виникає необхідність більш чіткого виокремлення інформаційної функції держави [184, с. 171].

У процесі виконання регулятивної функції в сфері інформаційної безпеки адміністративне право взяло на озброєння не властиві інструменти, запозичені здебільшого з цивільного права. У сучасному світі, де інформаційні відносини складні та диверсифіковані, державі доводиться з різних причин вдаватися до більш м'яких форм регулювання інформаційної діяльності, властивим цивільно-правовим формам регулювання. Мова в першу чергу йде про різні інструменти правового регулювання, які характеризуються такими методами, як узгодження, стимулювання та переконання. Невластивою для адміністративного права формою є договірна форма правового регулювання, застосування якої зустрічається в межах державно-приватного партнерства. Як наслідок, в адміністративному праві застосовуються не тільки властиві інструменти вертикального регулювання приписів і заборон, але й форми цивільно-правового, або горизонтального регулювання, яким притаманні такі принципи, як узгодження волі та рівність сторін.

Сучасному адміністративному праву властиві нехарактерні принципи, як «рівні засади з учасниками відносин» і «взаємовигідна співпраця» державної влади і господарюючих суб'єктів приватного сектора щодо інформаційної безпеки. Іншим відступом від принципів вертикального регулювання відносин за допомогою приписів і заборон, яким характеризується адміністративно-правове регулювання інформаційної безпеки та забезпечення інформаційної безпеки, є державна (фінансова або матеріальна) підтримка господарюючих суб'єктів приватного сектора економіки, що передбачено Планом заходів на 2018 рік з реалізації Стратегії кібербезпеки України [185]

Варто звернути увагу на суто інформаційні методи адміністративно-

правового регулювання, які, як всі попередні види методів регулювання інформаційної безпеки, відступають від класичних канонів адміністративного права. Тут мова не йде про встановлення приписів суб'єкту адміністративно-правового регулювання, а, скоріше, про управління його діями за допомогою його власної зацікавленості, яка найчастіше полягає в матеріальній вигоді. Такі засоби впливу на суспільні відносини в сфері інформаційної діяльності також сьогодні досить часто застосовуються в адміністративному праві. Серед них: надання пільг; надання матеріальних заохочень; звільнення від будь-яких зобов'язань тощо. В межах різних програм підтримки підприємництва мова не йде про створення будь-яких розпоряджень для господарюючих суб'єктів, а, навпаки, про узгодження позицій щодо концептуального бачення системи аудиту інформаційної безпеки; про пільги, преференції, заходи з підтримки, стимулювання тощо [64, с. 17].

Виділення економічних форм адміністративно-правового регулювання має особливий інтерес так як вони мають першорядне значення при регулюванні забезпечення інформаційної безпеки господарюючих суб'єктів. Державна підтримка є ще одним видом інформаційної форми адміністративно-правового регулювання інформаційної безпеки.

Державна підтримка підприємницької діяльності є специфічною формою державного регулювання інформаційної безпеки і може здійснюватися, в свою чергу, за допомогою правових, економічних та організаційних форм. За словами Я. В. Петрушка, державна підтримка суб’єктів господарювання може виявитися досить ефективним засобом регулювання економіки, однак така ефективність досягається лише за наявності певних організаційних та правових умов, які наразі в Україні не сформовані належним чином, хоча варто вказати на певну позитивну тенденцію, що намітилась у цій сфері протягом останніх декількох років [186, с. 111].

Державна підтримка підприємницької діяльності у сфері забезпечення інформаційної безпеки не відрізняється значними особливостями, що дозволяють виділити в окрему економічну форму адміністративно-правового

регулювання. На відміну від інших форм державного регулювання, за допомогою яких встановлюються певні рамки діяльності господарюючих суб'єктів, державна підтримка спрямована на розширення можливостей цих господарюючих суб'єктів і виражається в матеріальній (фінансовій) формі.

Незважаючи на багатоликість форм і видів державної підтримки, слід зупинитися саме на видах підтримки, які отримують фінансове вираження в грошовому еквіваленті. Серед них: інвестиції, субсидії, бюджетне та податкове кредитування, податкові пільги. Такі форми адміністративно-правового регулювання припускають покладання додаткових фінансових зобов'язань на державний і місцеві бюджети, що передбачено Доктриною інформаційної безпеки України та Стратегії кібербезпеки України.

Матеріальна державна допомога, інші види підтримки господарюючих суб'єктів, що мають фінансове вираження (пільги, субсидії, інвестиції тощо), мають певну специфіку, яка полягає в необхідності брати до уваги пріоритет дотримання бюджетного балансу, характерна для всіх заходів, які можемо віднести до економічного виду адміністративно-правового регулювання.

Державна підтримка, поряд з іншими заходами адміністративно-правового регулювання інформаційної безпеки, може бути виділена в окрему економічну форму адміністративно-правового регулювання, яка характеризується особливостями об'єкта керуючого впливу в залежності від форми власності (державні, кооперативні, акціонерні, комерційні, колективні, приватні, індивідуальні об'єкти) дає найбільшу кількість видів форм адміністративно-правового регулювання.

Водночас, актуальною є класифікація форм адміністративно-правового регулювання направлених на досягнення певного результату адміністративно-правового регулювання. У даному випадку доцільно виділити позитивне регулювання затвердження програм і інше), або реакцію на негативні явища в сфері державного управління. Як приклад, завдяки модернізації профільного законодавства (Закон України «Про стандартизацію»), а також осучасненню й демократизації інститутів та процедур стандартизації для пересічних об’єктів

кіберзахисту ситуація в цій галузі загалом розвивається в оптимальному напрямку – база стандартизації інформаційної безпеки стає в Україні дедалі більш сучасною та диверсифікованою [64, с. 15]. Це дозволяє виділити особливості адміністративно-правового регулювання в сфері інформаційної безпеки, в зв'язку з негативними явищами, що відбуваються в інформаційній сфері внаслідок агресії Росії в Донецькій і Луганський областях [187; 188].

Сьогодні кількість актів, спрямованих на коригування негативного впливу в інформаційному середовищі, значно зросла, що робить цю класифікацію форм адміністративно-правового регулювання особливо актуальною на даний момент. Більш того, до даної форми адміністративно-правового регулювання можна віднести правові акти, які не виділяються в межах класичних класифікацій форм адміністративно-правового регулювання (наприклад, рекомендаційні акти індикативного планування та прогнозування – аналітичні доповіді Національного інституту стратегічних досліджень при Президенті України). Особливості сфери інформаційних відносин вимагають виділення альтернативних класифікацій форм адміністративно-правового регулювання інформаційної безпеки, тобто відходу від класичного розподілу форм на правові та не правові або організаційні та матеріально-технічні.

Адміністративно-правове регулювання забезпечення інформаційної безпеки в кожному часовому проміжку має підкорятися певним стратегічним планом на основі принципів методів, функцій і форм адміністративно-правової науки та з урахуванням принципів забезпечення інформаційної безпеки, задекларованих у законодавстві.

Як пише О. В. Олійник, методологічні засади адміністративно-правового забезпечення інформаційної безпеки України зумовлюють необхідністю формування загальнодержавної системи забезпечення інформаційної безпеки як найважливішої функції держави, справи всього українського народу. До найважливіших адміністративно-правових засад забезпечення інформаційної безпеки ми відносимо засоби правового регулювання відносин як сукупність правових механізмів, прийомів і способів забезпечення інформаційної безпеки

в широкому розумінні цієї сфери діяльності [189, с. 68].

На думку представників Національного інституту стратегічних досліджень при Президенті України феномен адміністративно-правового регулювання настільки складний, що вимагає розробки спеціального законопроекту про державне регулювання інформаційної безпеки, де, зокрема, могли б бути вказані цілі або функції адміністративно-правового регулювання інформаційної безпеки. Функції предметно-змістовного дії як елемент компетенції суб'єктів забезпечення інформаційної безпеки здійснюються при цьому в циклічному взаємозв'язку, відображаючи управлінське пізнання, і тоді розширюється горизонт управлінських впливів. Сьогодні впорядкування процесу за допомогою системи адміністративних регламентів і майбутнього закону про адміністративні процедури зміцнить правовий фундамент.[190].

Ключовою категорією при оцінці стану інформаційної безпеки держави, суспільства і особи та при оцінці управлінської діяльності, є поняття «ризик».

На відміну від цивілістичної наукової літератури ризик в публічному праві, в тому числі в науці адміністративного права, раніше практично не досліджувався, що штучно спрощувало механізм управління. Ризик в правовій сфері є ймовірне неправомірне відхилення від правових моделей діючих і майбутніх законів. Чинників для появи ризиків багато, На етапі оцінки ризиків формується стратегія управління ризиками, а оскільки повністю уникнути ризиків у більшості випадків неможливо, то вагоме значення має вирішення питання допустимості (прийнятності, виправданості) ризику, яке потребує подальшого дослідження та обґрунтування [191, с. 7].

Ризик-орієнтований підхід отримує визнання в діяльності Державної служби спеціального зв’язку і захисту інформації і інших учасників законопроектної діяльності, в роботі Кабінету Міністрів України при встановленні бюджетних параметрів. Стратегії розвитку оборонно-промислового комплексу України на період до 2028 року, інші правові акти містять норми про аналіз прийнятих рішень і їх наслідків [192]. Ризик виступає як параметр рішень і дій в змісті адміністративно-правового регулювання в

сфері забезпечення інформаційної безпеки, в зв'язку з чим в правових актах повинна бути орієнтація на прогнозний і ризикової аналіз, яка формується на підставі даних моніторингу передбачених Доктриною інформаційної безпеки України та Стратегією кібербезпеки України [64].

Адміністративно-правовий механізм забезпечення інформаційної безпеки, на наш погляд, слід збагатити досвідом з ризик-менеджменту, аналізу загроз або ризиків у сфері інформаційної безпеки, оскільки останні категорії більш повно розкриті в науці, ніж в законодавстві [193; 194; 195].

Збір, аналіз і використання інформації, що проводяться в межах моніторингу, є важливою функцією суб'єктів адміністративно-правового регулювання забезпечення інформаційної безпеки. Сьогодні її збагачення досягається на основі інформаційно-комунікаційних технологій і систем, а правове регулювання інформаційних операцій поєднується з встановленням правил про доступ до інформації про діяльність публічних органів, про проекти і діючі правові акти.

На думку І. Ф. Коржа, міцність правопорядку, авторитетність права значною мірою залежать від спроможності законодавця своєчасно враховувати відносини, що виникають і породжують спори, конфлікти, які потребують юридичного регулювання і захисту і які, насамперед, знаходять відображення в правозастосовній (судовій та адміністративній) практиці. Саме стабільна, авторитетна, динамічна правова система, яка забезпечена відповідним їй апаратом судової влади та правоохоронних органів – є найбільш ефективною формою упорядкування і динаміки суспільних відносин [196, с. 25].

В системі забезпечення інформаційної безпеки є важливою організаційна функція адміністративного процесу, що включає значну кількість оперативних, інструктивних, методичних і інших дій. Окремо виділимо координацію як функцію адміністративного процесу, що дозволяє погоджувати і об'єднувати дії різних суб'єктів адміністративного права в межах цільових програм та інших документів у сфері забезпечення інформаційної безпеки тощо.

У даний широко застосовуються такі заходи адміністративно-правового

регулювання окремих видів інформаційної діяльності, як ліцензування, акредитація та сертифікація, які, в першу чергу, направлені на забезпечення прав і свобод людини та громадянина і інших конституційно-правових цінностей, наприклад, Ліцензійні умови провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України [197].

У функції адміністративно-правового регулювання інформаційної безпеки держави входять підтримка єдності інформаційного простору; забезпечення свободи інформаційної діяльності. Невиконання таких функцій призводить до кризових явищ в політиці, соціально-економічному житті.

На думку І. М. Дороніна: «Необхідності застосування надзвичайного або екстраординарного законодавства в тій соціальні сфери, що перебувають під впливом заходів із реалізації безпекових функцій держави. В умовах сучасного світу правова регламентація, що здійснюється для виконання поставлених цілей, обмежується характером інформаційного суспільства та явищем необмеженості в розповсюдженні інформації. Унаслідок цього досить часто зазначене екстраординарне законодавство не досягає поставлених цілей» [198, с. 93-94]. Як наслідок, порушення стану інформаційної безпеки суспільства і окремих громадян в цілому.

Функції адміністративно-правового регулювання інформаційної безпеки носять комплексний характер, вони не обмежуються суто економічними цілями. Розглядаючи функцію адміністративного процесу – аналіз і оцінка ефективності адміністративно-правової діяльності, зазначимо, що для України в останнє десятиліття характерно введення системи показників управління за результатами на основі постанов і розпоряджень про показники та оцінки ефективності діяльності центральних і регіональних органів виконавчої влади та їх керівників. Наприклад, Порядок проведення моніторингу та оцінки результативності реалізації державної регіональної політики; Завдання, ключові показники результативності, ефективності та якості службової діяльності

державних службовців, які займають посади державних секретарів міністерств, на 2018 рік [199; 200]

У даний час мова йде про переоцінку ролі державного управління, яке, будучи формою реалізації виконавчої влади, є більш багатогранна та проявляється в нормативно-правовому регулюванні, координації, сприянні та у встановленні взаємодії між органами державної влади та бізнесом і громадянами.

Юристи і економісти, філософи, соціологи, математики, кібернетики висловлюють різні точки зору з питань сутності та класифікації функцій наукового управління. Не зупиняючись на дискусійних сторонах цієї проблеми, зауважимо, що в країнах Європейського Союзу у числі загальних функцій управління включають контроль [175].

Проблема функцій управління знаходиться в центрі уваги дослідників процесів управління. Автором найбільш розгорнутої класифікації функцій управління був А. Файоль. Французький теоретик організації управління запропонував класифікувати функції наступним чином: технічні, комерційні, фінансові, охоронні, рахункові, адміністративні. Адміністративні функції, які згодом поглинули всі інші, постають у нього як послідовні етапи реалізації керуючого впливу і складаються з: передбачення, організації, розпорядництва, координації, контролю [201].

М. Фуко пише, що за останні три-чотири століття функції держави серйозно розрослися під дією різних факторів, серед яких: соціальні революції, тероризм і забезпечення безпеки, науково-технологічний прогрес [202, с. 313].

Основними цілями збільшення кількості функцій адміністративно-правового регулювання інформаційної безпеки стали: необхідність захисту основних прав і свобод громадян (в тому числі і господарюючих суб'єктів); забезпечення територіальної цілісності та суверенітету; підтримання стабільного зростання національної економіки; стимулювання економічного розвитку; дотримання балансу в різних напрямах інформаційної безпеки; забезпечення безпеки інформаційної діяльності на глобальному, регіональному

та місцевому рівнях.

Крім методів впливу державної влади на відносини у сфері інформаційної безпеки, в науці адміністративного права виділяються форми такого впливу. Мова в першу чергу йде про різні заходи впливу на інформаційну безпеки, що здійснюються органами державного управління. Йдеться про зовнішній вираженні адміністративно-правового впливу на суб'єктів забезпечення інформаційної безпеки, тобто про інструмент, за допомогою якого виражається адміністративно-правове регулювання. Перекладені з статичного в динамічний стан вищевказані засоби стають методами, тобто прийомами, способами дії. Відповідно, можна говорити про технічні, організаційні, інформаційні, фінансові, правові, кадрові та інтелектуальні методи. До вказаних методів доцільно віднести: технічні; організаційні; інформаційні; фінансові; правові; кадрові; інтелектуальні (патентування, ноу-хау).

У процесі адміністративно-правового регулювання інформаційної безпеки господарської діяльності в даний час слід провести вироблення та прийняття Плану заходів з реалізації Доктрини інформаційної безпеки України, відповідно до Указу Президента України від 9 лютого 2018 року № 25/2018 «Про рішення Ради національної безпеки і оборони України від 26 січня 2018 року «Про додаткові заходи щодо протидії інформаційній агресії Російської Федерації», за напрямами: регламентація діяльності у сфері інформаційної безпеки, що утворює систему нормативно-правових актів для суб'єктів, діяльність яких здійснюється в інформаційній сфері, що визначають права і обов'язки, міру взаємної відповідальності, в тому числі введення заборон, націлених на недопущення шкоди споживачам інформаційних послуг; формування організаційно-економічних структур, що забезпечують строгий контроль за дотриманням вимог забезпечення інформаційної безпеки; вироблення соціально-інформаційної політики, визначення та результативне застосування механізмів реалізації адміністративно-правового регулювання інформаційної безпеки як особливого виду регулювання соціально-економічних процесів [203].

Організація адміністративно-правового регулювання забезпечення інформаційної безпеки проводиться на основі чітко визначених принципів, на яких базується система забезпечення безпеки та функціонування інформаційної безпеки країни. При адміністративно-правовому регулюванні забезпечення інформаційної безпеки слід враховувати: правила регулювання забезпечення інформаційної безпеки повинні бути єдині для всіх учасників, так як дозволяють передбачити ефект від цієї діяльності; за порушення правил передбачено невідворотне покарання. Подібний підхід до правових норм містить у собі справжній баланс і співвідношення економічних інтересів, тобто забезпечення інформаційної безпеки для всіх учасників діяльності в інформаційній сфері та споживачів інформаційних послуг; дотримання норм усіма учасниками інформаційної діяльності в суспільстві формуючи правову свідомість і законослухняну поведінку. Як підкреслювалося вище, про ефективність адміністративно-правового механізму можна судити за ступенем його корисності для життєво важливих інформаційних інтересів особи, суспільства та держави. Відповідно, за ступенем наближеності показників життєво важливих інтересів до високого рівня інформаційної безпеки можна зробити висновок про ефективність державного управління та державного регулювання і дієвості адміністративно-правових норм в механізмі державного управління в інформаційній сфері в цілому, і кожного суб'єкта забезпечення інформаційної безпеки окремо [64].

Розглянувши адміністративно-правове регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки зроблено наступні висновки.

Державне управління в сфері забезпечення інформаційної безпеки полягають у створенні умов для гармонійного розвитку національної інформаційної інфраструктури, для реалізації конституційних прав і свобод людини та громадянина, законних інтересів особи, суспільства та держави у національному інформаційному просторі, у отриманні інформації та користування нею фізичними та юридичними особами з метою забезпечення

непорушності конституційного ладу, суверенітету та територіальної цілісності України, політичної, економічної та соціальної стабільності, в безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

Державне регулювання забезпечення інформаційної безпеки є система нормативно-правових актів, що регламентує стабільне функціонування національної інформаційно-комунікаційної інфраструктури, національних інформаційних ресурсів, національного інформаційного простору, реалізацію інформаційних прав і свобод людини та громадянина, законні інтереси суспільства та держави, міжнародних зобов'язань України в інформаційній сфері, протидії екстремізму, сепаратизму, внутрішнім та зовнішнім загрозам національним інтересам визначеним Конституцією та законодавством України.

Методологічні засади адміністративно-правового забезпечення інформаційної безпеки України зумовлюють необхідністю формування загальнодержавної системи забезпечення інформаційної безпеки як важливої функції держави, справи всього українського народу. До адміністративно-правових засад забезпечення інформаційної безпеки відносяться засоби правового регулювання відносин як сукупність правових механізмів, прийомів і способів забезпечення інформаційної безпеки в широкому розумінні цієї сфери діяльності.

Адміністративно-правове регулювання забезпечення інформаційної безпеки є сукупність закріпленої в законодавстві системи заходів і прийомів, спрямованих на забезпечення безпечної діяльності в інформаційному просторі що динамічно розвивається, фізичних і юридичних осіб, сприятливої для інновацій, інвестицій, яка забезпечує населення, високий рівень життя і економічний прогрес. Тому зміст адміністративно-правового регулювання інформаційних відносин вимагає обґрунтування у межах адміністративно-правового режиму інформаційної безпеки

Концептуальний підхід до визначення поняття «адміністративно-правове забезпечення інформаційної безпеки» спирається на те, що правовий зміст

даної категорії розглядається як системна сукупність взаємопов'язаних, але структурно самостійних складових частин: державного управління інформаційною безпекою, державного регулювання інформаційної безпеки у контексті забезпечення прав і свобод особи, законних інтересів особи, суспільства та держави. Потреба такого виділення визначена різним змістом і обсягом прав кожної групи суб'єктів, що істотно відрізняються один від одного сукупністю викликів і загроз, специфічними адміністративно-правовими механізмами забезпечення безпеки для кожної групи суб'єктів

2.3 Система суб'єктів забезпечення інформаційної безпеки

Діяльність, що здійснюється суб'єктами адміністративно-правового забезпечення інформаційної безпеки, є як найважливішої формою реалізації правового забезпечення інформаційної безпеки, так і функцією даних суб'єктів, яка полягає в реалізації повноважень, наданих цим суб'єктам, з метою вирішення завдань державного управління в сфері забезпечення інформаційної безпеки особи, суспільства та держави. У науковій літературі тема суб'єктів у сфері забезпечення безпеки відображена досить різнопланово. Актуальність теми дослідження диктує необхідність визначення кола суб'єктів, які від імені держави здатні використовувати сукупність правових (юридичних) способів і засобів.

Суб'єкти адміністративного права – це визнані нормами права в якості можливих учасників управлінських відносин, що володіють адміністративної правоздатністю і адміністративною дієздатністю, носії юридичних прав та обов'язків. В адміністративному праві існують різні класифікації суб'єктів адміністративного права: відповідно до загальної теорії права виділяються громадяни і організації; громадяни, особи без громадянства та іноземні громадяни; органи державного управління; державні та громадські підприємства і установи; органи громадських організацій; службовці, які є носіями адміністративних прав і обов'язків [204].

Найбільш просту та точну класифікацію суб'єктів адміністративного права, на наш погляд, запропонував В. Б. Авер'янов: державні організації та їх представники і недержавні організації та їх представники; суб'єкти колективні та індивідуальні; фізичні, юридичні особи і колективні суб'єкти без статусу юридичної особи тощо [168, с. 190].

Автори підручника «Адміністративне право України. Повний курс» В. В. Шалунько, П. В. Діхтієвський, О. В. Кузьменко, С. Г. Стеценко до основних суб'єктів публічної адміністрації відносять: органи виконавчої влади; суб'єкти місцевого самоврядування; суб'єкти делегованих повноважень: громадські об'єднання; інші суб'єкти під час здійснення делегованих законодавством виконавчих функцій [205, с. 73].

Остання класифікація найбільш відповідає цілям нашого дослідження. Складовими елементами системи забезпечення безпеки України, поряд з центральними та місцевими органами виконавчої влади, органами державної влади та місцевого самоврядування, підприємствами, установами і організаціями різних форм власності, є громадські об'єднання та громадяни, які беруть участь в інформаційній діяльності. Істотним недоліком чинної системи правового регулювання в сфері забезпечення інформаційної безпеки є те, що в даний час не всі компоненти адміністративно-правового статусу зазначених органів нормативно закріплені.

Під органом державної влади розуміється, перш за все, організований колектив людей. Під організованим колективом людей розуміється колектив, який має внутрішню організаційну структуру, систему взаємозв'язків. Підтримка належним чином внутрішньої організаційної структури та системи взаємозв'язків в організованому колективі людей неможливо без реалізації відповідних владних повноважень внутрішньо-організаційного характеру. Такі повноваження є у уповноважених осіб в організованому колективі людей, визнаному в тій чи іншій формі державою.

Владні повноваження державного органу виражаються у праві видавати державно-правові акти (нормативні і індивідуальні) та в можливості

матеріальними, організаційними та примусовими засобами забезпечувати їх дотримання та виконання. Реалізація владних повноважень, як щодо видання нормативних або індивідуальних державно-правових актів, так щодо використанню матеріально-організаційних і примусових засобів їх забезпечення має на увазі виникнення певних юридичних наслідків у інших (зобов'язаних) суб'єктів права.

Органи державної влади відрізняються від інших колективних суб'єктів права, перш за все, наявністю зовнішніх державно-владних повноважень, наданих державою для досягнення поставлених перед ними цілей.

Самостійність органу державної влади полягає в можливості самостійно вирішувати поставлені перед органом завдання шляхом реалізації наявних у органу прав і виконання покладених на орган обов'язків. Очевидно, що діяльність органів виконавчої влади з організації забезпечення інформаційної безпеки слід розглядати, спираючись, перш за все, на категорію «державне управління», як адміністративно-політичну діяльність держави, здійснювану органами виконавчої влади.

Під діяльністю органів влади в сфері забезпечення безпеки держави, в тому числі інформаційної безпеки слід розуміти цілеспрямовану роботу з виявлення, попередження та нейтралізації (ліквідації) загроз життєво важливим об'єктам держави і здійснення заходів з планування та реалізації економічних процесів в країні. Прикладне значення механізму гарантування безпеки держави розкривається через функції, які він виконує. Безумовно, функція – це дія, діяльність, здійснення чи виконання певних операцій, що відбувається відповідно до зазначеного плану, алгоритму, припису тощо, тобто має чітко виражену траєкторію та сферу застосування [206, с. 2].

Беручи до уваги наявні в законодавстві норми, що допускають існування правових інститутів, що не входять в законодавчу, виконавчу, судову гілки влади, представляються обґрунтованими погляди дослідників В. В. Шалунько, П. В. Діхтієвський, О. В. Кузьменко, С. Г. Стеценко про необхідність наділення окремих державних органів України правовим статусом підсистем державної

влади, які не відносяться до певної гілки влади, наділених адміністративними повноваженнями або яким делеговані адміністративні повноваження [205, с. 86]. Прикладом відносини органів до кількох гілок влади може стати прокуратура, органи якої наділені владними повноваженнями.

У правовій дослідницької традиції існує безліч різних визначень категорії державного органу, проте, з погляду на дослідження В. М. Шаповала присвяченого В. Б. Авер'янову «Виконавча влада в Україні в контексті реформи державного правління (досвід після прийняття Конституції України 1996 року)», орган держави – це організована частина чинного державного механізму, що володіє владними повноваженнями, спеціальними компетенціями та необхідними засобами для здійснення завдань в конкретній галузі державного управління [207].

Сукупність правових засобів, за допомогою яких державою встановлюються межі реалізації громадянином прав у сфері державного управління, не може поширюватися за межі відповідної нормотворчої діяльності. Причому ця нормотворча діяльність здійснюється, перш за все, на законодавчому рівні. Законодавча діяльність – це завжди зовнішня діяльність органу законодавчої влади. Органи законодавчої влади є суб'єктами адміністративно-правового обмеження прав громадян в процесі здійснення зовнішньої державно-владної діяльності.

О. О. Косиця пише, що у юридичній літературі зустрічається формулювання системи органів державної влади у сфері інформаційної безпеки як сукупності взаємовідносин суб'єктів державного управління (органів державної влади), які проводять державно-управлінську діяльність на основі розмежування компетенції між ними щодо об'єктів державного управління з метою гарантування конституційних прав і свобод людини та громадянина, розвитку громадянського суспільства та захищеності інформаційного суверенітету держави, та яка включає в себе дві складові: систему органів законодавчої влади, що здійснюють функцію нормативно-правового регулювання загальнодержавного керівництва у сфері забезпечення

інформаційної безпеки, та систему органів виконавчої влади, які виконують функцію часткового формування у межах наданих повноважень і реалізації державної політики інформаційної безпеки у сучасних умовах [208, с. 6]

У даний час дослідниками виділяється кілька рівнів системи суб'єктів забезпечення інформаційної безпеки в Україні:

- рівень Президента України, який очолює Раду національної оборони та безпеки України [209];

- законодавчий рівень, на якому відбувається формування правових основ інформаційної безпеки України, встановлюється правовий статус учасників відносин, щодо забезпечення інформаційної безпеки, регламентується система органів влади і їх компетенція в названій сфері діяльності; виконавчий рівень суб'єктів забезпечення інформаційної безпеки, який включає велику кількість органів державної влади;

- рівень судових органів (перш за все, Конституційного суду України), і органів прокуратури, які забезпечують дотримання норм права учасниками правовідносин, що виникають у сфері інформаційної безпеки;

- правоохоронний (представлений МВС, спецслужбами і органами безпеки, які здійснюють оперативно-розшукову та попереджальну діяльність);

- функціональний, представлений державними інститутами, що здійснюють забезпечення інформаційної безпеки на рівні існуючої системи заходів;

- науково-дослідний рівень.

Європейська практика показує, що держава не ставить перед собою завдання щодо забезпечення інформаційної безпеки господарюючих суб'єктів як інституційних одиниць. Держава створює умови для нормативно-правового, інформаційного, наукового і іншого забезпечення діяльності щодо інформаційної безпеки інституційних одиниць, їх органів, зниження рівня зовнішніх загроз і ризиків.

Суб'єкти досліджуваної діяльності утворюють ієрархічну систему органів державної влади та недержавних формувань спеціальної компетенції.

Складовою частиною правового статусу органу державної влади є компетенція, яка складається з владних повноважень (прав і обов'язків, пов'язаних із здійсненням влади, в тому числі право на видання певних актів); підвідомчості, правового закріплення кола об'єктів, справ, предметів відання, на які поширюються владні повноваження. Термін «повноваження» використовується переважно для характеристики прав і обов'язків виконавчого органу, спрямованих на виконання завдань і функцій або в більш широкому значенні для позначення всієї сукупності правових можливостей держави впливати на суспільні відносини з метою їх упорядкування та стимулювання розвитку. Спираючись на аналіз чинного законодавства, можна констатувати відсутність однакового законодавчого підходу до вживання поняття «компетенція». Компетенція державного органу – це юридично надані права на рішення певного кола питань і на видання певних видів правових актів, права, що встановлюють місце даного органу в системі державних органів, які реалізуються ним самостійно.

М. М. Андріїв, розглядаючи поняття та структура компетенції органів публічної влади зазначає, що компетенція є правовою категорією для визначення певного обсягу прав і обов’язків (повноважень) органу [209, с. 4]. Компетенція виступає базовим поняттям адміністративно-правового становища колективних суб'єктів, родовим по відношенню до інших статусних елементів. Якщо предмети ведення вказують на конкретне питання сфери життєдіяльності, то обсяг діяльності органів держави та місцевого самоврядування в межах предмета відання буде характеризуватися поняттям «компетенція». Під адміністративно-правовим статусом органів виконавчої влади в сфері забезпечення інформаційної безпеки слід розуміти певне правове становище, досягнення якого тягне наділення повноваженнями та функціями, спрямованими на забезпечення стану захищеності особи, суспільства, держави.

З погляду на дослідження В. М. Брижка щодо гносеології у сфері інформаційного права, з точки зору правової гносеології, статус органів державного управління в сфері інформаційної безпеки – це правова категорія,

що відображає правове становище та соціальне призначення державного органу в механізмі правової держави, виражене в сукупності управлінських функцій і повноважень з певних предметів ведення та відповідальності, встановлених державою.

Складний процес реформування органів управління відповідно до Стратегії реформування державного управління України на 2016-2020 роки викликає необхідність пошуку нових форм і методів управління соціально-економічними системами у контексті інформатизації, з урахуванням забезпечення їх сталого розвитку та захисту інформаційних інтересів суб'єктів господарської і іншої діяльності, в тому числі інтересів особи, суспільства, держави [211]. В інформаційній безпеці гносеологія спрямована на дослідження логіки захисту інформаційно-інфраструктурних процесів у електронно-інформаційному середовищі на основі розвитку та використання інформаційно-комунікаційних технологій, інформаційних систем, мереж та інформаційних ресурсів [212, с. 31].

До відання вищого законодавчого органу України – Верховної Ради відносяться: ратифікація та денонсація міжнародних договорів і угод України; заслуховування послань Президента України, послань Конституційного Суду України, виступів Голови Кабінету Міністрів України, керівників органів виконавчої влади з питань забезпечення безпеки, в тому числі в інформаційній сфері; розробка за піднятими в них проблемах комплексу законодавчих заходів; визначення розмірів бюджетних асигнувань на фінансування суб'єктів забезпечення інформаційної безпеки. Безпосередньо питаннями інформаційної безпеки з позиції правого регулювання техніко-технологічного забезпечення займається Комітет з питань інформатизації та зв'язку [213]. Одним з напрямів роботи Комітету є підготовка парламентських слухань, наприклад, «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України» [214].

Загальне керівництво державними органами, що забезпечують інформаційну безпеку, здійснює глава держави – Президент України.

Координуюча роль належить Раді національної оборони та безпеки України, яка визначає стратегію забезпечення внутрішньої та зовнішньої безпеки, контролює та координує діяльність державних органів забезпечення безпеки, в тому числі в інформаційній сфері.

Принципами забезпечення безпеки та національних інтересів відповідно до Закону України «Про національну безпеку України» є: дотримання балансу життєво важливих інтересів особи, суспільства та держави; взаємна відповідальність особи, суспільства та держави щодо забезпечення безпеки; інтеграція України в європейський політичний, економічний, безпековий, правовий простір, набуття членства в Європейському Союзі та в Організації Північноатлантичного договору, розвиток рівноправних взаємовигідних відносин з іншими державами [72].

Правову основу діяльності Президента України, Кабінету Міністрів України та Ради національної оборони та безпеки України, всієї системи суб'єктів забезпечення інформаційної безпеки складають Конституція України, загальновизнані принципи та норми міжнародного права, міжнародні договори України, Закон України «Про національну безпеку України», інші закони, укази та розпорядження Президента, акти Кабінету Міністрів України.

Доктрина інформаційної безпеки України та Закон України «Про основні засади забезпечення кібербезпеки України» називає таких суб'єктів забезпечення інформаційної безпеки: Президент України; Рада національної безпеки і оборони; Кабінет Міністрів; Міністерства інформаційної політики, закордонних справ, оборони, культури; Генеральний штаб Збройних Сил; Збройні Сили і інші військові формування; Державне агентство України з питань кіно; Національна рада України з питань телебачення і радіомовлення; Державний комітет телебачення і радіомовлення України; Служба безпеки України; розвідувальні та контррозвідувальні органи, суб’єкти оперативно-розшукової діяльності; Державна служба спеціального зв'язку та захисту інформації України; Національний інститут стратегічних досліджень; міністерства та інші центральні органи виконавчої влади; місцеві державні

адміністрації; органи місцевого самоврядування; Національний банк України; підприємства, установи та організації, віднесені до об’єктів критичної інфраструктури, що забезпечують реалізацію цієї Стратегії кібербезпеки України відповідно до своєї компетенції [4; 19; 62].

Взаємодія органів виконавчої влади при реалізації Доктрини інформаційної безпеки та Стратегії кібербезпеки здійснюється в порядку, встановленому Кабінетом Міністрів [215, с. 137]. На думку М. А. Дмитренка: «При удосконалюванні державної системи інформаційної безпеки України необхідно зберігати баланс між демократією та безпекою і не допускати створення одноособового органу державної влади, що здійснює діяльність у сфері інформаційної безпеки, варто дотримуватися колективних основ, тобто зміцнювати систему всіх державних органів, покликаних вирішувати проблеми інформаційної безпеки, ні в якому разі не допускати монополізму одного з них. У числі пріоритетних завдань зазначених суб'єктів – підвищення ефективності міжвідомчої взаємодії, вироблення оптимального алгоритму прийняття управлінських рішень в усіх сферах державної політики, розробки та реалізації документів стратегічного планування в соціально-інформаційній сфері» [216, с. 16].

Серед суб'єктів забезпечення інформаційної безпеки слід виділити Раду національної оборони та безпеки України як конституційного органу щодо забезпечення безпеки країни. Рада національної оборони та безпеки є конституційним дорадчим органом, що здійснює підготовку рішень Президента України з питань забезпечення безпеки держави, громадської, інформаційної інших видів безпеки, передбачених законодавством України, організації оборони, військового будівництва, оборонного виробництва, військового і військово-технічного співробітництва з іноземними державами, з інших питань, пов'язаних із захистом конституційного ладу, суверенітету, незалежності та територіальної цілісності України, з питань міжнародного співробітництва в галузі забезпечення безпеки [209]. У складі Ради діє Департамент інформаційної безпеки [217].

Кабінет Міністрів України бере участь у формуванні Доктрини інформаційної безпеки України, яка розробляється Радою національної оборони та безпеки України на довгостроковий період. Доктрина інформаційної безпеки містить пріоритети, цілі та заходи внутрішньої та зовнішньої політики у сфері забезпечення інформаційної безпеки. Кабінет Міністрів України організовує та забезпечує виконання заходів організаційного, нормативно-правового та методичного характеру, необхідних для реалізації Доктрини інформаційної безпеки.

Разом з тим вихідними моментами при визначенні повноважень Кабінету Міністрів України служать положення Конституції України, Закону України «Про Кабінет Міністрів України» та регламент Кабінету Міністрів України відповідно до яких Кабінет Міністрів розробляє план заходів на 2018 рік з реалізації Стратегії кібербезпеки України, Порядок формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави; здійснює заходи щодо забезпечення законності, прав і свобод громадян у інформаційній сфері; боротьбі з кіберзлочинністю; здійснює інші повноваження, покладені Конституцією, законами України [185; 218; 219].

До загальних повноважень Кабінету Міністрів України належать: організація реалізації внутрішньої та зовнішньої політики України; здійснення регулювання в соціально-інформаційній сфері; забезпечення єдності системи виконавчої влади в Україні, напрями та контроль діяльності органів виконавчої влади; формування цільових програм та забезпечення їх реалізації; реалізація права законодавчої ініціативи.

Повноваження органу виконавчої влади характеризуються як можливість здійснювати покладені функції в певних правових формах із застосуванням, в залежності від ситуації, встановлених методів управління. У зв'язку з цим можна відзначити, що будь-яка соціально значуща функція, покликана сприяти досягненню цілей і завдань державного управління і, таким чином, регулювати суспільні відносини, використовуючи різні соціальні та правові регулятори, реалізується через відповідну діяльність і здійснюється спеціальними

державними органами, уповноваженими на це законом, у межах виключної компетенції, з використанням наданих законом повноважень.

Коли мова йде про суб'єктів забезпечення інформаційної безпеки, слід звернути увагу на систему забезпечення національної безпеки країни. Систему забезпечення національної безпеки на основі чинного законодавства та у межах єдиної державної політики утворюють взаємодіючі сили забезпечення, інші державні органи та організації, що несуть в межах своєї компетенції всю повноту відповідальності за забезпечення національної безпеки. При здійсненні органами виконавчої влади спеціальних функцій в встановлених сферах ведення, обов'язковим є тісна взаємодія органів виконавчої влади та місцевих органів виконавчої влади. Останніми в сфері забезпечення інформаційної безпеки, крім здійснення взаємодії, проводяться заходи залучення громадян, громадських об'єднань і організацій до сприяння у вирішенні проблем інформаційної безпеки.

Рішення серйозних правових проблем, що знаходяться у сфери державних інтересів у зв'язку із забезпеченням територіальної цілісності країни, інформаційної безпеки, здійснюється Конституційним Судом України відповідно до Закону України «Про Конституційний Суд України» [220]. Велике значення набувають акти Конституційного Суду України в процесі вдосконалення законодавства та правозастосовної практики в сфері інформаційної діяльності. Конституційний Суд відзначив складність і багатогранність функцій адміністративно-правового регулювання в сфері інформаційної безпеки.

Конституційний Суд визначив, що забезпечення економічної та інформаційної безпеки є важливими функціями держави, справою всього Українського народу [221]. Держава має право та зобов'язана здійснювати в сфері інформаційних відносин контрольну функцію, яка за своєю конституційно-правовою природою похідна від організуючого та регулюючого впливу на суспільні відносини та властива всім органам державної влади в межах закріпленої компетенції. Адміністративно-правове регулювання

забезпечення інформаційної безпеки демонструє реалізацію державою функції щодо захисту прав і свобод громадян.

Надані центральному органу виконавчої влади повноваження, відповідно до Закону України «Про центральні органи виконавчої влади», повинні бути спрямовані на вчинення певного керуючого впливу в сфері забезпечення інформаційної безпеки, що в свою чергу, виражається в реалізації управлінських функцій з урахуванням діяльнісної характеристики органу з вирішення проблемних питань в цій сфері [222]. До повноважень органів виконавчої влади стосується виконання законів та інших нормативних правових актів, які регламентують правовідносини в інформаційній сфері. Органи виконавчої влади організують розроблення та реалізацію державних програм забезпечення інформаційної безпеки, здійснюють проведення заходів з реалізації завдань інформаційної політики в межах повноважень.

На думку Н. В. Москалюк, типологія функцій органів виконавчої влади включає функції: формування державної політики; з ухвалення нормативно-правових актів; з контролю та нагляду; з управління державним майном; з надання державних послуг [223, с. 141]. При здійсненні органами виконавчої влади спеціальних функцій щодо забезпеченні інформаційної безпеки в встановлених сферах ведення, обов'язковим є взаємодія органів виконавчої влади усіх рівнів відповідно до Положення про електронну взаємодію державних електронних інформаційних ресурсів [224].

Серед органів виконавчої влади у сфері забезпечення інформаційної безпеки займає Міністерство інформаційної політики України. Міністерство є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сферах інформаційного суверенітету України, державного іномовлення та інформаційної безпеки [225].

Міністерство протидіє негативним інформаційним впливам зі сторони Російської Федерації, забезпечуючи інформаційну безпеку в соціально-психологічному аспекті. Як зазначено у Звіті Міністерства інформаційної політики України за 1 квартал 2018 року, місія Міністерства полягає у

створенні умов для формування конкурентного та незалежного інформаційного простору України, що ґрунтується на принципах і засадах громадянського суспільства та професійної спільноти, здатних до саморегуляції та саморозвитку, як гарантії попередження впливу на незалежні ЗМІ та як необхідної умови розвитку незалежної демократичної держави Україна, а також популяризації її цінностей у світі [226].

У контексті техніко-технологічного забезпечення інформаційної безпеки України головну роль відіграє Державна служба спеціального зв'язку та захисту інформації України. Відповідно до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» основним завданням є: формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних системах і на об’єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам [227].

Керівним органом служби є Адміністрація Державної служби спеціального зв’язку та захисту інформації України. Основними завданнями Адміністрації є: забезпечення інформаційної безпеки, здійснення контролю у сфері визначеної Законом «Про Державну службу спеціального зв'язку та захисту інформації України» [228]. Адміністрація Державної розробляє проекти законів і інших нормативно-правових актів з питань, що належать до її компетенції. Наприклад, Державні стандарти України: Захист інформації. Технічний захист інформації. Основні Положення. ДСТУ 3396.0-96; Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96; Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97 [229-231].

Виконання основних завдань, поставлених перед Державною службою спеціального зв'язку та захисту інформації України як єдиної централізованої

системою органів безпеки у сфері забезпечення інформаційної безпеки, досягаються за умови її тісної взаємодії з іншими органами виконавчої влади (Міністерством оборони України, Міністерством внутрішніх справ України, Службою зовнішньої розвідки України і іншими), з місцевими органами державної влади, підприємствами, установами, організаціями, громадськими об'єднаннями та громадянами.

Система органів виконавчої влади в забезпеченні інформаційної безпеки включає в себе державні структури, які відповідно до Конституції України та законами здійснюють правоохоронну діяльність.

До суб'єктів забезпечення інформаційної безпеки на різних рівнях відносяться організації, інститути, служби, окремі особи (оперативні працівники, співробітники служб безпеки, інженерно-технічні працівники служб захисту інформації тощо), які забезпечують інформаційну безпеку об'єкта на основі практичних дій, при введенні в дію механізму забезпечення інформаційної безпеки і організації практичних дій.

До державних органів, що забезпечують інформаційну безпеку, відповідно до законодавства України, слід віднести Збройні Сили, Міністерство оборони, Генеральний штаб Збройних Сил України (Головне управління зв'язку та інформаційних систем), інші війська і військові формування України, органи Міністерства внутрішніх справ України (Департамент інформатизації МВС України, Департамент кіберполіції, Державна служба охорони Національної поліції), підрозділи Національної гвардії України, Службу зовнішньої розвідки України [232-236].

Провідне місце в системі органів виконавчої влади в справі забезпечення інформаційної безпеки України належить Службі безпеки Україна, яка динамічно і ефективно розвиває та зміцнює свій професійний потенціал. Служба безпеки представляє собою єдину централізовану систему органів, яка здійснює в межах своєї компетенції державне управління в галузі забезпечення безпеки України шляхом реалізації основних функцій, до яких відносяться: контррозвідувальна діяльність, протидію екстремізму та тероризму, боротьба зі

злочинністю та корупцією, забезпечення інформаційної безпеки [237].

Традиційно юридична наука приділяє значну увагу вивченню компетенції органів Служби безпеки України при ліквідації або мінімізації інформаційних загроз особи, суспільства та держави. В останні роки помітно зросла кількість наукових праць у вигляді окремих монографій, дисертацій, наукових статей, присвячених зазначених питань. Зазначена служба найчастіше згадується в літературі серед державних органів, що забезпечують інформаційну безпеку держави [238; 239].

Особливе місце в системі органів забезпечення інформаційної безпеки займає Міністерство внутрішніх справ України. Усі структурні підрозділи Міністерства – апарат, учбові заклади системи МВС України, Національна поліція, Національна гвардія України, Державна прикордонна служба України, Державна служба України з надзвичайних ситуацій, Державна міграційна служба мають спеціальні підрозділи із забезпечення інформаційної безпеки.

У структурі Національної поліції діє кіберполіція, яка відповідно до Положення про Департамент кіберполіції протидіє кіберзлочинам у сфері інформаційної безпеки охоплюючи: соціальну інженерію – технологію управління людьми в Інтернет просторі; мальваре (англ. malware) – створення та розповсюдження вірусів і шкідливого програмного забезпечення; протиправний контент який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості та насильства; рефайлінг (англ. – re-fileing) – незаконну підміну телефонного трафіку [241, с. 11].

Як зауважує С. С. Єсімов, розглядаючи діяльність Національної поліції з забезпечення інформаційної безпеки у контексті діяльності засобів масової інформації, завдання поліції у сфері забезпечення інформаційної безпеки конкретизовано в наказі МВС України від 19 серпня 2014 року № 840 «Про деякі питання інформаційної безпеки України» [242]. Нормативними документами передбачено налагодження ефективної взаємодії з представниками Національної ради України з питань телебачення та радіомовлення в регіонах спрямованої на виявлення та припинення

протиправної діяльності провайдерів, фізичних і юридичних осіб, що здійснюють незаконну ретрансляцію заборонених рішеннями Окружного адміністративного суду м. Києва від 23 березня 2014 року, Національної ради України з питань телебачення і радіомовлення від 17.07.2014 № 292 і № 663 програм у місцях масового відпочинку та скупчення людей, баз відпочинку, розважальних закладів тощо [243, с. 211-212].

Підрозділи Державної служби охорони Національної поліції здійснюють фізичну охорону об’єктів інформаційної інфраструктури державної та недержавної власності віднесені до критичної інформаційної інфраструктури на підставі Закону України «Про Національну поліцію» [244]. Практична діяльність підрозділів Національної поліції щодо боротьбі з злочинами у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку представлена рядом заходів попереджувального характеру, цільовими оперативно-розшуковими заходами.

Структурними елементами системи органів забезпечення інформаційної безпеки особи, що представляється як система, елементами якої є інформаційно-правова та інформаційно-психологічна безпека, стають державні органи, які забезпечують інформаційну безпеку країни на рівні існуючої системи заходів захисту інформаційного простору. Це Державне агентство України з питань кіно; Національна рада України з питань телебачення і радіомовлення; Державний комітет телебачення і радіомовлення та Міністерство культури України [245-247]. Основною метою діяльності вказаних державних органів є підтримання стану захищеності суб'єктів інформаційних відносин, що включає якісне інформаційне середовище (оперативність, повнота, достовірність споживаної інформації), захищеність суб'єктів від негативних інформаційних впливів (інформаційно-психологічна безпека), захищеність інформації (безпека інформації), що забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин.

Доцільно на підставі вище викладеного створити спеціальний орган для координації діяльності державних та недержавних суб'єктів власників критично

важливої інформаційної інфраструктури в сфері забезпечення інформаційної безпеки.

Для держави ресурси стійкості пов'язані з підвищенням якості інформаційного середовища (повнота інформації, характер і масштаб трансльованих цінностей та ін.), для особи – з розширенням сфери усвідомлюваного функціонування свідомості, підвищенням ефективності самоврядування життєдіяльністю, розвитком адекватної інформаційно-орієнтовної основи соціальної поведінки людини, адекватної системи його суб'єктивних відносин до навколишнього світу та самому собі, формуванням регуляторів безпечної активності – системи цінностей та інших компонентів інтенціональної підструктури безпеки особи. Слід зауважити, що об'єкт «особа» є центральним у забезпеченні інформаційної безпеки держави, оскільки особистість як одиниця суспільства – безпосередній носій індивідуальної свідомості, впливаючи на менталітет соціуму, а тому питання інформаційної безпеки держави в значній мірі (залежно від аспекту її розгляду) є похідними від проблем безпеки особи.

Функціонально інформаційно-психологічна безпека, як і інші аспекти безпеки людини, спрямована на реалізацію прав і свобод, потреб, інтересів та прагнень особистості, підвищення якості життя, включаючи суб'єктивне відчуття захищеності, забезпечення можливостей особистісного розвитку та самореалізації. З цих позицій визначаються критерії інформаційно-психологічної безпеки.

Аналіз наукових праць показав, що ключовими об'єктами інформаційної безпеки можуть виступати, по-перше, держава і її національні інтереси в інформаційній сфері, по-друге, підприємство (організація), по-третє, особа (суб'єкт, психіка, свідомість), по-четверте, інформація. В останньому випадку цей об'єкт пасивний, вимагає тільки збереження (захисту), а в трьох попередніх – об'єкт може розглядатися з позиції захисту від зовнішніх негативних інформаційних впливів і з позиції нарощування внутрішніх ресурсів стійкості перед такими впливами.

Забезпеченням інформаційної безпеки господарюючих суб'єктів і окремих підприємств займаються дві групи суб'єктів. Перша група займається цією діяльністю безпосередньо на підприємстві, підпорядкована керівництву. Серед цієї групи можна виділити спеціалізовані суб'єкти (служби інформаційної безпеки і економічної безпеки та інші) основним призначенням яких є постійна професійна діяльність із забезпечення інформаційної безпеки підприємства (у межах своєї компетенції) та не спеціалізовані, так як їх діяльність призначена для забезпечення безпеки підприємства (юридичний відділ тощо). До третьої частини цієї групи суб'єктів належить увесь інший персонал і підрозділи підприємства, які у межах посадових інструкцій і положень про підрозділи зобов'язані вживати заходів до забезпечення інформаційної безпеки.

До другої групи суб'єктів відносяться органи і організації, які функціонують самостійно не підпорядковані керівництву підприємства, але їх діяльність має суттєвий (позитивне чи негативне) вплив на інформаційну безпеку підприємства.

Провідна роль у забезпеченні інформаційної безпеки критичної інфраструктури належить телекомунікацій. Численні випадки цілеспрямованого застосування інформаційно-комунікаційних технологій для виведення з ладу об'єктів критичної інфраструктури демонструють новий технологічний рівень інформаційного протиборства в кіберпросторі. При цьому статистика багаторічної латентної активності шкідливих програм продемонструвала необхідність серйозного вдосконалення підходів в галузі інформаційної безпеки.

Зокрема, необхідно комплексне рішення, що поєднує розвиток нормативної бази, впровадження європейської практики управління інформаційною безпекою, комплексів сертифікованих засобів захисту інформації, в першу чергу, засобів тестування систем захисту та моніторингу подій безпеки. Першорядні кроки слід зробити в напрямі розвитку методології, засобів тестування та аудиту безпеки програмного коду.

Повноцінне забезпечення безпеки інформаційної сфери держави можливо тільки із застосуванням власного обладнання засобів захисту, яке відповідає стандартам Організації Північноатлантичного договору (НАТО). про що прямо говориться в Доктрині інформаційної безпеки Україні та Стратегії кібербезпеки України. В умовах гібридної війни з Російською Федерацією питання безпеки при використанні інформаційно-комунікаційних технологій виходять на якісно інший рівень створення єдиної системи кібербезпеки як складової частини інформаційної та національної безпеки держави. Для вирішення проблем нових викликів і загроз у цій галузі необхідна правова база адаптована до стандартів НАТО.

Закони, в першу чергу, повинні бути спрямовані на криміналізацію протиправних діянь, що вчиняються з використанням інформаційно-комунікаційних технологій, надання слідчих повноважень правоохоронним органам, які розслідують справи, забезпечення схоронності цифрових доказів, регулювання пов'язаних з інформаційно-комунікаційними технологіями послуг і контроль переданих мережею даних. У зв'язку з цим необхідні активне міжнародне співробітництво та вироблення спеціальних процедур судочинства або доведення [248; 249]. При цьому всі ці заходи повинні здійснюватися при строгому дотриманні норм у галузі прав людини.

Суттєву роль у сфері забезпечення інформаційної безпеки грають інститути громадянського суспільства та громадяни, які відповідно до Конституції та чинного законодавства України мають права здійснювати контроль у зазначеній сфері.

Доктрина інформаційної безпеки України передбачає активну участь громадян і інститутів громадянського суспільства у формуванні стратегії інформаційної безпеки, безпосередньої участі у інформаційному протиборстві з негативними інформаційними впливами. Водночас, на наявність певний недоліків у зазначеній діяльності, особливо щодо нормативно-правого регулювання, вказано у доповідній записці Національного інституту стратегічних досліджень при Президенті України «Участь громадських

об’єднань у протидії інформаційній агресії РФ» [250].

Розглянув систему суб’єктів забезпечення інформаційної безпеки в Україні можна зробити висновки.

Первинним системоутворюючим елементом забезпечення інформаційної безпеки є правовий суб'єкт, який співіснує з правовими особами (фізичними і юридичними), взаємодіючи між собою на підставі суб'єктно-комунікативних взаємозв'язків. Суб'єкт забезпечення інформаційної безпеки – явище багатоаспектне, визначається чинним правом і іншими соціальними нормами в тій мірі, в якій дані соціальні норми знаходять свою закінченість в чинному праві, представляючи сукупність укладених в спеціальну юридичну форму правових якостей захисту інформаційних прав і свобод людини та публічного управління у сфері інформаційної безпеки.

Суб'єкт забезпечення інформаційної безпеки – це індивідуальна або колективна особа, потенційний учасник конкретних інформаційних відносин, що володіє правосуб'єктністю, яка за своїми особливостями є носієм суб'єктивних юридичних прав і обов'язків, бере участь у правовідносинах, відповідно цілям і завданням забезпечення інформаційної безпеки, докладаючи певні зусилля для досягнення позитивного інтересу, використовуючи засоби та методи адміністративно-правого регулювання.

Система суб'єктів забезпечення інформаційної безпеки – цілісна, синергетична сукупність елементів, що перебувають у обумовлених функціями забезпечення інформаційної безпеки суспільних відносинах, об'єднаних сферою інтересів і потреб, що відображають правові характеристики адміністративно-правових засобів регулювання, зміст і елементи правового статусу суб'єктів, які беруть участь у відносинах, регульованих нормами інформаційного права, системними за змістом.

Для забезпечення інформаційної безпеки характерна багаторівнева система суб'єктів, заснована на принципі єдності та диференціації. Перший рівень – це три групи суб'єктів: фізичні і юридичні особи, публічно-правові утворення, складові підсистеми цих суб'єктів. Інші рівні (структурні елементи

зазначених підсистем) це різного роду спеціальні суб'єкти адміністративного права, поділ яких обумовлено диференціацією предмета відповідного правового регулювання.

Для системи суб'єктів забезпечення інформаційної безпеки як суб'єктно-комунікативної характерний особливий спосіб взаємодії, який виступає похідним елементом правового регулювання цілеспрямованого впливу нормативно-правової системи на інформаційно-технічний, організаційно-правовий, психолого-педагогічний напрями забезпечення інформаційної безпеки. В умовах євроінтеграції в інформаційний і правовий простір співвідношення між правовим регулюванням напрямів забезпечення інформаційної безпеки змінюється, виступаючи в якості особливого різновиду державно-управлінської діяльності, правове регулювання трансформується в професійний вид діяльності, забезпечив правовий зв'язок між суб'єктами.

2.4 Особливості адміністративно-правового режиму забезпечення інформаційної безпеки

У межах адміністративно-правового регулювання забезпечення інформаційної безпеки доцільно привернути увагу до організаційно-правових механізмів управління, при яких забезпечення стабільного стану захищеності та динаміки зміни загроз вимагає спеціальних процедур і режимів. Адміністративно-правові режими стають необхідним елементом державного регулювання забезпеченням інформаційної безпеки, дієвим інструментом протидії інформаційній експансії Росії в умовах подальшої ескалації гібридної війни. У зв'язку з цим розширюється сфера їх практичної реалізації.

Особливо глибоко та ґрунтовно інститут правових режимів був проаналізований в роботах вчених-представників теорії держави та права.

В юридичній літературі виділяють правові режими, врегульовані однією галуззю права (галузеві) та врегульовані кількома галузями права (міжгалузеві). Визначення змісту адміністративно-правового режиму, основних його ознак

були предметом дослідження вчених: В. Б. Авер'янова, О. Ф. Андрійко, О. М. Бандурки, Ю. П. Битюка, В. М. Гаращука, І. С. Гриценка. Є. В. Додіна, Р. А. Калюжного, Н. В. Коваленко, Т. О. Коломоєць, В. К. Колпакова, А. Т. Комзюка, О. В. Кузьменко, С. О. Кузьніченко, Т. П. Мінки, О. І. Остапенка, Ю. С. Шемшученка, Х. П. Ярмакі та інших авторів.

На думку Т. П. Мінки, під правовим режимом адміністративного права слід розуміти форму функціонування відносин, що складають предмет адміністративного права, які забезпечуються особливим поєднанням правових способів, типів та методів адміністративно-правового регулювання, що створюють відповідний рівень динаміки цих відносин та визначають мету адміністративно-правового регулювання. Правовий режим адміністративного права змістовно включає предмет, особливе поєднання способів, типів і методів та мети адміністративно-правового регулювання. Правовий режим адміністративного права – це комплексна, багаторівнева, динамічна й відкрита система, що постійно змінює свою внутрішню структуру. Це проявляється в тому, що норми адміністративного права під час регулювання адміністративно-правових відносин або доповнюються нормами інших галузей публічного чи приватного права, або для регулювання певного виду адміністративно-правових відносин використовуються методи інших галузей права [251].

У дисертаційному дослідженні Н. В. Коваленко, адміністративно-правовий режим розглядається як особливий порядок правого регулювання, запровадження якого обумовлено предметом правого регулювання, що полягає у встановленні у сукупності правил сформульованих у формі дозволів, заборон, процедур, регламентів, які повинні дотримуватися суб'єкти публічного управління з метою ефективного забезпечення прав, свобод, законних інтересів фізичних осіб, прав та свобод юридичних осіб [252, с. 412].

Поняттю та видам правового режиму в юридичній літературі присвячено багато досліджень юристів, що спеціалізуються в різних галузях права. Слово режим (лат. regimen – управління, керівництво) означає встановлений національним законодавством і нормами міжнародного права порядок у

суспільних відносинах (національний режим, правовий режим, прикордонний режим тощо). Режим розглядається як свого роду розширений блок у загальному арсеналі правового інструментарію, що з’єднує в одну конструкцію визначений комплекс правових засобів [253, с. 218].

В юридичній літературі правовий режим найчастіше визначається як комплекс соціальних відносин певного об'єкта або виду діяльності, закріплений юридичними нормами та забезпечений сукупністю організаційних засобів, або як юридична конструкція, утворена сукупністю нормативно-правових актів, об'єднаних за допомогою юридичних засобів у режимні правила. Говорячи про способи правового регулювання, як про основу змісту правового режиму, один із способів виступає в якості домінуючого, створюючи специфічну спрямованість в регулюванні.

Адміністративно-правовий режим є галузевої різновидом правового режиму. Поняття правової режим і адміністративно-правовий режим співвідносяться як загальне і особливе.

На думку О. В. Вакарюк, правовий режим галузі права є сукупністю юридичних засобів регулювання – галузевим юридичним інструментарієм, – опосередкованих галузевим методом правової дії, яка базується на принципах, специфічних для даної галузі [254, с. 199].

Галузевий правовий режим є цілісна система регулятивного впливу, яка характеризується специфічними прийомами регулювання дією єдиних принципів, загальних положень, особливим порядком виникнення та формування змісту прав і обов'язків, специфікою санкцій, способів їх реалізації. Адміністративно-правовий режим визначається специфікою в основі якого лежать принципи адміністративно-правового регулювання, методи та способи адміністративно-правового впливу, правове становище учасників адміністративно-правових відносин.

Це режим, який може бути позначений як загальний режим діяльності державної адміністрації. Адміністративно-правовий режим деякі автори визначають, як спеціальний комплекс оперативних державних управлінських

рішень і адміністративно-правових заходів переконання та примусу, здатних забезпечити досить оперативно стабілізацію суспільних відносин в регіоні або державі в цілому, подальше упорядкування суспільних відносин, що вийшли за межі впливу звичайних адміністративно-правових заходів.

Адміністративно-правовий режим, на відміну від інших правових режимів, являє собою поєднання адміністративно-правових засобів регулювання, опосередковане централізованим порядком, імперативним методом юридичного впливу, яке виражається в тому, що суб'єкти правовідносин за своїм статусом займають юридично нерівні позиції.

О. В. Адабаш в якості основної відмітної ознаки бачить те, що адміністративно-правовий режим відрізняється від інших режимів предметом регулювання, тобто державним управлінням, являє собою цілісну систему регулятивного впливу на ті ділянки соціальної діяльності, де необхідне забезпечення публічних інтересів [255, с.38].

У змісті даних режимів беруть участь норми конституційного, адміністративного, міжнародного, фінансового права. Режими зачіпають різні за характером права і обов'язки суб'єктів режимного регулювання. Це стосується режиму в зоні проведення антитерористичної операції [256, с. 267].

Однак, включення в правові режими, що забезпечують безпеку, охорону територій, об'єктів, установ, норм різної галузевої приналежності не змінює природи основних регулятивних засобів цих режимів, вони є адміністративно-правовими.

За ступенем жорсткості (обсягів правого регулювання) адміністративно-правові режими прийнято розділяти на загальні та спеціальні. Під загальними режимами в юридичній літературі прийнято розуміти сукупність правових засобів, що дозволяють публічної влади досягати поставлених перед цілей в процесі повсякденного позитивного регулювання будь-яких процесів.

Повсякденність і позитивність управлінської діяльності у межах загальних адміністративно-правових режимів не дозволяють кардинально виділяти наявність особливостей у використанні правових способів досягнення

управлінської мети. Особливість загальних адміністративно-правових режимів обумовлена, перш за все, специфікою самих об'єктів регулювання або специфікою регульованих в цих межах режимних процесів.

Найбільший інтерес для дослідження особливостей обмеження прав громадян в правових режимів представляють спеціальні адміністративно-правові режими. Спеціальним адміністративно-правовим режимом, на думку С. О. Кузніченка, названо особливий порядок правового регулювання, що встановлений у нормативно-правових актах і який забезпечується й охороняється державою з метою регулювання суспільних відносин в окремій сфері державного управління, виокремлюючи конкретний рівень діяльності (сприятливий або несприятливий) для задоволення інтересів суб’єкта права [257, с. 22].

Ознаками спеціальних адміністративно-правових режимів є: встановлюються в сфері діяльності публічної адміністрації в зв'язку з виконанням органами державної влади та місцевого самоврядування обов'язків забезпечити безпеку, охорону, захист; утворюють режимні правила, що складаються із заборонних і зобов'язуючих адміністративно-правових норм, що обмежують загальну правосуб'єктність фізичних і юридичних осіб; суб'єкти особливих правових режимів є виконавчі органи державної влади); адміністративно-правовий метод впливу при регулюванні правовідносин, що виникають між населенням і публічною адміністрацією з приводу дотримання режимних правил; порушення правил режиму викликає застосування адміністративного примусу.

У свою чергу спеціальні адміністративно-правові режими за юридичними властивостями можна також поділити на ординарні та надзвичайні (екстраординарні). Надзвичайні режими вводяться в разі виникнення надзвичайних ситуацій соціального або природно-техногенного характеру, у випадках, коли це необхідно для забезпечення оборони та безпеки держави, стихійних лих тощо.

Як зазначає В. В. Середа: «Правові надзвичайні режими у сфері

публічного права мають такі особливості: формуються за допомогою юридичних засобів обмежувального характеру (заборон, призупинень та ін.); в межах правових режимів основним методом правового регулювання є імперативний із переважання дозвільного типу правового регулювання; закріплюються на рівні законодавчих і відомчих нормативних актів; спрямовані на припинення протиправної поведінки, можливості вчинення протиправних діянь, захист законних інтересів особи, суспільства, держави; пов’язані з виникненням публічних правових відносин, де одним із суб’єктів є держава в особі державних органів або посадових осіб; юридичні засоби-стимули мають гарантуючий характер, дозволяючи виконувати суб’єктам покладені на них юридичні обов’язки [258, с. 103].

З погляду на дослідження М. В. Коваліва, А. І. Рутар, Ю. В. Павлишин, «Порядок і підстави введення правового режиму надзвичайного стану», серед адміністративно-правових режимів, у межах яких протікає правоохоронна діяльність, особливе місце займають режими надзвичайного та воєнного стану, врегульовані відповідними законами «Про правовий режим надзвичайного стану», «Про правовий режим воєнного стану» [259; 260; 261].

На прикладі надзвичайних спеціальних адміністративно-правових режимів доцільно розглянути особливості нормативно-правового обмеження прав громадян у межах окремих правових режимів, що зумовлено важливістю суспільних відносин, що регулюються зазначеними режимами. Найбільший обсяг обмежень визначено у Законах України «Про правовий режим надзвичайного стану», «Про правовий режим воєнного стану» [260; 261].

Однак, незважаючи на зазначені обставини, формулювання надзвичайного, військового і особливого стану, закріплені в чинному законодавстві, схожі. Всі ці положення визначають встановлені законами окремі обмеження прав і свобод суб'єктів права та покладання на них додаткових юридичних обов'язків.

Крім окремих обмежень прав і свобод суб'єктів права, покладання додаткових юридичних обов'язків, Л. Г. Чистоклетов, О. Л. Хитра,

Л. О. Остапенко, Р. В. Скриньковський до відмінних рис надзвичайних режимів відносить надання надзвичайних повноважень органам влади для підтримки режиму; введення форм особливого управління територією, на якій встановлений надзвичайний режим, включаючи створення тимчасових спеціальних органів; перерозподіл компетенції; призупинення діяльності окремих органів державної влади та місцевого самоврядування [262, с. 6004].

Сутністю адміністративно-правового режиму є саме офіційно встановлений і нормативно закріплений особливий порядок правового регулювання. Цей порядок властивий будь-якому з видів адміністративно-правових режимів без його встановлення та приведення в дію структурних елементів неможлива діяльність регіонів і держави в цілому.

При дослідженні адміністративно-правових режимів слід враховувати положення, що дозволяють більш детально розглянути цей інститут адміністративного права, це: метод правового регулювання, який в адміністративному праві ґрунтується на централізованому засобі та інтегративному типі регулювання, що виражається в юридичній нерівності суб'єктів правовідносин; особливі адміністративно-правові способу встановлення та форми виникнення прав і обов'язків, способів юридичного впливу та захисту прав; особливі процедурні та процесуальні форми; особливі форми нагляду та контролю в процесі застосування адміністративно-правових режимів; різні види адміністративного примусу, що застосовуються.

Правовою основою адміністративно-правових режимів виступають Конституція України, закони, Укази Президента, постанови Кабінету Міністрів України, акти центральних органів виконавчої влади.

Нормативно-правова основа адміністративно-правових режимів багато в чому залежить від характеру та виду режиму. Необхідно підкреслити роль значення Конституції України, норми якої закріплюють такі види адміністративно-правових режимів, як режим надзвичайного стану, режим воєнного стану, режим державного кордону.

Настюк В. Я. та Бєлєвцева В. В. розмежовує загальний режим діяльності

державної адміністрації та спеціальні адміністративно-правові режими, які вводяться додатково для забезпечення правового порядку спеціальними законами, застосовуючи в більшій мірі забороняючи та зобов'язуючи норми, закріплюючи режимні правила життєдіяльності, особливий статус суб'єктів режиму; можливість в деяких випадках поєднання режимів, що вводяться на всій країни, що вводяться в окремій місцевості [263, с. 43]. Різноманітність правових режимів передбачає можливість проведення їх класифікації.

Але доцільно зауважити, що Н. В. Коваленко говорить про те, що не ефективно досліджувати адміністративно-правові режими через критерії їх класифікації [252, с. 415]. Визначивши в якості основного критерію мети режимів, їх можна розділити на кілька груп:

- адміністративно-правові режими певних державних станів (надзвичайного або воєнного стану, охорони державних і митних кордонів, регулювання зовнішньоторговельної діяльності та інші);

- функціональні адміністративно-правові режими, що забезпечують функції управління та сфери діяльності (податкову, екологічну тощо);

- легалізуючи режими, що передбачають офіційну реєстрацію юридичних і фізичних осіб, регламентацію нормативних вимог щодо різних видів діяльності.

У сфері інформаційної безпеки існує кілька груп адміністративно-правових режимів. Перша група цих режимів включає адміністративно-правові режими для конкретних державних станів, в тому числі, умов надзвичайного, воєнного стану, охорони державних кордонів, митного простору. До другої групи належать функціональні адміністративно-правові режими, основною метою яких є реалізація функцій управління в конкретних суспільних галузях, зокрема, фінансовій, транспортній, енергетичної тощо. Ще одну групу адміністративно-правових режимів складають легалізуючи режими, які стосуються офіційної реєстрації юридичних і фізичних осіб, регламентації певних видів діяльності. Такі адміністративно-правові режими конкретизуються або як звичайні, повсякденно застосовуються у межах певного

кола правового регулювання, або як особливі, що вводяться для досягнення спеціалізованого порядку дій і підтримки стану певної галузі економіки на необхідному рівні (наприклад, Порядок вжиття тимчасових надзвичайних заходів з подолання наслідків тривалого порушення нормальної роботи ринку електричної енергії [264]).

Зокрема, до першої групи можуть бути включені адміністративно-правові режими, що встановлюються правилами діяльності як певного роду правилами або стандартами, передбаченими для конкретного виду діяльності. До них відносяться правила надання послуг телефонного, телеграфного зв'язку, діяльності провайдерів тощо, зазвичай затверджуються підзаконними актами. Наприклад, рішення Національної комісії, що здійснює державне регулювання у сфері зв’язку та інформатизації від 10 грудня 2013 року № 803 «Про затвердження Правил здійснення діяльності у сфері телекомунікацій (діяльність з надання послуг доступу до Інтернет) [265].

Друга підсистема функціональних адміністративно-правових режимів вводиться або в певні періоди, або при виникненні певних юридичних фактів. Дані режими характеризуються значно меншим обсягом регулювання та своєрідністю, пов'язаним з більш жорсткими методами регулювання. З їх допомогою забезпечується циклічність юридичних дій суб'єктів права. Наприклад, Державні будівельні норми України Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва ДБН А.2.2-2-96 [266].

Мета адміністративно-правових режимів реалізувати особливий вид регулювання у межах якого використовується специфічна комбінація юридичних, організаційних і інших засобів для забезпечення певного стану. До засобів відносяться: уповноважені державні органи, спеціально створювані або наділені повноваженнями формувати та підтримувати відповідний режим; правові акти та норми, що встановлюють особливий порядок діяльності; система контролю та відповідальності за діяльність у межах адміністративно-правового режиму; детальна регламентація дій і взаємовідносин суб'єктів

права; застосування обмежено-дозвільних і заборонних методів, поєднаних в необхідних випадках зі цільовим стимулюванням суб'єктів права; наявність спеціальних організаційно-технічних, матеріально-фінансових засобів (техніки, ресурсів тощо). Такий підхід розкривається у адміністративно-правових режимах забезпечення інформаційної безпеки.

Наприклад, О. В. Орел, А. С. Мідіна розглядаючи адміністративно-правові засади оцінки рівня ризиків безпеки інформації в процесах службово-бойової діяльності Національної гвардії України вказують, що адміністративно-правових режим виступає як сукупність прийомів і способів, урегульованих нормами права, спрямованих на захист безпеки інформації, визначення рівня кількісно-якісної оцінки небезпеки в процесах службово-бойової діяльності, що виражаються в інструментах і діяннях, за допомогою яких задовольняються інтереси суб’єктів права з метою удосконалення інформаційного простору [267, с. 48].

Контроль є невід'ємною інструментальної функцією адміністративно-правового режиму публічного управління, що забезпечує зворотний зв'язок об'єкта управління з його суб'єктом, але не збігається з подальшим регулюючим впливом контролюючого суб'єкта на контрольований суб'єкт, що є наслідком отримання контрольної інформації. Контроль є одним з важливих організаційно-правових засобів адміністративно-правового забезпечення та відрізняється ознаками: по-перше, необхідно достатній обсяг перевірки, по-друге, комплексність оцінки контрольованих суб'єктів, по-третє, допустимість оперативного втручання в діяльність підконтрольних фізичних і юридичних осіб з метою виправлення виявлених в процесі контролю недоліків і зловживань. Дана характеристика контролю може бути деталізована, зокрема, як призупинення або скасування незаконних або недоцільних актів управління, застосування адміністративно-запобіжних, адміністративно-відновлювальних заходів, прийняття рішень про притягнення до різних видів правової відповідальності.

Адміністративно-правові режими, як правило, відображають існуючі

положення нормативно-правових актів. Однак є приклади фіксації адміністративно-правових режимів в спеціальних актах, наприклад, у стандартах серії ISO 27k, що присвячені побудові системи управління інформаційною безпекою.

ISO/IEC 27000:2012 Цей стандарт містить огляд та словник термінів, що відносяться до системи управління інформаційною безпекою (далі – СУІБ). Словник (глосарій) містить ретельно сформульовані формальні дефініції більшості базових термінів, пов’язаних з інформаційною безпекою.

ISO/IE 27001:2013. Стандарт містить вимоги у галузі інформаційної безпеки щодо створення, розвитку і підтримки СУІБ. Основою стандарту є система управління ризиками, пов’язаними з інформацією.

ISO/IEC 27002:2013 Висвітлює найкращі практичні поради щодо менеджменту інформаційної безпеки для тих, хто відповідає за створення, реалізацію або обслуговування СУІБ.

ISO/IEC 27003:2010. У цьому стандарті розглядаються найважливіші аспекти, необхідні для успішної розробки та впровадження СУІБ відповідно до стандарту ISO 27001.

ISO/IEC 27004:2009 Стандарт містить рекомендації щодо розробки та використання вимірювань і мір вимірювання для проведення оцінки ефективності реалізованої СУІБ, а також заходи і засоби контролю та управління відповідно до ISO 27001.

ISO/IEC 27011:2008. Прийняття цього стандарту дозволить телекомунікаційним організаціям забезпечити базові вимоги щодо управління інформаційною безпекою (конфіденційність, цілісність, доступність).

ISO/IEC 27014:2013. Цей стандарт є керівництвом щодо створення концепції і принципів управління інформаційною безпекою, за допомогою яких організації (різних типів і розмірів) можуть оцінити, корегувати, контролювати діяльність організації щодо інформаційної безпеки.

ISO/IEC 27035:2011. Встановлює рекомендації щодо менеджменту інцидентів інформаційної безпеки і стосується керівників підрозділів з

інформаційної безпеки, інформаційних систем, сервісів та мереж [268].

Такі юридичні акти стають юридичною основою оперативних вказівок, наказів і розпоряджень. При цьому особливого значення в забезпеченні юридично-операціональної діяльності фізичних і юридичних осіб відводиться встановленню прямого зв'язку змісту нормативного акта з вищеназваними розпорядчими документами, послідовності прийняття та практичної реалізації.

До ознак спеціальних адміністративно-правових режимів відносяться:

- сфера їх застосування, пов'язана з діяльністю органів виконавчої влади та виконавчо-розпорядчих місцевих органів адміністративно-територіальних утворень у зв'язку з виконанням ними обов'язків щодо забезпечення різних видів безпеки, захисту прав і свобод фізичних і юридичних осіб;

- режимні правила, що складаються із заборонних і зобов’язуючих адміністративно-правових норм, що обмежують загальну правосуб'єктність фізичних і юридичних осіб;

- адміністративно-правовий метод впливу, що застосовується при регулюванні правовідносин, що виникають між населенням і органами виконавчої влади та місцевого самоврядування з дотримання режимних правил;

- заходи дисциплінарного і адміністративного примусу, що застосовуються у випадках порушення режимних правил.

Н. В. Коваленко досліджуючи окремі складові адміністративно-правового режиму конфіденційної інформації зазначає, що під правовим режимом конфіденційної інформації необхідно розуміти сукупність ознак і особливостей, притаманних їй, враховуючи певні цивільно-правові наслідки. Інформація не є загальним юридичним терміном і не має загальних властивостей об’єктів цивільного права. Можна стверджувати, що визначити і дослідити правовий режим конфіденційної інформації доволі важко, оскільки цей вид інформації є багатогранним об’єктом і може перехрещуватися у різних правовідносинах. Механізм правового регулювання інформації, конфіденційної інформації буде іншим – відмінним від речей і від об’єктів права інтелектуальної власності. Отже, адміністративно-правовий режим є сукупністю норм права, що може

визначатись як складова частина нормативно-правової системи права та має субстанціональні ознаки, зумовлені специфікою предмета та методу правового регулювання. Важливо вказати на спорідненість правових конструкцій категорії правового режиму та категорії правового інституту [269, с. 80].

Залежно від підвідомчості спеціальні адміністративно-правові режими забезпечення інформаційної безпеки поділяють на: що встановлюються та регульовані центральними органами державної влади; регіональні режими, що встановлюються місцевими органами державної влади; режими, що встановлюються суб’єктами господарської діяльності тобто корпоративний рівень зазначеного режиму, встановлений внутрішніми документами організації або об'єднання. Деякі види режимів можуть перебувати у всіх трьох групах.

У 90-ті роки минулого століття виділялась роль адміністративно-правового режиму в якості універсального явища для державного та місцевого управління. У даний час представники науки адміністративного права сходяться на думці, що потрібні нові підходи до змісту та до побудови системи адміністративного права з підгалузями, інститутами, нормами права, що обумовлює застосування такого інституту як правовий режим.

Адміністративно-правові режими формуються за допомогою норм адміністративного права з подальшою орієнтацією на реалізацію цілком певних повноважень державних органів і органів місцевого самоврядування, рішення завдань, що стоять перед недержавними організаціями, підприємствами та установами,громадянами. Публічний інтерес, який виражається в такій діяльності суб'єктів, обумовлює цільову спрямованість. Виділення адміністративно-функціонального режиму забезпечення інформаційної безпеки мотивується функціональною класифікацією діяльності, пов'язаної з предметною спеціалізацією класу адміністративно-функціональних режимів забезпечення інформаційної безпеки.

Адміністративно-правовий режим у сфері інформаційної безпеки це закріплений нормами адміністративного права, гарантований і стабільний порядок регулювання діяльності державних органів, органів місцевого

самоврядування, їх посадових осіб, інститутів громадянського суспільства і громадян, спрямований на регламентацію суспільних відносин в інформаційній сфері, припинення діяльності, що допускає можливість нанесення шкоди інформаційній безпеці передбачає можливість застосування спеціальних режимних заходів, інших спеціальних форм і методів діяльності уповноважених органів, обумовлених необхідністю адекватної протидії загрозам інформаційної безпеки.

На нашу думку, з огляду на важливість проблеми забезпечення інформаційної безпеки особи, суспільства та держави режим інформаційної безпеки варто віднести до особливих. Різноманітність позицій і думок про співвідношення та зміст різних елементів адміністративно-правових режимів обумовлено різноманіттям видів самих режимів. Перераховуючи останні роботи з даної тематики, слід звернути увагу на кілька нових варіантів адміністративно-правових режимів.

На думку Ю. П. Лісовської, адміністративно-правове забезпечення інформаційної безпеки – це комплекс превентивних дій економічного, політичного, юридичного, технологічного та організаційного характеру, спрямованих на попередження, виявлення і ліквідацію загроз інтересам особи, держави та суспільства в інформаційній сфері. Ознаки адміністративно-правового забезпечення інформаційної безпеки: нормативно-правова база з питань забезпечення інформаційної безпеки; органи, сили та засоби забезпечення інформаційної безпеки; забезпечення збалансованого існування інтересів особи, держави та суспільства в інформаційній сфері; координація діяльності елементів системи забезпечення інформаційної безпеки на усіх рівнях державного управління; проведення державної політики щодо забезпечення інформаційної безпеки [270, с. 13].

У наукових дослідженнях, присвячених адміністративно-правовим режимам, виділяють відносно нові режими, зокрема, режим конфіденційної інформації. Проблема правового регулювання адміністративно-правового режиму інформаційної безпеки набуває особливої актуальності в умовах

гібридної війни, нестабільної економічної ситуації зумовленої бойовими діями на сході країни та складності забезпечення інформаційної безпеки на всіх рівнях. Розробка даного режиму є не тільки важливою для юридичної науки теоретичної проблемою, але і проблемою, що стосується практичної діяльності органів державної влади, місцевого самоврядування інших суб'єктів забезпечення інформаційної безпеки при дотриманні балансу інформаційних інтересів особи, суспільства та держави. У зв'язку з цим необхідні розробка та прийняття законодавчих і інших нормативно-правових актів, що визначають завдання, цілі, підстави, принципи та межі дії адміністративно-правового режиму інформаційної безпеки.

При виявленні адміністративно-правових методів державного регулювання щодо забезпечення режиму інформаційної безпеки необхідно законодавчо визначити:

- підстави і порядок встановлення адміністративно-правового режиму інформаційної безпеки, час дії;

- сфери економіки з найбільшим числом об’єктів критичної інформаційної інфраструктури, які необхідно особливо контролювати в умовах адміністративно-правового режиму інформаційної безпеки з можливими загрозами для особи, суспільства та держави, що зобов'язує законодавця певним чином нормативно реагувати на запобігання або мінімізацію;

- сукупність обставин економічного, соціально-політичного, кримінального характеру, надзвичайних ситуацій природного, техногенного характеру, які суттєво впливають на рішення державних органів влади і управління при забезпеченні адміністративно-правового режиму інформаційної безпеки;

- повноваження органів державної влади та місцевого самоврядування, механізм реалізації (напрями, інструменти, заходи для забезпечення), правові та соціальні гарантії, перелік заходів і тимчасових обмежень для громадян, посадових та юридичних осіб (санкцій) у зв'язку з його введенням;

- правову базу, яка регулює питання формування та застосування сил і

засобів для забезпечення адміністративно-правового режиму інформаційної безпеки, відповідальність за порушення адміністративно-правового режиму інформаційної безпеки, яка регулюються нормами декількох галузей права.

- співвідношення різних адміністративно-правових режимів та адміністративно-правового режиму інформаційної безпеки, адміністративних методів захисту, способів здійснення контролю та нагляду з боку держави за адміністративно-правовим режимом інформаційної безпеки.

Безпеці за природою властивий стан динамічної (нестійкої) рівноваги, де трансформація параметрів системи, в тому числі з огляду на неконтрольований розвиток факторів, що утворюють загрози, тягне за собою подальші зміни в усій сукупності елементів, що підсилюються з плином часу.

Забезпечення інформаційної безпеки є динамічним процесом, на який впливають поточні тенденції розвитку суспільства. Відносини між рівнями забезпечення інформаційної безпеки є рухомими. Вони організовані за принципом зворотного зв'язку, в результаті чого діяльність практично всіх суб'єктів в даній системі включена в динамічну взаємодію тому, що цілі, завдання, потреби та мотиви суб'єктів різних рівнів системи можуть збігатися, але можуть вступати в протиріччя, їх сукупність не є арифметичну суму.

Функціонування системи забезпечення інформаційної безпеки на кожному рівні та при здійсненні взаємодії, організованій за принципом зворотного зв'язку, передбачає реалізацію процесів синергетики. Для складних систем, до яких відноситься забезпечення інформаційної безпеки, існують досить ефективні, організаційно-правові та управляючі синергетичні ідеї, які можуть сприяти підвищенню ефективності правового регулювання та оптимізувати правові засоби забезпечення інформаційної безпеки.

У даному аспекті можна констатувати, що адміністративно-правове забезпечення є синергетична система, у зв’язку з тим, що їй об'єктивно притаманні властивості, що детермінують самоорганізацію та саморозвиток. Ряд класичних підходів одновимірного регулювання суспільних відносин у сфері забезпечення інформаційної безпеки певною мірою втрачає актуальність

у зв'язку зі зменшенням ефективності правового впливу. Одним з проявів якого є домінування організаційно-управлінського впливу елементів зазначеного механізму щодо результатів впливу останніх, в разі їх автономного функціонування.

На етапі європейської інтеграції дослідження адміністративно-правового забезпечення інформаційної безпеки не може залишатися поза масштабних і багатопланових процесів наростання загального і універсального, яке знаходить своє вираження як в національних економічних і соціальних системах, так і в Європейському співтоваристві в цілому.

В контексті юридичної євроінтеграції необхідно звернути увагу на те, що процес вдосконалення адміністративно-правого режиму забезпечення інформаційної безпеки передбачає обов'язкове дотримання наступних умов:

- адміністративно-правовий режим забезпечення інформаційної безпеки повинно бути несуперечливим і відповідати внутрішнім потребам забезпечення суверенітету (у контексті агресії Російської Федерації) та динамічного та сталого розвитку держави;

- з метою такого вдосконалення необхідно співвіднести з правовими нормами, концептами та інститутами НАТО.

Цілком очевидно, що аналогічне погодження та відповідність, що веде до інтернаціоналізації правових форм, здійснюються за допомогою таких юридично-технічних засобів, як рецепція, уніфікація, гармонізація і імплементація.

Важливо відзначити, що переважна більшість процесів, що конституюють нові способи комунікацій і діяльності, в тому числі, щодо забезпечення інформаційної безпеки, передбачають формування та правове оформлення принципово нових інститутів адміністративного права на основі рішення гносеологічно складних фундаментальних завдань і методологічних підходів як раз за рахунок формування нових адміністративно-правових режимів, що яскраво проявляється в сфері інформаційної безпеки. Доцільно зауважити, що в Україні на сьогодні сформувалася єдина законодавча та нормативна правова

база у сфері забезпечення інформаційної безпеки, в якій чітко простежуються основні напрями державної політики в цій галузі.

Активізація законодавчого процесу щодо формування адміністративно-правового інституту режиму інформаційної безпеки збігається з періодами розвитку національної економіки та необхідністю захисту критичної інформаційної інфраструктури. Це свідчить про стійкість взаємозв'язку державного управління та державного регулювання економікою і інституту режиму інформаційної безпеки та викликає необхідність вивчення даного інституту з позиції його адміністративно-правового застосування в умовах окремих господарюючих суб'єктів.

В умовах гібридної війни адміністративно-правові режими стають необхідним елементом державного регулювання інформаційних процесів, ефективним інструментом проведення заходів забезпечення інформаційно-психологічної безпеки особистості. Доктрина інформаційної безпеки України є каталізатором для застосування даного інституту, оскільки реалізується в процесі здійснення комплексу політичних, організаційних, соціально-економічних, правових, інформаційних, дипломатичних і інших заходів.

На наш погляд, адміністративно-правові режими є затребуваними інститутами адміністративно-правового регулювання в цілому, що дозволяє у межах даної проблематики виділити адміністративно-правовий режим інформаційної безпеки. Особливості його встановлення становлять значну проблему з огляду на різні рівні забезпечення інформаційної безпеки та правовий режим техніко-технологічних засобів інформаційно-комунікаційних систем. Активізація правотворчого процесу щодо формування адміністративно-правового інституту режиму інформаційної безпеки викликана необхідністю забезпечення територіальної цілісності та суверенітету, що зумовило інтерес правників до забезпечення інформаційної безпеки держави, суспільства та особи.

Динаміка основних фінансово-економічних показників інформаційної сфери формує потребу в створенні ефективної правової бази розвитку IT-

індустрії (ріст попиту на аналітиків інформаційної безпеки (17,9%), з огляду на збереження комерційних таємниць, документації, клієнтських баз), побудови якісно інших теоретичних моделей державного регулювання забезпечення інформаційної безпеки на принципі поєднання публічних і приватних інтересів [271, с. 10]. Слід зазначити, що в науковій літературі, як правило, регулювання відносин безпеки в інформаційній сфері розглядається виключно з точки зору теорії адміністративного права як моделі конкуренції публічних і приватних інтересів. З погляду на дослідження Національного інституту стратегічних досліджень при Президентів України «Проблеми впровадження сучасних стандартів інформаційної безпеки в умовах становлення національної системи кібербезпеки України» [64], доцільно відзначити, що структура та природа адміністративно-правового режиму забезпечення інформаційної безпеки досі розглядається як система правових обмежень приватних інтересів підприємств і організацій, які надають інформаційні послуги, на користь публічних інтересів. Практика показує суттєві недоліки існуючої моделі як основи для правової моделі регулювання технічної складової інформаційної безпеки, що вимагає конструювання нової парадигми адміністративно-правового управління на основі відкритої моделі адміністративно-правового управління.

Адміністративно-правовий режим забезпечення інформаційної безпеки повинен інтегрувати в собі сфери розвитку та безпеки, тим самим забезпечуючи своєрідне зрощення політики безпеки та розвитку, що, як показує досвід США та Великої Британії, призводить до перерозподілу фінансових потоків на потреби розвитку інформаційної інфраструктури та її техніко-юридичного регулювання. Інформаційна безпека передбачає не тільки захист людей від критичних ситуацій і поширених загроз, але й забезпечення свобод, які є сутністю життя та можливостей реалізації своїх устремлінь.

Розвиток і імплементація у національне законодавство нормативних вимог Європейського Союзу та НАТО щодо використання диспозитивних форм і методів адміністративно-правового регулювання направлених на забезпечення інформаційної безпеки зацікавленими суб’єктами, сприяє створенню нової

юридичної конструкції адміністративно-правого механізму забезпечення інформаційної безпеки, де заміна класичних директивних форм адміністративно-правового регулювання повинна слугуватиме досягненню двох цілей – забезпечення основних інформаційних прав и свобод фізичних і юридичних осіб і одночасно стимулювання цифрової економіки.

Розглянув особливості адміністративно-правового режиму забезпечення інформаційної безпеки доцільно зробити висновки:

- адміністративно-правовий режим забезпечення інформаційної безпеки є комплексною юридичною категорією, дослідження якої доцільно здійснювати на міждисциплінарній основі із застосуванням методології інформаційного права з акцентуванням уваги на інформаційному, комунікаційному та синергетичному аспектах, оскільки за цільовим призначенням адміністративно-правовий режим забезпечення інформаційної безпеки є складною, відкритою, незавершеною інформаційно-комунікаційною системою, що забезпечують правове регулювання процедурних (включаючи інформаційні) відносин, через систему адміністративних процедур які характеризуються високим ступенем динамічності у регулюванні, завдяки новітніх програмних компонентам і засобам комунікації, охоплюючи різні за обсягом напрями – забезпечення інформаційної безпеки особи, суспільства та держави;

- адміністративно-правовий режим забезпечення інформаційної безпеки створює особливі процесуальні відносини або процесуальні правила, які відповідають основним принципам правового регулювання інформаційно-правових відносин, є складною категорію, що складається з матеріальних і процесуальних елементів співвідношення яких залежить від того в якій мірі ліквідація загроз, що розглядається, врегульовано спеціальними адміністративними та техніко-юридичними нормами, застосування якої системи стандартів технічного регулювання, найбільшою мірою відповідає конкретному випадку та основній меті інформаційної безпеки – захисту від негативного впливу шкідливих чинників на свідомість та психологічний стан людини (засобів масової інформації, Інтернету та інших інформаційних

джерел); на технічні та програмні засоби інформаційно-комунікаційних систем; на національні інформаційні ресурси;

- особливості адміністративно-правових режимів забезпечення інформаційної безпеки об’єктів критичної інформаційної інфраструктури розкриваються через механізм саморегулювання за участю публічно-правових суб’єктів, встановлення балансу інтересів, у контексті правового регулювання реалізації законних інтересів власників критичної інформаційної інфраструктури, що випливає з адміністративних і інших публічних правовідносин утворюючи баланс публічних і приватних інтересів;

- особливість організаційно-правового забезпечення адміністративно-правового режиму забезпечення інформаційної безпеки обумовлює застосування технічних стандартів інформаційної безпеки прийнятих у ЄС і НАТО, які сформульовані в результаті виявлення типових (повторюваних) правових випадків щодо уніфікації техніко-юридичних норм, які регламентують порядок діяльності суб'єктів забезпечення інформаційної безпеки, у контексті правових відносин, що виникають з адміністративних та інших публічних правовідносин, з метою орієнтації положень на однаковість процедури усунення загроз у інформаційно-телекомунікаційних системах, що інтерпретується як особливий спосіб юрисдикційного усунення прогалин у праві та протиріч, що виникають під час діяльності особи та суб'єктів господарської діяльності у інформаційній сфері.

Висновки до розділу 2

Дослідивши структура механізму адміністративно-правого забезпечення інформаційної безпеки в Україні доцільно зробити наступні висновки.

Конструювання механізму правового регулювання забезпечення інформаційної безпеки має здійснюватися відповідно до цілі правового регулювання. Ціль правового регулювання, будучи частиною управлінського процесу та результатом правової політики, передбачає об'єднання певних

правових засобів для досягнення правового результату, визначаючи при цьому природу механізму правого регулювання.

Ціль правового регулювання інформаційної безпеки залежить від правової політики держави в інформаційній сфері, визначається суб'єктами, що здійснюють нормативно-правове регулювання інформаційної безпеки з урахуванням свободи розсуду та розвитку приватної ініціативи юридичних і фізичних осіб власників інформаційних систем.

Вирішальну роль у формуванні цілей правового регулювання забезпечення інформаційної безпеки, що мають транснаціональний характер, грають норми визначені в актах міжнародних та наднаціональних організацій ЄС і НАТО. Мета правового регулювання, поставлена відповідно до принципів розвитку інформаційного суспільства для досягнення необхідного результату, вимагає органічного поєднання публічно-правових і приватноправових засобів в структурі механізму правового регулювання. Це дозволить врахувати підприємницький характер інформаційної діяльності та інформаційної безпеки.

Елементами механізму правого регулювання забезпечення інформаційної безпеки є: засоби нормативного характеру, що включають норми права, які містяться в законодавстві, норми-принципи, норми «м'якого права», норми саморегулювання власників інформаційних систем, звичаї, правила інформаційної безпеки інформаційних систем; етичні кодекси та правила: юридичні факти як підстави виникнення інформаційних правовідносин в сфері інформаційної безпеки; правовідносини, що виникають в системах забезпечення інформаційної безпеки (зобов'язальні, контрольні, наглядові та корпоративні правовідносини); акти застосування та реалізації права.

Принципи інформаційного права та принципи побудови адміністративно-правового механізму забезпечення інформаційної безпеки співвідносяться як ціль та засіб її досягнення. До числа базових принципів побудови правового механізму забезпечення інформаційної безпеки відносяться: принцип економічної ефективності; принцип використання правових засобів відповідно до мети правового регулювання; принцип пріоритетного використання

приватноправових засобів; принцип використання публічно-правових засобів виключно для цілей антикризового управління інформаційними системами.

Державне управління в сфері забезпечення інформаційної безпеки полягають у створенні умов для гармонійного розвитку національної інформаційної інфраструктури, для реалізації конституційних прав і свобод людини та громадянина, законних інтересів особи, суспільства та держави у національному інформаційному просторі, у отриманні інформації та користування нею фізичними та юридичними особами з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності України, політичної, економічної та соціальної стабільності, в забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

Адміністративно-правове регулювання забезпечення інформаційної безпеки є система нормативно-правових актів, що регламентує стабільне функціонування національних інформаційно-комунікаційної інфраструктури, інформаційних ресурсів, інформаційного простору, реалізацію інформаційних прав і свобод людини та громадянина, законні інтереси суспільства та держави, міжнародних зобов’язань України в інформаційній сфері, протидію екстремізму, сепаратизму, внутрішнім та зовнішнім загрозам національним інтересам визначеним Конституцією та законодавством України.

Адміністративно-правове регулювання забезпечення інформаційної безпеки є сукупність закріпленої в законодавстві системи заходів і прийомів, спрямованих на забезпечення безпечної діяльності в інформаційному просторі що динамічно розвивається, фізичних і юридичних осіб, сприятливої для інновацій, інвестицій, яка забезпечує населенню високий рівень життя і економічний прогрес. Тому зміст адміністративно-правового регулювання інформаційних відносин вимагає обґрунтування у межах адміністративно-правового режиму інформаційної безпеки.

Первинним системоутворюючим елементом забезпечення інформаційної безпеки є правовий суб'єкт, який співіснує з правовими особами (фізичними і

юридичними), взаємодіючи між собою на підставі суб'єктно-комунікативних взаємозв'язків. Суб'єкт забезпечення інформаційної безпеки – явище багатоаспектне, визначається чинним правом і іншими соціальними нормами в тій мірі, в якій дані соціальні норми знаходять свою закінченість в чинному праві, представляючи сукупність укладених в спеціальну юридичну форму правових якостей захисту інформаційних прав і свобод людини та публічного управління у сфері інформаційної безпеки.

Суб'єкт забезпечення інформаційної безпеки – це індивідуальна або колективна особа, потенційний учасник конкретних інформаційних відносин, що володіє правосуб'єктністю, яка за своїми особливостями є носієм суб'єктивних юридичних прав і обов'язків, бере участь у правовідносинах, відповідно цілям і завданням забезпечення інформаційної безпеки, докладаючи певні зусилля для досягнення позитивного інтересу, використовуючи засоби та методи адміністративно-правого регулювання.

Система суб'єктів забезпечення інформаційної безпеки – цілісна, синергетична сукупність елементів, що перебувають у обумовлених функціями забезпечення інформаційної безпеки суспільних відносинах, об'єднаних сферою інтересів і потреб, що відображають правові характеристики адміністративно-правових засобів регулювання, зміст і елементи правового статусу суб'єктів, які беруть участь у відносинах, регульованих нормами інформаційного права, системними за змістом.

Для забезпечення інформаційної безпеки характерна багаторівнева система суб'єктів, заснована на принципі єдності та диференціації. Перший рівень – це три групи суб'єктів: фізичні і юридичні особи, публічно-правові утворення, складові підсистеми цих суб'єктів. Інші рівні (структурні елементи зазначених підсистем) це різного роду спеціальні суб'єкти адміністративного права, поділ яких обумовлено диференціацією предмета відповідного правового регулювання.

Адміністративно-правовий режим забезпечення інформаційної безпеки є комплексною юридичною категорією, дослідження якої доцільно здійснювати

на міждисциплінарній основі із застосуванням методології інформаційного права з акцентуванням уваги на інформаційному, комунікаційному та синергетичному аспектах, оскільки за цільовим призначенням адміністративно-правовий режим забезпечення інформаційної безпеки є складною, відкритою, незавершеною інформаційно-комунікаційною системою, що забезпечують правове регулювання процедурних (включаючи інформаційні) відносин, через систему адміністративних процедур які характеризуються високим ступенем динамічності у регулюванні, завдяки новітніх програмних компонентам і засобам комунікації, охоплюючи різні за обсягом напрями – забезпечення інформаційної безпеки особи, суспільства та держави.

Особливості адміністративно-правових режимів забезпечення інформаційної безпеки розкриваються через механізм саморегулювання за участю публічно-правових суб’єктів, встановлення балансу інтересів, у контексті правового регулювання реалізації законних інтересів власників критичної інформаційної інфраструктури, що випливає з адміністративних і інших публічних правовідносин утворюючи баланс публічних і приватних інтересів.

Особливість організаційно-правового забезпечення адміністративно-правового режиму інформаційної безпеки обумовлює застосування технічних стандартів інформаційної безпеки прийнятих у ЄС і НАТО, які сформульовані в результаті виявлення типових (повторюваних) правових випадків і уніфікації техніко-юридичних норм, які регламентують порядок діяльності суб'єктів забезпечення інформаційної безпеки, у контексті відносин, що виникають з адміністративних та інших публічних правовідносин, з метою орієнтації положень на однаковість процедури усунення загроз у інформаційно-телекомунікаційних системах і в національному інформаційному просторі, що інтерпретується як особливий спосіб юрисдикційного усунення прогалин у праві та протиріч, що виникають під час діяльності особи та суб'єктів господарської діяльності у інформаційній сфері.

У науковій літературі регулювання відносин безпеки в інформаційній

сфері розглядається з точки зору теорії адміністративного права як моделі конкуренції публічних і приватних інтересів. Структура та природа адміністративно-правового режиму забезпечення інформаційної безпеки досі розглядається як система правових обмежень приватних інтересів підприємств і організацій, які надають інформаційні послуги, на користь публічних інтересів. Практика показує недоліки існуючої моделі як основи для правової моделі регулювання інформаційної безпеки, що вимагає конструювання нової парадигми адміністративно-правового управління на основі відкритої моделі адміністративно-правового управління.

Адміністративно-правовий режим забезпечення інформаційної безпеки повинен інтегрувати в собі сфери розвитку та безпеки, тим самим забезпечуючи своєрідне зрощення політики безпеки та розвитку, що, як показує досвід США та Великої Британії, призводить до перерозподілу фінансових потоків на потреби розвитку інформаційної інфраструктури та її техніко-юридичного регулювання. Інформаційна безпека передбачає не тільки захист людей від критичних ситуацій і поширених загроз, але й забезпечення свобод, які є сутністю життя та можливостей реалізації своїх устремлінь.

РОЗДІЛ 3

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

На початку XXI століття діяльність держави у правовій галузі суттєво та динамічно змінилася, проте зміни, які відбулися до теперішнього часу, не отримали свого системного, комплексного науково-теоретичного аналізу, в сфері інформаційної безпеки. Особливо це стосується питань гарантій та захисту прав і свобод громадян, підтримання інформаційної безпеки особи, яка стає самостійним предметом державної політики.

Нинішній розвиток людини та суспільства невипадково характеризується освоєнням правового способу життєдіяльності, як одного з найбільш оптимальних ціннісних інститутів виживання та досягнення благополуччя. Очевидно, що забезпечення інформаційної безпеки на сучасному етапі просто неможливе без активного впливу з боку права як системи норм і правової системи суспільства. У складних переплетеннях сфери безпеки і права, як нормативного регулятора, народжується нова форма інформаційної безпеки, яка надає суспільній життєдіяльності прогнозованість, стійкість, адекватність і визначеність. Саме інформаційна безпека, як стан захищеності інтересів особи, прав і свобод людини, суспільства та держави дозволяє бачити і оцінювати нормальне функціонування політико-економічної системи держави. А механізм інформаційної безпеки надає інформаційній сфері додаткові гарантії життєздатності та нормальне функціонування.

Будучи регульованою системою, механізм інформаційної безпеки сам потребує нормативно-правового впливу. Взаємодія складових ланок (елементів) механізму інформаційної безпеки втілюється в правових відносинах, в особливому суб'єктно-об'єктному середовищі, у кореспондуючих зв'язках, а реалізація здійснюється в актах вольового характеру, що застосовуються з

урахуванням місця та ролі тієї чи іншої ланки системи забезпечення інформаційної безпеки.

При цьому, на думку Л. Й. Аведян, інтереси інформаційної безпеки України вимагають розглядати інтеграцію інформаційної інфраструктури країни у європейську систему за напрямами:

- підтримка досліджень і розробок у галузі інформації та комунікації; вплив на їхнє спрямування та заохочення до поширення технічних знань і можливостей в економіці; сприяння обміну технологіями між лабораторіями та фірмами, запровадження нововведень на ринках;

- побудова та вдосконалення інформаційної інфраструктури, контроль за її діяльністю, побудова глобальних систем комунікації і дослідження впливу систем на міжнародні, національні та приватні пріоритети;

- збереження порушеної новими технологіями рівноваги між чотирма основними інформаційними цінностями: конфіденційністю інформації, інформацією як суспільним благом, інформацією як товаром, інформацією як невіддільним компонентом існування держави (необхідне відновлення рівноваги та встановлення нових засобів контролю для нових інформаційних відносин);

- недоторканність приватного життя, конфіденційність інформації персонального характеру на різних рівнях у різних сферах державного управління та в приватному секторі;

- створення урядової політики в галузі інформації та комунікації [272, с. 2]. Реалізація зазначених напрямів робить необхідним пошук рішення проблем забезпечення інформаційної безпеки в комплексному використанні політичних, економічних, моральних, психологічних механізмів, що спонукають до досягнення взаємної відповідальності особи, суспільства та держави для забезпечення стабільності суспільних відносин з метою створення необхідних передумов для функціональної безпеки національного інформаційного простору.

Інформаційна безпека розглядається як нормативно-регламентований і

організаційно забезпечений юридичними засобами стан захищеності інформаційної системи держави, що характеризується на нашу думку, цілою сукупністю різних правових показників, які відображають: рівень злочинності в цілому і окремих видах, у тому числі в сфері інформаційних технологій; якість і кількість правового матеріалу; рівень правової свідомості різних категорій населення; рівень розвитку правової культури різних соціальних груп; наявність прогалин, суперечливості чи неефективності правових актів, що регламентують інформаційну сферу суспільних відносин; економічну забезпеченість і соціальну популярність застосування правових норм правоохоронними органами та посадовими особами у сфері інформаційних технологій; розвиток правових і не правових тенденцій в сфері інформаційних технологій, якість і кількість криміналізації суспільних відносин в інформаційній сфері; рівень свавілля працівників судових, правоохоронних і інших органів та посадових осіб, покликаних вирішувати юридичний конфлікт у сфері інформаційної безпеки; недоліки у виконанні судових рішень.

Необхідно зауважити, що на думку М. В. Коваліва, С. С. Єсімова, Р. І. Крамар, Р. М. Скриньковського, досвід країн-членів ЄС показує, що розвиток правової держави залежить від рівня розвитку громадянського суспільства, а інтереси особи зі сфери державного функціонування все більше переміщуються у сферу активізації громадянського суспільства. Водночас, існує певна протидія, що носить двосторонній характер: по-перше – держава не делегує свої повноваження громадянському суспільству, не маючи відповідного нормативно-правового механізму реалізації; по-друге – громадянське суспільство не проявляє зацікавленості у процесі аутсорсингу. Це негативно позначитися на функціонуванні організаційно-правового механізму забезпечення прав і свобод людини та громадянина, у першу чергу в інформаційній сфері [273, с. 6002].

Зазначений підхід знайшов відображення у Переліку індикаторів розвитку інформаційного суспільства та Методиці формування індикаторів розвитку інформаційного суспільства де рівень інформаційної безпеки (пункти

29) визначається на основі порівняльного аналізу інформації національних та міжнародних урядових організацій та консалтингових компаній [274; 275].

Ефективність діяльності органів, що забезпечують інформаційну безпеку (Міністерство інформаційної політики, Державна служба спеціального зв'язку та захисту інформації України, Національна поліція) залежить від: якості здійснюваного аналізу загальної соціальної ситуації, тобто розуміння всіх факторів та умов життєдіяльності суспільства; від своєчасності та адекватності вжиття заходів виявлення та запобігання правопорушень; моніторингу (контролю) загального стану інформаційної безпеки інформаційних систем, обумовленого характером і природою загроз, що виходять від внутрішніх і зовнішніх джерел небезпек; вибором юридичних (легальних) засобів забезпечення [276].

У зв’язку з цим доцільно доповнити Положення про інтегровану інформаційно-пошукову систему органів внутрішніх справ щодо обліку подій у сфері інформаційної безпеки (*Додаток И*).

На нашу думку, з урахуванням динамічного розвитку національного інформаційного простору, нормативно-правове регулювання інформаційної безпеки повинно складатися з двох рівнів і включати:

- комплексну нормативно-правову регламентацію процесів управління забезпеченням інформаційної безпеки, закріплену в актах законодавства, підготовлених на основі всебічного наукового розгляду і обґрунтування стадій, методології та системи відносин, що складаються в процесі адміністративно-правового регулювання діяльності суб'єктів забезпечення у визначеній сфері;

- нормативно-правову регламентацію діяльності Національної поліції за окремими напрямами забезпечення інформаційної безпеки, що складається з галузевих нормативно-правових актів Національної поліції, документів інших органів (наприклад, Міністерства інформаційної політики України, Державної служби спеціального зв'язку та захисту інформації України [277]), що забезпечують реалізацію державних функцій у сфері інформаційної безпеки.

Взаємозв'язок законодавчого та відомчого нормативного регулювання

доцільно розділити відповідно до характеристики об'єкта управління та предмета управлінсько-правового регулювання, що відповідатиме на питання, які правовідносини поза управлінських меж оформляються (або повинні оформлятися) за допомогою нормативних приписів. Відправним при цьому є теоретичне уявлення про предмет регулювання як про суспільні відносини, що складають об'єкт управлінського впливу, який здійснюється за допомогою правових норм, втілених у законодавстві. Вони адресуються учасникам управлінських відносин, визначають межі можливої та належної поведінки, впливаючи, тим самим, на волю та свідомість відповідних суб’єктів.

На сьогоднішній день рівень відомчого регулювання складають спільні нормативно-правові акти МВС України (Національна поліція, Департамент інформатизації Міністерства внутрішніх справ України), Міністерства інформаційної політики України, Міністерства оборони України, Державної служби спеціального зв'язку та захисту інформації України, Національної комісії, що здійснює державне регулювання у сфері зв’язку та інформатизації [278]. У процесі відомчого адміністративно-правового регулювання забезпечення інформаційної безпеки повинна бути вибудувана певна ієрархія індивідуальних інтересів. У цьому зв'язку можна визначити наступні групи інтересів: первинні інтереси, пов'язані із забезпеченням життєдіяльності індивідів; вторинні інтереси, продиктовані забезпеченням необхідного рівня функціонування інформаційно-комунікаційних систем; інтереси, спрямовані на реалізацію соціальних перспектив фізичної і юридичної особи в інформаційній сфері.

Комплексну нормативно-правову регламентацію процесів управління забезпеченням інформаційної безпеки доцільно здійснювати за рахунок систематизації і уніфікації адміністративного законодавства в галузі інформаційної безпеки за допомогою кодифікованого нормативного правового акта, який встановить вихідні засади адміністративно-публічного забезпечення інформаційної безпеки в Україні.

В якості такого нормативно-правового акту можна запропонувати

спільний наказ Міністерства інформаційної політики України, МВС України, Державної служби спеціального зв'язку та захисту інформації України «Про основи адміністративно-правового забезпечення інформаційної безпеки в Україні», в якому доцільно вирішити такі завдання:

- створення однакового понятійно-категорійного апарату, який гранично ясно та чітко розкриває сутність, структуру та зміст інформаційної безпеки у сфері адміністративно-правового регулювання в Україні, співвідносно з виробленими юридичною наукою категоріями;

- створення в Україні єдиної системи спеціалізованих органів виконавчої влади та виконавчо-розпорядчих органів місцевого самоврядування, які наділяються повноваженнями з питань забезпечення виконання загальнообов'язкових умов та вимог інформаційної безпеки, пов'язаними з безпосереднім втручанням даних органів в адміністративно-господарську, організаційно-розпорядчу та іншу діяльність фізичних і юридичних осіб;

- систематизація та уніфікація адміністративно-правових методів діяльності органів виконавчої влади та виконавчо-розпорядчих органів місцевого самоврядування, які будуть забезпечувати виконання загальнообов'язкових умов і вимог інформаційної безпеки при безпосередньому втручанні в адміністративно-господарську, організаційно-розпорядчу та іншу діяльність фізичних та юридичних осіб;

- формальне визначення функцій адміністративно-правового забезпечення інформаційної безпеки, що передаються органам місцевого самоврядування органами державної влади України в якості аутсорсингу;

- створення оптимальної системної моделі взаємодії методом планомірної та послідовної зміни окремих системних якісних показників на підставі скорочення можливості прямого втручання у сферу технологічних і цивільно-правових відносин, що зумовлює відповідні зміни у колі та характері суспільних відносин, які охороняються адміністративним правом.

Необхідно зауважити, що національне право має нормативно-правові акти, які, у вказаній послідовності, визначають основні аспекти взаємодії

державних органів у боротьбі зі злочинністю. Як приклад, можна розглядати: Інструкцію про взаємодію правоохоронних і інших державних органів України у боротьбі із злочинністю; Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків [279; 280].

За допомогою відомчого юридичного інструментарію формується специфічний правовий режим, що дозволяє суб'єктам найбільш повно та послідовно реалізовувати визначені компетенцією повноваження, що обов'язково має здійснюватися у межах суспільних інтересів. З одного боку, створюється свого роду ієрархія повноважень суб'єктів, з цієї точки зору – їх значимість для забезпечення інформаційної безпеки, з іншої – своєрідна черговість у їх реалізації.

Забезпечення інформаційної безпеки характеризуються особливим способом регулятивного впливу на суспільні відносини, що відзначається позитивними наслідками. Специфіка використання окремих адміністративно-правових засобів в праворегулюючому процесі багато в чому зумовлена особливістю юридичної конструкції, яка визначає інтенсивність виразу в кожному з стимулюючих, компенсаційних, гарантуючих засад. Правові засоби, покликані досягати поставлену мету, виконують дві основні функції: компенсаційну та стимулюючу. У них яскраво проявляються цілі і завдання адміністративно-правового регулювання у сфері інформаційної безпеки, юридична природа та соціальне призначення. Крім названих, вони виконують, як і всякий інший правовий засіб, забезпечувальну, виховну, комунікативну, мотиваційну, ціннісно-орієнтаційну функції та функцію соціального контролю.

Необхідно зауважити, що закон України «Про центральні органи виконавчої влади» та Положення про МВС України не дають чіткої відповіді чи МВС України, будучи центральним органом виконавчої влади, що здійснює, відповідно до закону України «Про Національну поліцію», функції у галузі забезпечення інформаційної безпеки, наділено повноваженнями з видання нормативно-правових актів міжгалузевого характеру, спрямованих на

регулювання суспільних відносин в економічній, адміністративно-політичній, соціальній та інших сферах, з метою вирішення завдань забезпечення інформаційної безпеки [158; 160; 312, с. 76-78]. Вказану прогалину доцільно усунути шляхом внесення доповнення у Положення про Міністерство внутрішніх справ (*Додаток К*) та у Регламент Міністерства внутрішніх справ України (*Додаток Л*), що, співзвучно з дослідженням К. Л. Богайяука «Функції публічного адміністрування в органах Національної поліції України: поняття та класифікація» та соціологічним опитуванням (*Додаток Б*) [281].

В умовах євроінтеграції, яка закріпила принципово нові відносини у політичній та економічній сферах, нові принципи співвідношення публічних і приватних інтересів, зміну ідеології та практики правового регулювання, зростає роль правового інституту адміністративної відповідальності у вирішенні конфліктів, що виникають в складний період переходу до правової держави, становлення громадянського суспільства та гібридної війни.

С. С. Єсімов зазначає, що концепція юридичної відповідальності суб'єктів публічного управління за порушення інформаційного законодавства в юридичній науці та практиці розроблена недостатньою мірою, немає її системного правового регулювання, не повною мірою сформовано категоріальний апарат, що відповідає європейським реаліям [282, с. 83].

Події останніх місяців, пов'язані з проведенням масованих кібератак і блокуванням роботи державних органів, комерційних банків, об'єктів життєзабезпечення яскраво продемонстрували вразливість і незахищеність інформаційного середовища, неефективність правової основи системи забезпечення інформаційної безпеки. Законодавство про адміністративну відповідальність відверто «не встигає» за стрімкими процесами розвитку інформаційного суспільства, що негативно впливає на стан правопорядку в суспільстві [283, с. 202].

У цих умовах особливої актуальності набуває наукове осмислення ролі та значення адміністративної відповідальності, покликаної, поряд з іншими видами юридичної відповідальності, забезпечувати вимоги інформаційної

безпеки у функціональному значенні та здійснювати профілактичну функцію.

Для забезпечення інформаційної безпеки застосовуються практично всі види заходів адміністративного примусу (попередження, припинення, стягнення) та заходи забезпечення провадження у справі про адміністративне правопорушення. Деякі вчені виділяються в якості особливого виду примусу адміністративно-правові відновлювальні заходи примусу, які застосовуються для того щоб відновити вихідний порядок, колишній стан речей, а також з метою відшкодування заподіяної шкоди [284, с. 84].

Але в механізмі адміністративно-правового регулювання суспільних відносин в інформаційній сфері особлива роль належить заходам адміністративного припинення. Заходи адміністративного припинення є самостійною різновидом заходів адміністративного примусу, володіють усіма ознаками останніх. Заходи адміністративного припинення застосовуються значно більшим числом органів державної влади та їх посадових осіб, ніж інші заходи адміністративного примусу, деякими громадськими формуваннями, які отримали ці повноваження у порядку аутсорсингу. Крім того, ці заходи є дуже численними та різноманітними за функціональним (цільовим) призначенням.

Заходи адміністративного попередження можна класифікувати за метою використання на дві категорії: заходи, здійснювані з метою попередження, припинення та покарання за вчинення адміністративних правопорушень всередині держави, і заходи, що здійснюються в надзвичайних обставинах (воєнний стан) або з метою попередження зовнішніх загроз національній, в тому числі інформаційній безпеці. При цьому заходи, які здійснюються з метою попередження правопорушень, носять превентивний характер. У мирний час різноманіття заходів адміністративно-правового та інформаційного характеру дозволяє гнучко та точково реагувати на протиправну дійсність у інформаційній сфері.

Децентралізація та недостатньо чітка ієрархія в діяльності суб'єктів забезпечення інформаційної безпеки в Україні, таких як Кабінет Міністрів України, Міністерство інформаційної політики України, Міністерство юстиції

України, МВС Україні, відсутність єдиних нормативно-правових основ забезпечення інформаційної безпеки окрім Доктрини інформаційної безпеки та Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах затверджених постановою Кабінету Міністрів України 29 березня 2006 року № 373, детального законодавчого регламентування відповідних адміністративних процедур, сприяє зловживанню при застосуванні заходів адміністративного примусу.

Проблема об'єктивного підбору засобів і інструментів для досліджуваної сфери регулювання, належного стимулювання діючих в даній сфері суб'єктів, забезпечення дії механізмів, обумовлених природою сфери інформаційної безпеки повинна вирішуватися відповідним органом регулювання на основі діючих адміністративно-правових принципів.

Специфіка фактичних і формально-юридичних підстав та правила призначення адміністративного покарання, адміністративно-процесуальний порядок застосування, принципи законності, публічності, індивідуалізації, повноти і об'єктивності дослідження обставин справи, презумпції невинності, гуманності, справедливості, рівності громадян перед законом, поваги гідності особи повинні враховуватися органами адміністративної юрисдикції при застосуванні заходів адміністративного примусу в сфері забезпечення інформаційної безпеки. Дані принципи важливі та знаходять відображення у чинній судовій практиці.

Однак, слід враховувати публічний характер мети держави щодо забезпечення інформаційної безпеки, яка випливає з імперативних норм встановлених правових режимів, і не завжди баланс та рівновага публічній і приватній сторін інформаційних правовідносин співвідноситься з завданнями держави щодо виконання зазначеної мети. Ряд правових інститутів, створених, в тому числі, для підтримки названого балансу, наприклад, інститут Уповноваженого Верховної Ради України з прав людини, швидше бореться з виявленими зловживаннями державною владою, ніж сприяє оптимізації державного управління в сфері інформаційної безпеки.

Різні сфери суспільного життя диктують імператив диференційованого підходу до правового регулювання. Сфера безпеки пов'язана з обмежувально-забороннними нормами права, що носять обов'язковий характер. Свобода інформаційних відносин може бути обмежена державою з метою забезпечення інформаційної безпеки. Примусові заходи, що не стимулюють, не заохочують, створені для виконання державних цілей, покликані задовольняти державний інтерес. Загрозам інформаційної безпеки сприяє нерозвиненість соціально-інформаційної інфраструктури та невирішеність проблем державно-правової системи забезпечення правопорядку, недооцінка органами виконавчої влади можливостей адміністративного примусу в інформаційній сфері. Забезпечення правопорядку базується на заходах адміністративного примусу, відповідні правові прогалини можуть витікати з невідповідності даних заходів меті забезпечення інформаційної безпеки держави.

Доцільно враховувати багатозначність завдань забезпечення інформаційної безпеки: як загальну превенцію, так й стимулювання та підтримку суб'єктів інформаційної діяльності – власників об’єктів критичної інформаційної інфраструктури. Вирішення цих завдань буде сприяти підвищенню ефективності діяльності суб'єктів досліджуваної діяльності з протидії загрозам інформаційній безпеці.

У першу чергу підлягають усуненню такі недоліки: відсутність законодавчої систематизації адміністративно-примусових заходів у сфері інформаційної безпеки; відсутність контролю за своєчасністю та відповідністю їх застосування (виражається у відсутності відповідного уповноваженого контрольно-наглядового органу виконавчої влади ведучого відповідну діяльність); відсутність органу виконавчої влади з функціями прогностично-рекомендаційного характеру в сфері інформаційної безпеки, що узагальнює правозастосовну діяльність за всіма заходами примусу та надає рекомендації з оптимізації та уніфікації (можливо, колегіальний дорадчий орган).

Системна організація законодавчого забезпечення інформаційної безпеки також необхідна, оскільки чітка регламентація норм, що носять імперативний

характер, завжди обумовлювала правопорядок в будь-якій сфері суспільних відносин. Необхідно перейти від довгострокової стратегії в сфері інформаційної безпеки (Доктрина інформаційної безпеки України) до проекту Закону «Про основи інформаційної безпеки», прийняття якого послужить основою вдосконалення відповідних адміністративно-примусових заходів.

Н. П. Борттник і С. В. Пєтков зазначають, що незважаючи на зростаючу зацікавленість до інформаційної безпеки, її специфічні особливості, достатня складність і висока вартість засобів технічного захисту, відсутність чітких критеріїв захищеності інформації тощо, обмежують практичне вирішення проблеми. Тому, для вирішення проблеми інформаційної безпеки, необхідна не проста розробка приватних механізмів захисту, а передусім розробка ідеології, методологічних основ захисту, які б могли враховувати не тільки перспективи розвитку інформаційних технологій і систем, але й перспективи розвитку спеціальних засобів протидії загрозам [285, с. 36].

Адміністративно-правове регулювання діяльності Державної служби спеціального зв’язку та захисту інформації України та Національної поліції у сфері інформаційної безпеки являє собою сукупність взаємопов'язаних і взаємодіючих адміністративно-правових засобів, за допомогою яких забезпечується результативний правовий вплив на суспільні відносини. Доцільно відзначити що законодавство про адміністративні правопорушення передбачає підстави та порядок застосування контрольно-наглядових та відновлювальних заходів у взаємозв'язку з додатковими, компенсаційними та превентивними засобами забезпечення інформаційної безпеки.

У вказаному контексті внесення у КУпАП процесуальних норм забезпечення порядку застосування контрольно-наглядових і відновлювальних заходів у взаємозв'язку з компенсаційними та превентивними засобами забезпечення інформаційної безпеки недоцільно.

Існуючий КУпАП прийнятий у 1984 році, був покликаний відображати в основному потреби державного управління, пріоритетом якого було забезпечення інтересів політичного режиму, що зумовило ігнорування

кодифікації законодавства про адміністративну відповідальність, особливо його процесуальної складової. Саме встановлення норм про адміністративну відповідальність було предметом регулювання не законодавця, а органів державного управління, згадуючи форми та методи захисту прав громадян при застосуванні владою заходів адміністративного покарання (перек. з рос. Т. П.) [286]. На нашу думку, з урахуванням зазначеного, положення порядку застосування контрольно-наглядових і відновлювальних заходів повинні бути відображені у адміністративно-процесуальному кодексі, як, наприклад, у відповідному кодексі Республіки Білорусь [287].

Наша думка, у цьому питанні, збігається з дослідженнями О. В. Банчука щодо адміністративно-деліктного законодавства Естонії – країни ЄС та учасниці Організації Північноатлантичного договору [288, с. 209-211].

В Україні за останні роки відслідковується стала тенденція до зниження адміністративного тиску на громадян, відходу від каральної функції та зміщення акценту на профілактику адміністративних правопорушень, які впливають на стан злочинності [289]. Водночас за даними Т. С. Пашковської є ріст незаконного втручання в діяльність інформаційних систем [290].

Необхідність наукової розробки проблеми незаконних втручань в діяльність інформаційних систем диктується зростаючою небезпекою останніх, зумовленої станом інформаційного середовища та її впливом на функціональну безпеку [291, с. 655].

Однак, можливості кримінально-правових засобів у справі забезпечення інформаційної безпеки не можуть бути безмежними. Особливо це стосується безпеки об’єктів критичної інформаційної інфраструктури, як складової інформаційної безпеки. Свідчення тому – застосування законодавства про протидію інформаційним правопорушенням і злочинам.

Питома вага зареєстрованих інформаційних злочинів у загальній структурі злочинності мінімальна і не відображає реальних масштабів їх суспільної небезпеки та поширеності. Деякі злочини, наприклад, несанкціоноване втручання в інформаційно-комунікаційну систему, згідно з

даними кримінальної статистики, взагалі обчислюються одиницями [292; 293]. Одна з причин незастосування кримінально-правових норм, як вказувалося в юридичній літературі, полягає у відсутності чітких меж між злочином і проступком, що одночасно свідчить про відсутність законодавчого встановлення меж кримінальної відповідальності. У цьому вбачається негативний момент як кримінального, так і адміністративного права.

На думку Я. В. Задорожної, між кримінальним правом та адміністративним правом існує тісний зв’язок у питаннях дослідження способу вчинення протиправного діяння як ознаки об’єктивної сторони правопорушення. Тобто представники адміністративного права, здійснюючи дослідження практично-прикладного характеру щодо способу вчинення адміністративного проступку, завжди звертаються до теорії кримінального права, що має як позитивні (наприклад, спрощує науково-дослідну діяльність певної особи), так і негативні наслідки (не сприяє розвитку вчення про склад адміністративного проступку в межах науки адміністративного права) [294, с. 14]. Дослідження В. О. Навроцького [295, с. 36-37] показують, що ця проблема зберігає свою практичну гостроту, оскільки значна частина помилок при застосуванні як кримінального, так і адміністративного законодавства у сфері інформаційної безпеки, пов'язана якраз з нечіткими уявленнями поліцейських щодо лінії, яка відмежовує злочини від адміністративних правопорушень.

Труднощі полягають ще й у тому, що дана проблема вимагає не тільки та не стільки роздільного (або навіть порівняльного) вивчення кримінального і адміністративного законодавства, скільки комплексного його дослідження, тобто одночасного вивчення норм, причому в тісному (по суті нерозривному) взаємозв'язку. Однак, це не входить у предмет нашого дослідження.

На думку автора, статті Кодексу України про адміністративні правопорушення: 41-3, 82 -7, 163-5, 163-6, ч. 1 ст. 164-14, ч. 1 ст. 164-17, ч. 2 ст. 166 -9, ч. 3 ст. 166-13, 166-21, 185-13, 188-5, 188-7, 188-11, 188-13, 188-14, 188-15, 188-18, ч. 5 ст. 188-19, 188-32, 188-36, 188-37, 188-46, 188-48

передбачають адміністративну відповідальність за порушення порядку обігу та використання інформації є правопорушеннями в сфері інформаційної безпеки [283, с. 205].

Необхідно зауважити, що при кримінологічному дослідженні інформаційну безпеку необхідно розглядати, виходячи з її структури, як полі ергатичну систему, яка має ієрархічну будову. У неї входять, залежно від функції і цілей управління, різні підсистеми, побудовані за ознаками підпорядкування, що відрізняються: за кількістю людей – операторів, які обслуговують підсистему; за ступенем дискретності участі людини в процесі управління та виду зв'язку керуючого суб'єкта з об'єктом управління [296, с. 80-81]. Вивчаючи інформаційну безпеку як єдине функціональне ціле і роль окремих моно або полі ергатичних ланок у забезпеченні інформаційної безпеки, по-перше, теорія збагачується знаннями, наявними в технічних дисциплінах і науках про людину та її діяльність, по-друге, при цьому виявляються найменш надійні ланки у системі інформаційної безпеки, що робить профілактичну роботу більш предметною.

Ефективність організації та забезпечення інформаційної безпеки Національною поліцією визначається відповідністю об'єктивному соціальному призначенню, що знаходить вираження у відповідних критеріях і показниках, а всі інші, відносно самостійні затратно-економічні, технологічні та технічні критерії ефективності повинні розглядатися як підлеглі соціальним цілям, поза якими їх застосування втрачає сенс і може навіть перешкоджати досягненню таких цілей.

Основні критерії оцінки організації діяльності Національної поліції у сфері інформаційної безпеки повинні включати: баланс організаційно-структурних та функціональних параметрів; адекватність (кількісно і якісно) ресурсної забезпеченості; професійний вишкіл і готовність кадрового корпусу; змістовне наповнення функцій управління, відповідне потребам організаційної та правоохоронної практики; якість організаційної та правоохоронної діяльності, яка задовольняє потреби суспільства та відповідає пріоритетам

захисту прав, свобод і життя людей.

Оцінка повинна висвітлювати процес виконання одного з головних завдання аналітичної функції управлінської діяльності Національної поліції у сфері інформаційної безпеки, що включає опис об'єкта оцінки, виявлення відхилень і збоїв в його функціонуванні, пояснення причин і умов, що їх породжують, обґрунтування управлінських рішень і заходів.

Виконання аналітичної функцією цього завдання може бути забезпечене в єдності двох напрямів: підвищення рівня методологічного та інформаційного забезпечення даної проблеми, розширення спектра сучасних наукових методів та інформаційних технологій, що використовуються при її вирішенні, підвищення професійного рівня кадрів, зайнятих в даній інформаційно-аналітичній сфері [297, с. 84-85].

Достовірність і обґрунтованість отриманих результатів підтверджуються використанням фундаментальних наукових положень різних галузей знання, ідей і принципів методології системного підходу, що довела свою універсальність і плідність у багатьох дослідженнях проблем управління Національною поліцією, аргументацією обґрунтованих висновків і пропозицій, їх логічністю та несуперечливістю, підкріплених також відповідним емпіричним матеріалом на підставі нових підходів до методології аналізу у гуманітарних дослідженнях, тобто, структурного підходу.

На думку С. Повторевої, структура об’єднує кількісні конструкції, в яких основні відношення між елементами підпорядковано певним правилам, що визначені системою оцінки [298, с. 191].

Зазначені вище аспекти доцільно включити до Системи оцінки діяльності Національної поліції. Однак, у відкритому доступі Системи оцінки діяльності Національної поліції не має. Але керівник Національної поліції С. М. Князєв заявляв про запровадження у 2018 році нової системи оцінки діяльності поліції, що відповідає Концепції інформатизації Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра

внутрішніх справ України, на 2016-2020 роки [299; 300],

На сучасному етапі розвитку європейського інформаційного простору основний напрям забезпечення інформаційної безпеки формується у межах комплексних програм профілактики правопорушень. Будучи об'єктивно необхідною функцією органів Національної поліції, профілактика у сфері забезпечення інформаційної безпеки тривалий час не мала широкого поширення в їх діяльності. Пояснення повільного розвитку профілактики у системі органів Національної поліції, на нашу думку, зумовлено наступними причинами: відсутність достатніх засад для здійснення профілактики в умовах соціально-політичних, правових та економічних реформ; поширеність думки про автоматичне вирішення проблем інформаційної безпеки в міру зміни технологій; перевага у забезпеченні інформаційної безпеки методів примусу; правова неврегульованість профілактичної діяльності; негативне ставлення поліції до профілактики, недооцінка її можливостей і дієвості в порівнянні з традиційними видами діяльності – адміністративно та кримінально юрисдикційними; відсутність внутрішніх передумов організаційного та кадрового характеру.

Сучасна практика профілактики правопорушень у сфері інформаційної безпеки не відповідає світовим підходам її організації з цілого ряду принципових позицій. В Україні профілактикою правопорушень, у межах своєї компетенції, займаються, в основному, правоохоронні органи. Відсутня відповідна галузь законодавства, яка регулює особливі відносини у сфері профілактики правопорушень для органів державної влади та місцевого самоврядування, неурядових організацій, структур бізнесу і інститутів громадянського суспільства. Існують лише окремі елементи державної системи профілактики правопорушень із незначною участю громадських об'єднань і населення. У Плані заходів на 2018 рік з реалізації Стратегії кібербезпеки України питання профілактики не піднімаються [185].

Відсутні комплексні дослідження проблем профілактики у зазначеній сфері суспільних відносин, побудованих на сучасних методологічних підходах

(з урахуванням методології запропонованої О. І. Остапенком і В. В. Денисенком в аспекті адміністративної деліктології, методів меметики, запропонованих фахівцями Вищої школи поліції Польщі, у поєднанні з поглядами В. К. Грищука на перспективну юридичну відповідальність та В. Л. Ортинського щодо новітніх методів дослідження адміністративно-правових явищ [301; 302; 303; 304, с. 38-41; 305, с. 211-212; 306]). Процес формування концептуальних основ профілактики правопорушень у сфері забезпечення інформаційної безпеки не забезпечений комплексом заходів правового та інформаційного характеру. Розробка системи попередження правопорушень у сфері забезпечення інформаційної безпеки, яка відповідає сучасним вимогам інформаційної безпеки, повинна, на нашу думку:

- базуватися на досвіді, накопиченому в Європейському Союзі у галузі розробки та реалізації загальнодержавних комплексних програм попередження правопорушень і правової просвіти населення;

- здійснюватися у межах єдиного методологічного підходу дослідження проблем інформаційної безпеки, з урахуванням кримінології та деліктології на основі аналітичної юриспруденції;

- спиратися на продуману соціальну політику при оптимальному поєднанні цілеспрямованих зусиль держави з ініціативами різних інститутів громадянського суспільства.

Прагнення входження в Європейський Союз створює реальні передумови для формування системи державних заходів впливу на стан і динаміку профілактичних процесів у сфері інформаційної безпеки. Практика організації попереджувальної діяльності, що склалася в країнах Європейського союзу, будується за принципами:

- профілактика правопорушень є важливою складовою національної державної політики;

- системності та комплексного підходу до організації превентивної діяльності, що передбачає використання всіх методів впливу на стан інформаційної безпеки. Дієздатна соціальна система впливу на злочинність

зменшує у людей бажання вчинити злочин і можливість реалізації злочинних задумів, забезпечує припинення злочинної діяльності, повинна будуватися на принципах:

- синергетійного підходу до організації механізму виховного впливу всіх суб'єктів профілактичної діяльності у сфері попередження девіантної поведінки людини з урахуванням віктимологічної профілактики, активного залучення громадян до роботи з підвищення пильності у сфері інформаційно-психологічної безпеки;

- адекватного матеріального, ідеологічного, кадрового, інформаційного, наукового забезпечення даної діяльності;

- постійної зміни системи впливу на організацію забезпечення інформаційної безпеки, в контексті змін соціальної та кримінальної реальності.

Дослідження європейського досвіду організації профілактики правопорушень у сфері забезпечення інформаційної безпеки дозволяє виділити загальні тенденції в розвитку систем профілактики: пріоритет профілактики в політиці протидії правопорушенням, тобто створення умов, щоб людина не вступила на злочинний шлях, а якщо вступила та зійшла з нього (добровільно чи з примусу) не опинилась там знову; розробка та прийняття законів, державних і локальних програм; організація єдиного координуючого органу; участь у міжнародному співробітництві у зазначеній сфері через систему інститутів громадянського суспільства; активна регіональна політика профілактики правопорушень; широке використання в процесі організації профілактичної діяльності, яка реалізується в різних видах на всіх рівнях соціального управління; програмно-цільового планування, яке є важливим інструментом реалізації державної політики та дозволяє організувати чітку, всебічно обґрунтовану роботу з досягнення поставлених цілей і завдань.

Виходячи з досвіду країн Європейського Союзу (В. Л. Ортинський, С. С. Єсімов [307; 308]), профілактичний вплив права на систему соціальних відносин у сфері забезпечення інформаційної безпеки стимулює соціально корисну поведінку людей, закріплює такі суспільні відносини, які за своєю

суттю забезпечують особисту безпеку.

Важливою нормативно-правовою основою профілактики правопорушень, в тому числі щодо забезпечення інформаційної безпеки, може стати прийняття закону «Про основи державної системи профілактики правопорушень», беручи до уваги відповідні нормативні акти держав, які мають однакову технологічну систему організації і загальні для країн Європейського Союзу принципи профілактики правопорушень – Литви, Латвії, Естонії (*Додаток М*). Доцільно зауважити, що наші дослідження знайшли, у певній мірі, підтвердження у ході соціологічного опитування працівників (Державної служби спеціального зв'язку та захисту інформації України, Національної поліції, представників вищих навчальних закладів, які мають відношення до забезпечення інформаційної безпеки (*Додатки Б-М*).

Дослідження шляхів підвищення ефективності адміністративно-правового забезпечення інформаційної безпеки дає змогу зробити висновки:

- інформаційна безпека розглядається як нормативно-регламентований і організаційно забезпечений юридичними засобами стан захищеності національного інформаційного простору, що характеризується сукупністю правових показників, які відображають: рівень злочинності в цілому та окремих видах; якість і кількість правового матеріалу; рівень правової свідомості та правової культури різних соціальних груп; наявність прогалин, суперечливості чи неефективності правових актів, що регламентують інформаційну безпеку, економічну забезпеченість і соціальну популярність застосування правових норм; розвиток правових і не правових тенденцій; якість і кількість криміналізації суспільних відносин; рівень свавілля працівників правоохоронних і інших органів, зобов'язаних вирішувати юридичний конфлікт, що виник; недоліки у виконанні судових рішень; рівень захищеності посадових осіб правоохоронних органів, що вирішують юридичні конфлікти та виконують прийняті рішення;

- ефективність діяльності органів, що забезпечують інформаційну безпеку, залежить: від якості аналізу загальної соціальної ситуації (всіх

факторів та умов життєдіяльності); від своєчасності та адекватності вжитих заходів щодо виявлення та запобігання правопорушень, моніторингу (контролю) загального стану інформаційної безпеки, обумовленого характером і природою загроз, що виходять від внутрішніх і зовнішніх джерел небезпек, вибором юридичних (легальних) засобів забезпечення;

- комплексну нормативно-правову регламентацію процесів управління забезпеченням інформаційної безпеки доцільно здійснювати за рахунок систематизації і уніфікації адміністративного законодавства за допомогою кодифікованого нормативного правового акта, який встановить вихідні засади адміністративно-правового забезпечення інформаційної безпеки в Україні;

- відомчий юридичний інструментарій формує специфічний правовий режим, що дозволяє найбільш повно та послідовно реалізовувати визначені компетенцією повноваження, з обов'язковим врахуванням суспільних інтересів, створюючи ієрархію повноважень, однієї з точки зору – їх значимість для забезпечення інформаційної безпеки, з іншої – своєрідну черговість у їх реалізації;

- ефективність організації та забезпечення інформаційної безпеки Національною поліцією визначається відповідністю об'єктивному соціальному призначенню, що знаходить вираження у відповідних критеріях і показниках, а всі інші, відносно самостійні затратно-економічні, технологічні та технічні критерії ефективності повинні розглядатися як підлеглі соціальним цілям, поза якими їх застосування втрачає сенс і може перешкоджати їх досягненню;

- основні критерії оцінки діяльності Національної поліції у сфері інформаційної безпеки повинні включати: баланс організаційно-структурних та функціональних параметрів; адекватність (кількісно і якісно) ресурсної забезпеченості; професійний вишкіл і готовність кадрового корпусу; змістовне наповнення функцій управління, відповідне потребам організаційної та правоохоронної практики; якість організаційної та правоохоронної діяльності, яка задовольняє потреби суспільства та відповідає пріоритетам захисту прав і свобод людини та громадянина.

Висновок до розділу 3

Дослідження шляхів підвищення ефективності адміністративно-правового забезпечення інформаційної безпеки в Україні дозволяють зробити наступні висновки:

- взаємодія суб'єктів забезпечення інформаційної безпеки щодо являє собою відкриту систему дворівневої конструкції з централізовано-сегментарним поділом владної компетенції між її основними елементами – Міністерством інформаційної політики України, Державною службою спеціального зв’язку та захисту інформації України, Національною поліцією де законодавчі параметри є визначальними і обумовлюють подобу структурно-владних форм, що конкретизують характеристики адміністративно-правового режиму предметно-конкретним змістом з реалізації техніко-юридичних норм, втілену в інституційно-логічну організацію;

- аналіз сутності загальних і специфічних рис взаємодії Міністерства інформаційної політики України, Державної служби спеціального зв’язку та захисту інформації України, Національної поліції щодо інформаційної безпеки розглядає взаємодію з максимальним наближенням до системних індивідуальних особливостей спрямованих на пріоритетне дослідження основоположних динамічних і статичних закономірностей цілісності, стійкості, ефективності як системи в цілому, так і її елементів, виявляючи еволюцію, об'єктивний стан і тенденції розвитку внутрішньо і зовнішньо системних взаємозв'язків і взаємозалежності, консолідуючи владні ресурси щодо спільних функцій у сфері інформаційної безпеки на основі інтегративних форм законодавчого та відомчого закріплення прямих і зворотних взаємозв'язків;

- ефективність діяльності Національної поліції, що забезпечують інформаційну безпеку, залежить: від якості аналізу загальної соціальної ситуації; від своєчасності та адекватності вжитих заходів щодо виявлення та запобігання правопорушень, моніторингу (контролю) загального стану інформаційної безпеки, обумовленого характером і природою загроз, що

виходять від внутрішніх і зовнішніх джерел небезпек, вибором юридичних (легальних) засобів забезпечення;

- комплексну нормативно-правову регламентацію процесів управління забезпеченням інформаційної безпеки доцільно здійснювати за рахунок систематизації і уніфікації адміністративного законодавства за допомогою кодифікованого нормативно-правового акта, який встановить вихідні засади адміністративно-публічного забезпечення інформаційної безпеки в Україні;

- важливою нормативно-правовою основою профілактики правопорушень, в тому числі у сфері забезпечення інформаційної безпеки, може стати прийняття закону «Про засади державної системи профілактики правопорушень», беручи до уваги положення закладені у нормативні акти держав, які мають однакову технологічну систему організації та загальні для країн ЄС принципи профілактики правопорушень.

ВИСНОВКИ

Проведене дослідження адміністративно-правового механізму забезпечення інформаційної безпеки в Україні дозволило прийти до основних наукових висновків, що мають значення для розвитку адміністративно-правового забезпечення інформаційної безпеки особи, суспільства та держави. Традиційно дослідження безпеки займаються ідентифікацією та реакцією на загрозливі дії для безпеки держави. Сьогодні опорні точки теорії безпеки зміщуються до інформаційної сфери. В умовах інформаційної війни, яку розв'язала Росія, стають помітні зміни в режимі забезпечення інформаційної безпеки. У такій ситуації Україна зустрічається з досить серйозними загрозами для соціально-економічної сфери загалом і окремих її галузей та підприємств, що вимагає активної розробки і ефективної реалізації такого науково-практичного інституту, як «діяльність із забезпечення інформаційної безпеки» через систему заходів адміністративного характеру. Це сприяло обґрунтуванню та вирішенню завдань, які мають важливе наукове і прикладне значення. У результаті сформульовано низку висновків, пропозицій та рекомендацій:

1. Інформаційну безпеку слід розглядати як систему суспільних відносин, що виражає зв'язок між інтересами особи, суспільства та держави в сфері інформації та правового забезпечення їхнього захисту, що охоплює стан захищеності інформаційного простору, інформації і інформаційних ресурсів держави, інформаційно-телекомунікаційної інфраструктури від можливих внутрішніх і зовнішніх загроз. Інформаційна безпека як система має значення з двох позицій: інформація, комунікація та знання – це елементи, процеси та цілі, які стоять серед основоположних прав і свобод, тому мають враховуватися при визначенні відносин між державою та громадянином; при опрацюванні специфічних вимог щодо захисту та впливу, які пов'язані з інформаційною технікою. Нормативно-правова природа інформаційної безпеки забезпечує її функціонування як інституційної організаційної та правової системи регулювання правовідносин, які є частиною системи суспільних відносин,

обумовлені змістом правових, техніко-технологічних, економічних політичних і культурних зв’язків, що характеризують суспільну та державну системи. Інформаційна безпека виступає об’єктом правового захисту. Правові засоби забезпечення інформаційної безпеки є провідним фактором захисту національних інтересів в цій сфері, а їхнє застосування визначається: оптимізацією балансу відносин між правом суб'єктів інформаційних відносин на отримання інформації та правом на встановлення обмежень таких відносин з боку інших осіб щодо відомостей, володарями яких вони є; розробкою та реалізацією правових заходів захисту інформації, доступ до якої повинен обмежуватися правовими підставами в процесі захисту інформаційних ресурсів. Правове забезпечення ліквідації загроз і ризиків у сфері інформаційної безпеки є основним фактором структурування, формування, розглядається як законотворча діяльність, спрямована на запобігання шкоди інтересам особи, суспільства та держави в інформаційній сфері.

2. Вихідні методологічні засади дослідження поняття та змісту інформаційної безпеки базуються на системі загальнонаукових і спеціальних юридичних методів: системного, синергетичного, герменевтичного, історико-правового, порівняльно-правового, формально-юридичного і інших. Системний метод дає змогу розглянути інформаційну безпеку, дві її складові – техніко-технологічну та гуманітарну – з позиції конструювання технологій управління завдяки правовому регулюванню, значенню критерію цілісності як основної властивості системного утворення; трирівневої структури як системного закону. Герменевтичний підхід дає змогу розширити кордони предметного поля інформаційної безпеки, синергетичний метод дозволить розглянути захист безпеки як складне функціональне явище, історико-правовий і порівняльно-правовий методи дозволять розкрити процес забезпечення інформаційної безпеки в єдності з ціннісною свідомістю суспільства. З позиції методології права парадигма інформаційної безпеки має структуру, яку утворюють: методологія правозастосування, законодавство України та міжнародні норми інформаційної безпеки, систематика адміністративного права, норми

адміністративного права, адміністративно-правові відносини, юридична кваліфікація адміністративно-правових відносин, тлумачення норм права, механізм застосування закону, державна правова політика в галузі інформаційної безпеки, культура і етика застосування законодавства, що встановлює обмеження прав і свобод людини та громадянина, стратегія та тактика діяльності суб'єктів забезпечення інформаційної безпеки, ефективність застосування законодавства, експертиза актів відомчого нормативно-правового забезпечення інформаційної безпеки.

3. Нормативно-правове регулювання інформаційної безпеки носить багатопрофільний характер і практично кожна галузь права має свій предмет в регулюванні інформаційних відносин. Адміністративне право в механізмі правового регулювання інформаційної безпеки займає ключове місце. Обумовлено це тим, що суб'єкти забезпечення мають адміністративно-правовий статус, у зв'язку з чим норми адміністративного права визначають порядок взаємовідносин з органами державної влади та управління, регламентують контрольно-наглядову, дозвільну і юрисдикційну діяльність в сфері інформаційної безпеки. Ціль правового регулювання інформаційної безпеки залежить від правової політики держави в інформаційній сфері. Вона визначається суб'єктами, що здійснюють нормативно-правове регулювання інформаційної безпеки з урахуванням свободи розсуду та розвитку приватної ініціативи юридичних і фізичних осіб, власників інформаційних систем і інформаційних ресурсів. Перспективою інформаційно-правової політики є формування відповідного інституційно-правового порядку, що сприяє досягненню державою бажаного результату, пов'язаного з національними інтересами в інформаційній сфері. Правова основа забезпечення інформаційної безпеки в теоретичному сенсі є сукупністю різних за юридичною силою права норм, що відносяться до різних галузей і відображають сутність процесів, що відбуваються в сфері забезпечення інформаційної безпеки, складаючи єдину систему, що сприяє вдосконаленню механізму правового забезпечення інформаційної безпеки, направленого на підтримання балансу інтересів особи,

суспільства та держави в інформаційній сфері завдяки вдосконаленню законодавчих засад.

Адміністративно-правові засоби регулювання інформаційної безпеки визначають сутність змісту відповідного напряму правового регулювання, тому саме якість цих правових засобів може поліпшити ефективність державного впливу на інформаційну сферу. Адміністративно засоби мають різноплановий характер і залежно від цілеспрямованості виконують різні функції в цій сфері. Уся система адміністративно-правових засобів, незалежно від функціональної і цільової спрямованості, покликана покращувати якість правового регулювання та робити інформаційну безпеку більш ефективною.

4. Механізм правового регулювання – це система спеціально-юридичних засобів, організованих послідовним чином, спрямованих на регулювання суспільних відносин певного виду. Конструювання механізму правового регулювання забезпечення інформаційної безпеки має здійснюватися відповідно до цілі правового регулювання. Ціль правового регулювання, будучи частиною управлінського процесу та результатом правової політики, передбачає об'єднання певних правових засобів для досягнення правового результату, визначаючи при цьому природу механізму правого регулювання. Вирішальну роль у формуванні цілей правового регулювання забезпечення інформаційної безпеки, що мають транснаціональний характер, відіграють норми, визначені в актах міжнародних та наднаціональних організацій ЄС і НАТО. Елементами механізму правого регулювання забезпечення інформаційної безпеки є: засоби нормативного характеру, що включають норми права, які містяться в законодавстві, норми-принципи, норми «м’якого права», норми саморегулювання власників інформаційних систем, звичаї, правила інформаційної безпеки інформаційних систем; етичні кодекси та правила: юридичні факти як підстави виникнення інформаційних правовідносин в сфері інформаційної безпеки; правовідносини, що виникають в системах забезпечення інформаційної безпеки (зобов'язальні, контрольні, наглядові та корпоративні правовідносини); акти застосування та реалізації права. Принципи інформаційного права та принципи побудови

адміністративно-правового механізму забезпечення інформаційної безпеки співвідносяться як ціль та засіб її досягнення. До числа базових принципів побудови правового механізму забезпечення інформаційної безпеки відносяться: принцип економічної ефективності; принцип використання правових засобів відповідно до мети правового регулювання; принцип пріоритетного використання приватноправових засобів; принцип використання публічно-правових засобів виключно для цілей антикризового управління інформаційними системами.

5. Державне управління в сфері забезпечення інформаційної безпеки полягає у створенні умов для гармонійного розвитку національної інформаційної інфраструктури, для реалізації конституційних прав і свобод людини та громадянина, законних інтересів особи, суспільства та держави у національному інформаційному просторі, у отриманні інформації та користування нею фізичними та юридичними особами з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності України, політичної, економічної та соціальної стабільності, в забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва. Основними функціями державного управління щодо забезпечення інформаційної безпеки є: прогнозування в сфері загроз інформаційній безпеці, яке проявляється в прийнятті концепцій і стратегій забезпечення інформаційної безпеки; планування переліку заходів та послуг в сфері забезпечення інформаційної безпеки; створення ситуаційних центрів різного рівня; контроль (який проявляється через здійснення, аналіз зібраної інформації, вжиття заходів щодо запобігання порушенням законності, шкідливих наслідків, шкоди); матеріально-технічне забезпечення інформаційної безпеки (розвиток інфраструктури, в тому числі через залучення іноземних інвестицій); кадрове забезпечення.

Адміністративно-правове регулювання забезпечення інформаційної безпеки є системою нормативно-правових актів, що регламентує стабільне функціонування національних інформаційно-комунікаційної інфраструктури,

інформаційних ресурсів, інформаційного простору, реалізацію інформаційних прав і свобод людини та громадянина, законні інтереси суспільства та держави, міжнародних зобов'язань України в інформаційній сфері, протидію екстремізму, сепаратизму, внутрішнім та зовнішнім загрозам національних інтересів, визначеним Конституцією та законодавством України. Адміністративно-правове регулювання забезпечення інформаційної безпеки безпосередньо пов'язане з державним управлінням та державним регулюванням у визначеній сфері, є сукупністю закріпленої в законодавстві системи заходів і прийомів, спрямованих на забезпечення безпечної діяльності в інформаційному просторі, що динамічно розвивається, фізичних і юридичних осіб, сприятливої для інновацій, інвестицій, яка забезпечує населенню високий рівень життя і економічний прогрес. Тому зміст адміністративно-правового регулювання інформаційних відносин вимагає обґрунтування у межах адміністративно-правового режиму інформаційної безпеки

6. Первинним системоутворюючим елементом забезпечення інформаційної безпеки є правовий суб'єкт, який співіснує з правовими особами (фізичними і юридичними), об'єднаних суб'єктно-комунікативних взаємозв'язками. Суб'єкт забезпечення інформаційної безпеки – явище багатоаспектне, визначається чинним правом і іншими соціальними нормами настільки, наскільки ці соціальні норми знаходять свою завершеність в чинному праві, становлячи сукупність укладених в спеціальну юридичну форму правових якостей захисту інформаційних прав і свобод людини та публічного управління у сфері інформаційної безпеки. Суб'єкт забезпечення інформаційної безпеки – це індивідуальна або колективна особа, потенційний учасник конкретних інформаційних відносин, який володіє правосуб'єктністю, яка за своїми особливостями є носієм суб'єктивних юридичних прав і обов'язків, бере участь у правовідносинах, відповідно до цілей і завдань забезпечення інформаційної безпеки, докладаючи певні зусилля для досягнення позитивного інтересу, використовуючи засоби та методи адміністративно-правого регулювання. Система суб'єктів забезпечення інформаційної безпеки – цілісна, синергетична сукупність елементів, що

перебувають у обумовлених функціями забезпечення інформаційної безпеки суспільних відносинах, об'єднаних сферою інтересів і потреб, що відображають правові характеристики адміністративно-правових засобів регулювання, зміст і елементи правового статусу суб'єктів, які беруть участь у відносинах, регульованих нормами інформаційного права, системними за змістом. Для забезпечення інформаційної безпеки характерна багаторівнева система суб'єктів, заснована на принципі єдності та диференціації. Перший рівень – це три групи суб'єктів: фізичні і юридичні особи, публічно-правові утворення, складові підсистеми цих суб'єктів. Інші рівні (структурні елементи зазначених підсистем) – це різного роду спеціальні суб'єкти адміністративного права, поділ яких обумовлено диференціацією предмета відповідного правового регулювання. Доцільне створення спеціального органу для координації діяльності власників критично важливої інформаційної інфраструктури.

7. Адміністративно-правовий режим забезпечення інформаційної безпеки є комплексною юридичною категорією, дослідження якої доцільно здійснювати на міждисциплінарній основі із застосуванням методології інформаційного права з акцентуванням уваги на інформаційному, комунікаційному та синергетичному аспектах, оскільки за цільовим призначенням адміністративно-правовий режим забезпечення інформаційної безпеки є складною, відкритою, незавершеною інформаційно-комунікаційною системою, що забезпечує правове регулювання процедурних (включаючи інформаційні) відносин через систему адміністративних процедур, що характеризуються високим ступенем динамічності у регулюванні, завдяки новітнім програмним компонентам і засобам комунікації, охоплюючи різні за обсягом напрями – забезпечення інформаційної безпеки особи, суспільства та держави. Особливості адміністративно-правових режимів забезпечення інформаційної безпеки розкриваються через механізм саморегулювання за участю публічно-правових суб'єктів, встановлення балансу інтересів у контексті правового регулювання реалізації законних інтересів власників критично важливої інформаційної інфраструктури, що випливає з публічних правовідносин, утворюючи баланс публічних і приватних

інтересів. Особливість організаційно-правового забезпечення адміністративно-правового режиму інформаційної безпеки обумовлює застосування технічних стандартів інформаційної безпеки, прийнятих у ЄС і НАТО, які сформульовані в результаті виявлення типових правових випадків і уніфікації техніко-юридичних норм, що регламентують порядок діяльності суб'єктів забезпечення інформаційної безпеки у контексті відносин, що виникають з адміністративних та інших публічних правовідносин, з метою орієнтації положень на однаковість процедури усунення загроз у інформаційно-телекомунікаційних системах, в національному інформаційному просторі, що інтерпретується як особливий спосіб юрисдикційного усунення протиріч, що виникають під час діяльності особи та суб'єктів господарської діяльності у інформаційній сфері.

Структура та природа адміністративно-правового режиму забезпечення інформаційної безпеки досі розглядається як система правових обмежень приватних інтересів підприємств і організацій, які надають інформаційні послуги, на користь публічних інтересів. Практика показує недоліки існуючої моделі як основи для правової моделі регулювання інформаційної безпеки, що вимагає конструювання нової парадигми адміністративно-правового управління на основі відкритої моделі правового управління.

8. Підвищення ефективності адміністративно-правового забезпечення інформаційної безпеки в Україні можливе на основі реалізації комплексу правових заходів, до яких відносяться: чітке відображення в праві і державних інститутах орієнтації на поєднання публічних і приватних економічних інтересів в інформаційній сфері; постійне та послідовне використання всіх правозахисних механізмів і процедур для подолання конфліктів в інформаційній сфері; підвищення правового рівня свідомості та діяльності державних службовців, представників всіх гілок і рівнів влади, населення країни. Як інструмент державного впливу на адміністративні процеси в сфері забезпечення інформаційної безпеки слід більш активно використовувати взаємодію суб'єктів забезпечення інформаційної безпеки, що є відкритою системою дворівневої конструкції з централізовано-сегментарним поділом владної компетенції між її

основними елементами: Міністерством інформаційної політики України, Державною службою спеціального зв'язку та захисту інформації України, Національною поліцією, іншими суб'єктами забезпечення інформаційної безпеки, визначених Доктриною інформаційної безпеки України, де законодавчі параметри є визначальними і обумовлюють подобу структурно-владних форм, що конкретизують характеристики адміністративно-правового режиму предметно-конкретним змістом з реалізації техніко-юридичних норм, втілену в інституційно-логічну організацію. Аналіз сутності загальних і специфічних рис взаємодії Міністерства інформаційної політики України, Державної служби спеціального зв'язку та захисту інформації України, Національної поліції, інших суб'єктів забезпечення інформаційної безпеки, визначених Доктриною інформаційної безпеки України, розглядає взаємодію з максимальним наближенням до системних індивідуальних особливостей, спрямованих на пріоритетне дослідження основоположних динамічних і статичних закономірностей цілісності, стійкості, ефективності як системи в цілому, так і її елементів, виявляючи еволюцію, об'єктивний стан і тенденції розвитку внутрішньо- і зовнішньосистемних взаємозв'язків і взаємозалежності, консолідуючи владні ресурси щодо спільних функцій у сфері інформаційної безпеки на основі інтегративних форм законодавчого та відомчого закріплення прямих і зворотних взаємозв'язків. Важливою нормативно-правовою основою профілактики правопорушень, в тому числі у сфері забезпечення інформаційної безпеки, може стати прийняття закону «Про засади державної системи профілактики правопорушень», беручи до уваги положення, закладені у нормативні акти держав, які мають однакову технологічну систему організації інформаційної безпеки та загальні для країн ЄС принципи профілактики правопорушень.

9. Запропоновано зміни і доповнення до норм чинного законодавства, зокрема: до Законів України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державно-приватне партнерство», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про телекомунікації»; до постанови Кабінету Міністрів України «Про затвердження

Положення про Міністерство внутрішніх справ України», наказів МВС України: «Про затвердження Положення про Інтегровану інформаційно-пошукову систему МВС України», «Про затвердження Регламенту Міністерства внутрішніх справ», до структури законопроекту «Про основи державної системи профілактики правопорушень».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16.09.2014 р. № 1678-VII / Відомості Верховної Ради України. 2014. № 40. Ст. 2021.

2. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р. URL. http://zakon3.rada.gov.ua/laws/show/386-2013-%D1%80 (дата звернення 01.07.2019).

3. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 році». Київ: НІСД, 2017. 928 с.

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII / Відомості Верховної Ради України. 2017. № 45. Ст. 403.

5. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17-23.

6. Гончар С. Ф., Леоненко Г. П., Юдін О. Ю. Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури. Вісник Національного університету «Львівська Політехніка». 2014. № 806. С. 34-39.

7. Винер Н. Кибернетика, или управление и связь в животном и машине. Пер. с англ. И. В. Соловьева и Г. Н. Поварова; 2-е изд. Москва: Наука; 1983. 344 с.

8. Глушков В. М. Про кибернетику как наука. Кибернетика, мышление, жизнь. Москва: Мысль, 1964. 511 с.

9. Системний аналіз інформаційних процесів: Навчальний посібник. В. М. Варенко, І. В. Братусь, В. С. Дорошенко, Ю. Б. Смольніков, В. О. Юрченко. Київ: Університет «Україна», 2013. 203 с.

10. Іванов В. Г., Іванов С. М., Карасюк В. В. Сучасні інформаційні системи і технології: конспект лекцій. Харків: Національний юридичний університет імені Ярослава Мудрого, 2014. 347 с.

11. Телешун С. О., Рейтерович І. В. Інформаційно-аналітична діяльність в державному управлінні : навчально-методичні матеріали. Київ: НАДУ, 2013. 36 с.

12. Гапеєва О. Л. Історіографічний аналіз проблеми інформаційної безпеки на пострадянському просторі. Historical and Cultural Studies. 2016. Vol. 3. № 1. P. 37-41.

13. Цимбалюк В. С., Бабінська А. В. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. Адміністративне право і процес. 2014. № 2 (8). URL. http://applaw.knu.ua/index.php/arkhiv-nomeriv/2-8-2014/item/284-pravove-rehulyuvannya-informatsiynoyi-bezpeky-v-ukrayini-problemy-teoriyi-ta-praktyky-tsymbaliuk-v-s-baby (дата звернення 01.09.2018).

14. Кочубей Л.О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі. Наукові записки Інституту політичних і етнонаціональних досліджень імені І. Ф. Кураса. 2015. Вип. 3. С. 220-237.

15. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. 30.04.2014. URL. http://troubleshooter.com.ua/ru/inform-bezopasnost/52-informatsijna-bezpeka-v-sistemi-zabezpechennya-natsionalnoji-bezpeki (дата звернення 01.09.2018).

16. Єсімов С. С. Шляхи удосконалення нормативно-правового регулювання в сфері інформаційної безпеки. Наукові записки Львівського університету бізнесу та права. 2013. Вип. 11. С. 73-76.

17. Мороз Н. С. Сутність інформації в контексті загальних принципів інформаційної безпеки. Вісник Національного університету «Львівська політехніка». Юридичні науки. 2016. № 845. С. 137-142.

18. Ярема О. Г., Єсімов С. С.. Предмет правового забезпечення

інформаційної безпеки в інформаційному праві. Науковий вісник Львівського державного університету внутрішніх справ. 2016. № 2. С.244-252.

19. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017 URL. http://zakon3.rada.gov.ua/laws/show/47/2017 (дата звернення 02.07.2019).

20. Валюшко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту: дис. … канд. політичних наук: 23.00.04. Київ, 2018. 210 с.

21. Семенюк О. Баланс життєво важливих інтересів особистості, суспільства та держави в інформаційній сфері. Юридична Україна. 2015. № 10-12. С. 65-69.

22. Довгань О. Д. Теоретико-правові основи забезпечення інформаційної безпеки України: автореф. дис. … д-ра юрид. наук: спец. 12.00.07. Київ, 2016, 46 с.

23. Конституція України : Закон України від 08.06.1996 р. № 254к/96-ВР / Відомості Верховної Ради України. 1996. № 30. Ст. 141.

24. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI / Відомості Верховної Ради України. 2010. № 34. Ст. 481.

25. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI / Відомості Верховної Ради України. 2011. № 32. Ст. 314.

26. Про внесення змін до деяких законів України щодо доступу до публічної інформації у формі відкритих даних : Закон України від 09.04.2015 р. № 319-VIII / Відомості Верховної Ради України. 2015. № 25. Ст. 192.

27. Про друковані засоби масової інформації (пресу) в Україні : Закон України від 16.11.1992 р. № 2782-XII / Відомості Верховної Ради України. 1993. № 1. Ст. 1.

28. Про телебачення і радіомовлення від 21.12.1993 р. № 3759-XII / Відомості Верховної Ради України. 1994. № 10. Ст. 43.

29. Про Суспільне телебачення і радіомовлення України : Закон України

від 17.04.2014 р. № 1227-VII / Відомості Верховної Ради. 2014. № 27. Ст. 904.

30. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 р. № 8073-X // Відомості Верховної Ради Української РСР. 1984. Додаток до № 51. Ст. 1122.

31. Перун Т. Загальна характеристика правовідносин у сфері забезпечення інформаційної безпеки в Україні. Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2017. № 861. С. 328–332.

32. Про Стратегію сталого розвитку «Україна – 2020» : Указ Президента України від 12.01.2015 р. № 5/2015 URL. http://zakon5.rada.gov.ua/laws/show/5/2015 (дата звернення 03.07.2019).

33. Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях : Закон України від 18.01.2018 р. № 2268-VIII / Відомості Верховної Ради України. 2018. № 10. Ст. 54.

34. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере. Москва: РГУП, 2016. 316 с.

35. Антонюк В. В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України: дис. … канд. з державного управління: спец.: 25.00.02. Київ, 2017. 218 с.

36. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання. Київ: Видавничий дім «Гельветика», 2017. 168 с

37. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : Указ Президента України від 26.05.2015 р. № 287/2015 URL. http://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення 03.07.2019).

38. Авер’янов В. Б. Вибрані наукові праці / Упорядники: Андрійко О. Ф., Нагребельний В. П., Кисіль Л. Є. і інші. За заг. ред.: Ю. С. Шемшученка, О. Ф. Андрійко. Київ: Інститут держави і права імені В. М. Корецького НАН України, 2011. 448 с.

39. Арістова В. І., Сулацький Д. В. Інформаційна безпека людини як споживача телекомунікаційних послуг: монографія. Київ: Право України, 2013. 184 с.

40. Архипова Є. О. Інформаційна безпека: соціально-філософський вимір: автореф. дис. ... канд. філософських наук: спец.: 09.00.03. Київ, 2012. 16 с.

41. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика. Київ: Едельвейс, 2014. 497 с.

42. Бурячок В. Л., Толюпа С. В., Семко А. А. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник. Київ: ДУТ-КНУ, 2016. 178 с.

43. Біленська Д. О. Адміністративно-правове регулювання інформаційних відносин в Україні: автореф. дис. … канд. юрид. наук: спец. 12.00.07. Харків, 2016. 23 с.

44. Гурковський В. І. Державне управління розбудовою інформаційного суспільства в Україні (історія, теорія, практика): монографія. Київ, 2010. 396 с.

45. Жуков Є. В. Держава в добу інформатизації (теоретико-правовий аналіз). Одеса: ХГЄУ, 2014. 211 с.

46. Коваленко Л. П. Інформаційне право України: проблеми становлення та розвитку: автореф. дис. ... д-ра юрид. наук: спец.: 12.00.07. Харків, 2014. 37 с.

47. Ліпкан В. А., Череповський К. П.. Інкорпорація інформаційного законодавства України. Київ: Ліпкан О.С., 2014. 391 с.

48. Ліпкан В. А., Дімчогло М. І. Консолідація інформаційного законодавства України. Київ: О. С. Ліпкан, 2014. 415 с.

49. Мукомела І. В. Правові засади інформаційного суспільства: загальнотеоретичний аналіз: автореф. дис. … канд. юрид. наук: спец. 12.00.01. Харків, 2016. 23 с.

50. Рибальський О. В. Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації. Київ: Видавництво НАВС, 2012. 104 с.

51. Сопілко І. М. Державна інформаційна політика України: стан та

шляхи реалізації: монографія. Київ: Леся, 2014. 423 с.

52. Селезньова О. М. Теоретико-методологічні засади інформаційного права України як інтегрованої категорії: автореф. дис. … д-ра юрид. наук: спец.: 12.00.07. Київ, 2015. 40 с.

53. Ткаченко В. В. Адаптація інформаційного законодавства України до міжнародних правових стандартів в умовах розвитку інформаційного суспільства : автореф. дис. ... канд. юрид. наук: спец.: 12.00.07. Київ, 2014. 22 с.

54. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави. Київ: Видавництво НА СБ України, 2014. 196 с.

55. Абрамов В., Мошинський Р. Теорія безпеки та інститути (про вибір методологічної основи наукового дослідження системи національної безпеки). Вісник Національної академії державного управління при Президентові України. 2011. № 3. С. 5-13.

56. Ортинський В. Л. Удосконалення державної політики у сфері інформаційних технологій у контексті діяльності органів виконавчої влади. Вісник Національного університету «Львівська політехніка». Юридичні науки. 2014. № 801. С. 3-8.

57. Дзьобань О. П., Панфілов О. Ю., Чемчекаленко Р. А. Методологічний контекст дослідження проблеми інформаційної безпеки. Зовнішня торгівля: економіка, фінанси, право. 2014. № 2. С. 171-180

58. Кельман М. С. Юридична наука: проблеми методології. Тернопіль: ТзОВ «Терно-граф», 2011. 492 с.

59. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи. Київ: Національна академія служби безпеки України, 2004. 471 с.

60. Арістова І. В. Методологія науки «інформаційне право». ІТ право: проблеми і перспективи розвитку в Україні: збірник матеріалів науково-практичної конференції (Львів, 18 листопада 2016 р.). Львів, 2016. С. 11-18.

61. Довгань О. Д., Ткачук Т. Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс.

Інформація і право. 2018. № 2 (25). С. 73-85.

62. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 р. № 96/2016 URL. http://zakon2.rada.gov.ua/laws/show/96/2016 (дата звернення 03.07.2019).

63. Щодо вдосконалення методології інтегрального оцінювання рівня економічної безпеки України. Аналітична записка. Національний інститут стратегічних досліджень при Президенті України. URL. http://www.niss.gov.ua/articles/1358/ (дата звернення 03.09.2018).

64. Гнатюк С. Л. Проблеми впровадження сучасних стандартів інформаційної безпеки в умовах становлення національної системи кібербезпеки України. Травень 2018 року. Аналітична записка. Національний інститут стратегічних досліджень при Президенті України. URL. http://www.niss.gov.ua/content/articles/files/1_cPPP-standarts_27-04_Gn_var_FIN-732b6.pdf (дата звернення 03.09.2018).

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

66. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави : Постанова Кабінет Міністрів України від 23.08.2016 р. № 563. URL. http://zakon3.rada.gov.ua/laws/show/563-2016-%D0%BF (дата звернення 03.09.2018).

67. Ткачук Т. Ю. Теоретичний дискурс пошуку основних складових системи інформаційної безпеки держави. Jurnalul juridic national: teorie şi practică. 2018. № 2. С.45-47.

68. Шмідт-Ассманн Е. Загальне адміністративне право як ідея врегулювання: основні засади та завдання систематики адміністративного права. 2-ге вид. перероб. і допов. пер. з нім. Г. Рижков, І. Сойко, А. Баканов; від. ред. О. Сироїд. Київ: К.І.С., 2009. 552 с.

69. Верховна Рада України, Німецький Фонд міжнародного правового

співробітництва. Стан та перспективи розвитку адміністративного права: законодавство, наука, освіта: матеріали семінару (Львів, 12-13 жовтня 2001 р.). Ч. 2. Німеччина та Республіка Польща. Львів, 2001. 208 с.

70. Рудольф фон Иеринг. Юридическая техника. Сост. А. В. Поляков. Москва: Статут, 2008. 231 с.

71. Яцко М. Г., Ткачук Т. Ю. Стан інформаційної безпеки України та основні завдання недержавних суб'єктів по її забезпеченню. Интернаука. 2017 № 1 (23). 1 т. С. 41-43.

72. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII / Відомості Верховної Ради України. 2018. № 31. Ст. 241.

73. Чернухін І. О. Досвід Федеративної республіки Німеччини в побудові системи захисту інфраструктури від кібернетичних загроз. Інформаційна безпека людини, суспільства, держави. 2014. № 1 (14). С. 27-43.

74. Гаврилов О. А. Стратегия правотворчества и социального прогнозирования. Москва: Издательство ИГП РАН, 1993. 128 с.

75. Дзюбенко О. Л. Юридична техніка відомчої нормотворчості в Україні: автореф. дис. … канд. юрид. наук: спец. 12.00.01. Київ, 2010. URL. http://mydisser.com/ru/catalog/view/7145.html (дата звернення 05.09.2018)

76. Брижко В. М. Сучасні основи захисту персональних даних в європейських правових актах. Інформація і право. 2016. № 3 (18). С. 45-56.

77. Войціховський А. В. Питання інформаційної безпеки України на сучасному етапі. Право і безпека. 2015. № 3 (58). С. 15-20.

78. Про внесення змін до деяких законів України щодо зовнішньополітичного курсу України : Закон України від 08.06.2017 р. № 2091-VIII / Відомості Верховної Ради України. 2017. № 30. Ст. 329.

79. Махмадов П. А. Информационная безопасность в системе политической коммуникации: состояние и приоритеты обеспечения (на материалах государств Центральной Азии): дис. … д-ра политических наук: спец.: 23.00.04. Душанбе, 2018, 323 с. URL. http://ifppanrt.tj/dissertatsii_polit/Dissertatsiya_Parviz.pdf (дата звернення

12.09.2018).

80. Чубко О. П. Тенденції розвитку сучасного права, обумовлені глобалізаційними процесами. Митна справа. 2013. № 1. Ч.1., Кн. 2. С. 26-33.

81. Рабінович С. П. Природно-правові підходи в юридичному регулюванні: монографія. Львів: Львівський державний університет внутрішніх справ, 2010. 576 с.

82. Берклич В. О. Функція держави щодо забезпечення й захисту прав та свобод людини і громадянина: автореф. дис.... канд. юрид. наук: спец. 12.00.01. Київ, 2013. 16 с.

83. Кельман М., Коваль І. Методологія дослідження як наукове пізнання. Вісник Національного університету «Львівська політехніка». Юридичні науки. 2016. № 855. С. 199-204.

84. Перун Т. Методологічні засади дослідження механізму забезпечення інформаційної безпеки в Україні Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2017. № 865. С 303-307.

85. Ромащенко В. А. Правове регулювання інформаційного суспільства в Україні: загальнотеоретичне дослідження: автореф. дис. … канд. юрид. наук: спец.: 12.00.01. Одеса, 2018. 26 с.

86. Мосов С. П., Уханова Н. С. Протидія негативним інформаційним впливам на людину і суспільство в умовах гібридної війни. Інформація і право. 2018. № 2 (25). С. 134-141.

87. Золотар О. О. Ґенеза суспільних відносин щодо інформаційної безпеки людини. Інформація і право. 2018. № 1 (24). С. 139-148.

88. Дзьобань О. П., Яроцький В. Л. Соціологічний та аксіологічний напрямки сучасних правових досліджень: загальне бачення Інформація і право. 2018. № 1 (24). С. 5-13.

89. Борець Л. В., Нашинець-Наумова А. Ю. Основи інформаційного права: Навчальний посібник. Київ, Видавництво «Сталь», 2015. 178 с.

90. Бачинський Т. В., Радейко Р. І., Харитонова О. І. Основи ІТ-права: навчальний посібник. Київ: Юрінком Інтер:2018. 208 с.

91. Золотар О. О. Інформаційна безпека людини:теорія і практика. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

92. Кормич Б. А. Інформаційне право: підручник. Харків: Бурун і К., 2011. 334 с.

93. Кормич Б. А., Федотов О. П., Аверочкіна Т. В. Правове регулювання інформаційної діяльності: навчально-методичний посібник. Одеса, 2018. 150 с.

94. Костецька Т. А. Інформаційне право України; навчальний посібник. Київ: Київський національний торгово-економічний університет, 2009. 170 с.

95. Кульчій О. О. Інформаційне право. Полтава, ВНЗ Укоопспілки «ПУЕТ», 2015. 193 с.

96. Куліш А. М., Кобзєва Т. А., Шапіро. В. С. Інформаційне право України: навчальний посібник. Суми: Сумський державний університет, 2016. 108 с

97. Марущак А. І. Інформаційне право України: підручник. Київ: Дакор, 2011. 456 с.

98. Марущак А. І. Пріоритети розвитку інформаційного права України. Інформація і право. 2011. № 1 (1). С. 20-24.

99. Цимбалюк В. С., Гавловський В. Д., Гриценко В. В. Основи інформаційного права України. Київ: Видавництво «Знання», 2004. 274 с.

100. Харитонов Є. О., Харитонов Є. І. ІТ-право та інформаційна безпека. Київ: Фенікс, 2017. 176 с.

101. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. ... канд. юрид. наук: 12.00.01. Київ, 2007. 236 с.

102. Лисенко С. О. Конституційні засади розуміння інформаційної безпеки. Публічне урядування. 2016. № 4. С. 154-161.

103. Хом’яков Д. О. Нормативно-правове регулювання інформаційної безпеки. Актуальні проблеми управління інформаційною безпекою держави: збірник тез наукових доповідей науково-практичної конференції (Київ, 30 березня 2018 р.). Київ: НА СБУ, 2018. С. 182-184.

104. Про Заяву Верховної Ради України «Про відсіч збройній агресії Російської Федерації та подолання її наслідків : Постанова Верховної Ради України від 21.04.2015 р. № 337-VIII / Відомості Верховної Ради України. 2015. № 22. Ст. 153.

105. Стратегія. URL. Матеріал з Вікіпедії – вільної енциклопедії https://uk.wikipedia.org/wiki/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%8F

106. Про Національну програму інформатизації : Закон України від 04.02.1998 р. № 74/98-ВР / Відомості Верховної Ради України. 1998. № 27-28. Ст. 181.

107. Про Концепцію Національної програми інформатизації : Закон України від 04.02.1998 р. № 75/98-ВР / Відомості Верховної Ради України. 1998. № 27-28. Ст. 182.

108. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 р. № 537-V / Відомості Верховної Ради. 2007. № 12. Ст. 102.

109. Ткачук Т. Ю. Інформаційна безпека держави у національному законодавстві європейських країн. Visegrad Journal on Human Rights. 2018. № 1. С. 145-150.

110. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. Резонанс. 2017. № 18. С. 3–14. URL. http://nbuviap.gov.ua/images/rezonans/2017/rez18.pdf (дата звернення 12.08.2018).

111. Ткачук Т. Ю. Политика информационной безопасности НАТО. Legea si Viata. 2018. № 5. С.187-191.

112. Заярний О. А. Правове забезпечення розвитку інформаційної сфери України: адміністративно-деліктний аспект: монографія. Київ: Видавничий дім «Гельветика», 2017. 700 с.

113. Калюжний Р. А., Баєв О. О. Нормативно-правове забезпечення інформаційної безпеки України. Правова інформатика. 2009. № 4 (24). С. 5-12.

114. Левченко О. В. Нормативно-правове регулювання інформаційної

безпеки України: стан та шляхи вирішення проблем. Збірник наукових праць Харківського університету Повітряних Сил. 2014. № 3 (40). С. 130-135.

115. «Активні заходи» СРСР проти США: пролог до гібридної війни. Аналітична доповідь. Д. В. Дубов, А. В. Баровська, Т. О. Ісакова, І. О. Коваль, В. П. Горбулін. 2-ге вид. Київ: НІСД, 2017. 52 с.

116. Пилипчук В. Г., Доронін І. М. Право національної безпеки та військове право: теоретичні та прикладні засади становлення і розвитку в Україні. Інформація і право. 2018. № 2 (25). С. 62-72.

117. Ткачук Н. І. Інформаційні права і свободи людини і громадянина в Україні: визначення термінів, співвідношення понять. Інформація і право. 2018. № 2 (25). С. 17-30.

118. Бачило И. Л. Информационное право: ученик. 5 издание. Москва.: Издательство Юрайт, 2018. 419 с.

119. Городов О. А. Информационное право: учебник. 2 издание. Москва: Проспект. 2018, 304 с.

120. Кузнецов П. У. Основы информационного права: учебник. 2 издание. Москва: Проспект, 2018. 340 с.

121. Бачило И. Л., Лапина М. А. Актуальные проблемы информационного права. Москва: Юстиция, 2018. 536 с.

122. Кузьменко А. М. Нормативно-правове регулювання забезпечення інформаційної безпеки особи, суспільства і держави: досвід Російської Федерації. Законодавство України: проблеми та перспективи розвитку: збірник матеріалів XIII Всеукраїнської науково-практичної конференції (Київ, 29 березня 2012 р.). Київ, 2012. С. 479-493.

123. Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні. Грудень 2017 року. Аналітична записка. Національний інститут стратегічних досліджень при Президенті України. URL. http://www.niss.gov.ua/content/articles/files/kiberbezpek-d3e61.pdf (дата звернення 16.08.2018).

124. Досвід Німеччини у функціонуванні платформ державно-приватного

партнерства в сфері кібербезпеки. Травень 2018 р. Аналітична записка. Національний інститут стратегічних досліджень при Президенті України. URL. http://www.niss.gov.ua/content/articles/files/1_AZ_Boyko_var77_FIN-4d2ef.pdf (дата звернення 16.08.2018).

125. Державно-приватне партнерство в кібербезпековій сфері: досвід республіки Польща. Березень 2018 р. Аналітична записка. Національний інститут стратегічних досліджень при Президенті України. URL http://www.niss.gov.ua/content/articles/files/Ozevan_Polska-4a9f3.pdf (дата звернення 16.08.2018).

126. Нормативно-правові та організаційні засади державно-приватного партнерства США у сфері кібербезпеки. Лютий 2018 р. Аналітична записка. Національний інститут стратегічних досліджень при Президенті України. URL. http://www.niss.gov.ua/content/articles/files/Isakova_USA-6424b.pdf (дата звернення 23.09.2018).

127. Дубов Д. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналітична доповідь. Київ: НІСД, 2018. 84 с.

128. Перун Т. С. Принципи забезпечення інформаційної безпеки України в умовах євроінтеграції. Eurasian Academic Research Journal. 2017. № 11 (17). С. 108-114.

129. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР / Відомості Верховної Ради України. 1994. № 31. Ст. 286.

130. Про державно-приватне партнерство : Закон України від 01.07.2010 р. № 2404-VI / Відомості Верховної Ради України. 2010. № 40. Ст. 524.

131. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави : Постанова Кабінету Міністрів України від 23.08.2016 р. № 563. URL. http://zakon2.rada.gov.ua/laws/show/563-2016-%D0%BF (дата звернення 04.07.2019).

132. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : Розпорядження Кабінету Міністрів України від 06.12.2017 р. № 1009-р. URL. http://zakon0.rada.gov.ua/laws/show/1009-2017-%D1%80 (дата звернення 04.07.2019).

133. Про стандартизацію : Закон України від 05.06.2014 р. № 1315-VII / Відомості Верховної Ради України. 2014. № 31. Ст. 1058.

134. Про метрологію та метрологічну діяльність : Закон України від 05.06.2014 р. № 1314-VII / Відомості Верховної Ради України. 2014. № 30. Ст. 1008.

135. Про технічні регламенти та оцінку відповідності : Закон України від 15.01.2015 р. № 124-VIII / Відомості Верховної Ради України. 2015. № 14. Ст. 96.

136. Про телекомунікації : Закон України від 18.11.2003 р. № 1280-IV // Відомості Верховної Ради України. 2004. № 12. Ст. 155.

137. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT). Будстанларт. URL. http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66893 (дата звернення 04.07.2019).

138. Про виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Постанова Кабінету Міністрів України від 25.10.2017 р. № 1106. Євроінтеграційний портал. URL eu-ua.org/plan-zakhodiv-z-vykonannia-uhody (дата звернення 04.07.2019).

139. Алексеев С. С. Право: азбука – теория – философия. Опыт комплексного исследования. Москва: Статут, 1999. 710 с.

140. Валігура К. Механізм правового регулювання: методологічний аспект. Visegrad journal on human rights. 2016. № 2/1. С. 17-22.

141. Куракін О. М. Механізм правового регулювання: теоретико-правова модель : автореф. дис. ... д-ра юрид. наук: 12.00.01. Харків, 2016. 40 с.

142. Система. Матеріал з Вікіпедії – вільної енциклопедії. URL.

https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0 (дата звернення 22.08.2018).

143. Швець С. В., Швець У. С. Основи системного аналізу: навчальний посібник. Суми: Сумський державний університет, 2017. 126 с.

144. Кривицький Ю. В. Механізм правового регулювання в сучасній теорії права. Часопис Київського університету права. 2009. № 4. С. 74-79.

145. Стукаленко О. В. Нотатки до розуміння категорії «механізм правового регулювання». Правова держава. 2017. № 26. С. 20-25.

146. Кархут О. Я. Механізм правового регулювання суспільних відносин у сфері освіти: теоретико-правовий аспект: автореф. дис. … канд. юрид. наук: спец.: 12.00.01. Київ, 2014. 24 с.

147. Кривицький Ю. В. Спеціалізовані норми права в механізмі правового регулювання: автореф. дис. … канд. юрид. наук: спец.: 12.00.01. Київ, 2010. 20 с.

148. Шапенко Л. Юридичні факти в механізмі правового регулювання страхових відносин. European political and law discourse. 2017. Vol. 4. Issue 2. P. 222-227.

149. Саржан С. Л. Поняття і сутність юридичних фактів у сфері правоохоронної діяльності. Науковий вісник Національного університету біоресурсів і природокористування України. 2013. Вип. 182. Ч. 1. С. 29-34.

150. Кистяковский Б. А. Философия и социология права. Составитель В. В. Сапова. Санкт-Петербург: РХГИ, 1999. 800 с. URL. http://www.kursach.com/biblio/0010016/415_1.htm (дата звернення 22.08.2018).

151. Алексеев С. С. Общая теория права. В 2-х томах. Том 1. Москва: Юридическая литература, 1981. 360 с.

152. Тарахонич Т. І. Види правового регулювання: теоретичні аспекти розуміння. Часопис Київського університету права. 2014. № 4. С. 28-32.

153. Старинський М. В. Політика як фактор впливу на правове регулювання валютних відносин в Україні Правовий вісник Української академії банківської справи. № 2014. № 2 (11). С. 32-37.

154. Ващук Ю. О. Сутнісні аспекти правової політики. Форум права. 2014. № 1. С. 67-71.

155. Курінний Є. Об'єкт та предмет українського адміністративного права: змістовна та аксіологічна сутність категорій. Публічне право. 2016. № 1 (21). С. 43-51.

156. Демків Р. Я. Правове регулювання як юридичне явище: окремі аспекти розуміння. Науковий вісник Ужгородського національного університету. Серія право. 2015. № 34. Том 1. С. 19-23.

157. Куракін О. М. Структура механізму правового регулювання. Науковий вісник Ужгородського національного університету. Серія право. 2015. № 35. Частина II. Том 1. С. 46-49.

158. Краус Н. М., Голобородько О. П., Краус К. М. Цифрова економіка: тренди та перспективи авангардного характеру розвитку. Ефективна економіка. 2018 № 1. URL. http://www.economy.nayka.com.ua/pdf/1_2018/8.pdf (дата звернення 22.092018).

159. Вольвак О. М. Теоретичні засади забезпечення ефективності правого регулювання. Порівняльно-аналітичне право. 2018. № 2. С. 22-25.

160. Кохановська О.В. Приватноправове розуміння інформаційних відносин в Україні. ІТ право: проблеми і перспективи розвитку в Україні: збірник матеріалів науково-практичної конференції (Львів, 18 листопада 2016 р.). Львів, 2016. URL. http://aphd.ua/publication-154/ (лата звернення 23.08.2018).

161. Ваньчук І. Д. Поняття й сутнісні ознаки правового регулювання суспільних відносин: сучасний погляд. Науковий вісник Ужгородського національного університету. Серія право. 2015. № 32. Том 1. С. 7-10.

162. Лазор Я. Поняття та види інформаційних систем. ІТ право: проблеми і перспективи розвитку в Україні: збірник матеріалів науково-практичної конференції (Львів, 18 листопада 2016 р.) Львів, 2016. URL. http://aphd.ua/publication-146/ (лата звернення 23.08.2018).

163. Вейтас М. В., Лукашенко М. І. Кібертероризм: тенденції розвитку та механізми протидії. Науковий огляд. 2018. № 4 (47). С. 1-15. URL.

http://oaji.net/articles/2017/797-1530622888.pdf (лата звернення 23.08.2018).

164. Теоретико-прикладні проблеми правового регулювання в Україні: збірник тез регіональної науково-практичної конференції (Львів, 15 грудня 2017 року). Львів: Львівський державний університет внутрішніх справ, 2017. – 380 с.

165. Подзігун С. М. Аналіз сучасних наукових підходів до розуміння сутності стратегічного управління. Глобальні та національні проблеми економіки. 2017. № 17. С. 411-414.

166. Яременко О. Державне управління інформаційною сферою в Україні: структурно-функціональний аспект. Правова інформатика. 2008. № 2 (18). С. 9-17.

167. Бурик З. М. Система методів державного регулювання сталого розвитку в Україні. Актуальні проблеми державного управління. 2016. № 1 (49). С. 1-8.

168. Адміністративне право України. Академічний курс: підручник: У 2 томах: Том 1. Загальна частина / Ред. колегія: В. Б. Авер'янов (голова). Київ: Видавництво «Юридична думка», 2004. 584 с.

169. Грохольський В. Л. Визначення сутності державного управління та його відмежування від суміжних понять. Інтернаука. Серія: «Юридичні науки». 2017. № 1 (1). С. 28-32.

170. Куц Ю. О. Природа та сутність державного управління. Теорія та практика державного управління і місцевого самоврядування. 2013. № 1. С.1-9. http://el-zbirn-du.at.ua/Kuc_s.pdf (дата звернення 11.09.2081).

171. Соловйов В. М. Поняття і сутність правового регулювання державного управління. Університетські наукові записки. 2007. № 3. С. 27-33.

172. Котковський В. Р. Теоретико-методологічні засади участі місцевих органів влади у формуванні та реалізації державної політики: автореф. дис. … д-ра наук з державного управління: спец.: 25.00.02. Харків, 2018, 43 с.

173. Дзьобань О. П., Мануйлов Є. М. Інформаційна безпека в контексті інформаційної культури. Інформація і право. 2017. № 1 (20). С. 74-81.

174. Fred C. Lunenburg, Beverly J. Irby. Development of Administrative Thought: A Historical Overview. International journal of organizational theory and development. 2013. Volume 1. № 1. P. 1-20.

175. Хомишин І. Ю. Сучасні інформаційні технології в освіті. ІТ право: проблеми і перспективи розвитку в Україні: збірник матеріалів науково-практичної конференції (Львів, 18 листопада 2016 р.). Львів, 2016. С. 151-154.

176. Криволапчук В. О. Сучасний погляд на методи адміністративного права. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. 2014. Вип. 4. С. 184-192.

177. Нестеряк Ю. В. Аналіз моделей інформаційної політики та державного регулювання засобів масової комунікації. Публічне управління та митне адміністрування. 2016. № 2. С. 65-70.

178. Жиляєв І. Б., Семенченко А. І., Фурашев В. М. Інструменти державного стратегічного управління: національна програма інформатизації. Інформація і право. 2018. № 1 (24).С. 44-58.

179. Доронін І. М. Трансформації національної безпеки в інформаційну епоху: загальна доктрина та її правова складова. Інформація і право. 2018. № 1 (24). С. 104-111.

180. Ткачук Т. Ю. Теоретичний дискурс пошуку основних складових системи інформаційної безпеки держави. Jurnalul juridic national: teorie şi practică. 2018. № 2. С.45-47.

181. Доронін І. М., Тарасюк А. В. Корпоративна культура кібербезпеки суб'єктів наукової та науково-технічної діяльності. Інформація і право. 2018. № 2 (25). С. 51-62.

182. Бєляков К. І. Технолого-правовий аналіз законодавства України в секторі інформаційної безпеки країни. Lex Portys. 2017. № 1. С. 210-218.

183. Державне підприємство «Державний центр інформаційної безпеки». Офіційний веб-сайт. URL. https://scis.com.ua/#about (дата звернення 22.09.2018).

184. Єсімов С. С., Мельник С. Я. Інформаційно-правова політика, як складова інформаційної функції держави. Науковий вісник Львівського

державного університету внутрішніх справ. Серія юридична. 2016. № 1. С. 167-178.

185. Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України від 11.07.2018 р. № 481-р. URL. https://www.kmu.gov.ua/ua/npas/pro-zatverdzhennya-planu-zahodiv-na-2018-rik-z-realizaciyi-strategiyi-kiberbezpeki-ukrayini (дата звернення 07.08.2019).

186. Петруненко Я. Поняття державної підтримки суб'єктів господарювання як засобу забезпечення ефективного використання бюджетних коштів. Підприємництво, господарство і право. 2018. № 6. С. 110-115.

187. Копан О. В. Дестабілізація соціально-політичної ситуації – провокація внутрішньодержавного конфлікту. Інформація і право. 2017. № 4 (23). С.73-78.

188. Уханова Н. С. Захист інформаційного простору від терористичних посягань та негативних інформаційно-психологічних впливів. Інформація і право. 2017. № 4 (23). С. 99-105.

189. Олійник О. В. Адміністративно-правові засоби забезпечення інформаційної безпеки. Юридичний вісник. 2015. № 1 (34) С. 65-69.

190. Закон про адміністративну процедуру: експерти розповіли, чого очікувати громадянам і бізнесу. 10 травня 2018 року. Центр політико-правових реформ. URL. http://pravo.org.ua/ua/news/20872932-zakon-pro-administrativnu-protseduru-eksperti-rozpovili,-chogo-ochikuvati-gromadyanam-i-biznesu (дата звернення 10.09.2018).

191. Великанова М. Оцінка ризику: формування правової стратегії управління ризиком. Підприємництво, господарство і право. 2018. № 1. С. 4-8.

192. Про схвалення Стратегії розвитку оборонно-промислового комплексу України на період до 2028 року : Розпорядження Кабінету Міністрів України від 20.06.2018 р. № 442-р. URL. http://zakon5.rada.gov.ua/laws/show/442-2018-%D1%8 (дата звернення 10.07.2019).

193. Золотар О. О. Особливості інформаційної безпеки людини в умовах

гібридної війни. Інформація і право. 2017. № 3 (22). С.124-131.

194. Nastyuk V. The democratic control over the safety sector during the fight against terrorism. Yearbook of Ukrainian law: Coll.of scientific papers /responsible for the issue O.V. Petryshyn. Kharkiv: Law, 2017. № 9. P. 98-102.

195. Кучерина С. Є., Олєйніков Д. О. Протидія антидержавному екстремізму як інструменту обмеження державного суверенітету в сучасних умовах. Інформація і право. 2018. № 2 (25). С. 113-123.

196. Корж І. Ф. Вільний доступ громадян до правової інформації – засаднича ознака забезпечення правової безпеки держави. Інформація і право. 2018. № 1 (24). С. 14-27.

197. Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України : Постанова Кабінету Міністрів України від 16.11.2016 р. № 821. URL. http://zakon2.rada.gov.ua/laws/show/821-2016-%D0%BF (дата звернення 01.07.2019).

198. Доронін І. М. Екстраординарний характер реалізації безпекових функцій держави в сучасному світі (інформаційно-правовий аспект). Інформація і право. 2018. № 2 (25). С. 75-85.

199. Про затвердження Порядку та Методики проведення моніторингу та оцінки результативності реалізації державної регіональної політики : Постанова Кабінету Міністрів України від 21.10.2015 р. № 856. URL. http://zakon5.rada.gov.ua/laws/show/856-2015-%D0%BF (дата звернення 20.09.2018).

200. Про затвердження завдань, ключових показників результативності, ефективності та якості службової діяльності державних службовців, які займають посади державних секретарів міністерств, на 2018 рік : Розпорядження Кабінету Міністрів України від 11.04.2018 р. № 239-р. URL. http://zakon5.rada.gov.ua/laws/show/239-2018-%D1%80 (дата звернення

20.09.2018).

201. Семенов А. А. Создание А. Файолем теории административного управления. Современные проблемы науки и образования. 2012. № 2.. URL: http://www.science-education.ru/ru/article/view?id=5794 (дата звернення 20.09.2018).

202. Фуко М. Безопасность, территория, население: курс лекцій. Санкт-Петербург: Наука: 2011. 544 с.

203. Про рішення Ради національної безпеки і оборони України від 26 січня 2018 року «Про додаткові заходи щодо протидії інформаційній агресії Російської Федерації» : Указ Президента України від 09.02.2018 р. № 25/2018. URL. http://zakon2.rada.gov.ua/laws/show/25/2018 (дата звернення 20.09.2018).

204. Скакун О. Ф. Теорія права і держави: підручник. Київ: Правова єдність, 2010. 525 с. URL. http://westudents.com.ua/glavy/70135-6-subkti-prava-yak-subkti-uchasniki-pravovdnosin.html (дата звернення 20.09.2018).

205. Галунько В., Діхтієвський П., Кузьменко О., Стеценко С. Адміністративне право України. Повний курс: підручник. Херсон: ОЛДІ-ПЛЮС, 2018. 446 с.

206. Гбур З. В. Основні функції держави у сфері забезпечення економічної безпеки. Актуальні проблеми державного управління. 2017. № 2 (52). С. 1-9.

207. Шаповал В. М. Виконавча влада в Україні в контексті реформи державного правління (досвід після прийняття Конституції України 1996 року). Присвячено В. Б. Авер'янову. Центр політико-правових реформ. 23 лютого 2016 року. URL. http://pravo.org.ua/ua/news/20871343-vikonavcha-vlada-v-ukrayini-v-konteksti-formi-dergeavnogo-pravlinnya-dosvid-pislya-priynyattya-konstitutsiyi-ukrayini-1996-roku (дата звернення 13.09.2018).

208. Косиця О. О. Інституціональний механізм системи інформаційної безпеки. Порівняльно-аналітичне право. 2016. № 4. URL. http://www.pap.in.ua/4_2016/45.pdf (дата звернення 13.09.2018).

209. Про Раду національної безпеки і оборони України : Закон України

від 05.03.1998 р. № 183/98-ВР / Відомості Верховної Ради України. 1998. № 35. Ст. 237.

210. Андріїв М. М. Поняття та структура компетенції органів публічної влади. Теорія та практика державного управління. 2017. № 2 (57). С. 2-8.

211. Деякі питання реформування державного управління України : Розпорядження Кабінету Міністрів України від 24.06.2016 р. № 474-р. URL. http://zakon2.rada.gov.ua/laws/show/474-2016-%D1%80 (дата звернення 01.07.2019).

212. Брижко В. М. Філософія права: гносеологія у сфері інформаційного права. Правова інформатика. 2014. № 2 (42). С.25-32.

213. Про перелік, кількісний склад і предмети відання комітетів Верховної Ради України восьмого скликання : Постанова Верховної Ради України від 04.12.2014 р. № 22-VIII / Відомості Верховної Ради України. 2015. № 1. Ст. 10.

214. Про Рекомендації парламентських слухань на тему: «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України» : Постанова Верховної Ради України від 31.03.2016 р. № 1073-VIII. / Відомості Верховної Ради. 2016. № 17. Ст. 191.

215. Антонюк В. В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України: дис. … канд. наук з державного управління: спец.: 25.00.02. Київ, 2017. 218 с.

216. Дмитренко М. А. Проблемні питання інформаційної безпеки України. 2018. URL. journals.iir.kiev.ua/index.php/pol_n/article/download/3318/2997 (дата звернення 20.08.2018).

217. Про деякі питання Апарату Ради національної безпеки і оборони України : Указ Президента України від 14.04.2017 р. № 109/201. URL. http://zakon0.rada.gov.ua/laws/show/109/2017 (дата звернення 20.08.2018).

218. Про Кабінет Міністрів України : Закон України від 27.02.2014 р. № 794-VII / Відомості Верховної Ради України. 2014. № 13. Ст. 222.

219. Про затвердження Регламенту Кабінету Міністрів України : Постанова Кабінету Міністрів України від 18.07.2007 р. № 950. URL. http://zakon5.rada.gov.ua/laws/show/950-2007-%D0%BF (дата звернення 20.08.2018).

220. Про Конституційний Суд України : Закон України від 13.07.2017 р. № 2136-VIII / Відомості Верховної Ради України. 2017. № 35. Ст. 376.

221. Рішення Конституційного Суду України у справі за конституційним поданням 49 народних депутатів України щодо відповідності Конституції України (конституційності) Указу Президента України «Про деякі питання здійснення керівництва у сферах національної безпеки і оборони». Справа № 1-3/2009 25 лютого 2009 року № 5-рп/2009. URL. http://zakon2.rada.gov.ua/laws/show/v005p710-09 (дата звернення 20.08.2018).

222. Про центральні органи виконавчої влади : Закон України від 17.03.2011 р. № 3166-VI / Відомості Верховної Ради України. 2011. № 38. Ст. 385.

223. Москалюк Н. В. Актуальні проблеми удосконалення нормативного закріплення функцій органів виконавчої влади в Україні. Актуальні проблеми вітчизняної юриспруденції. Спецвипуск. 2017. Ч.2. С. 139-142.

224. Деякі питання електронної взаємодії державних електронних інформаційних ресурсів : Постанова Кабінету Міністрів України від 08.09.2016 р. № 606. URL. http://zakon3.rada.gov.ua/laws/show/606-2016-%D0%BF (дата звернення 20.08.2018).

225. Питання діяльності Міністерства інформаційної політики України : Постанова Кабінету Міністрів України від 14.01.2015 р. № 2. URL. http://zakon2.rada.gov.ua/laws/show/en/2-2015-%D0%BF (дата звернення 28.08.2018).

226. Найкраща контрпропаганда – це правда. Звіт про роботу Міністерства інформаційної політики України. січень – березень 2018. URL. https://mip.gov.ua/files/mip_zvit_2018_1kvartal.pdf (дата звернення 28.08.2018).

227. Про Державну службу спеціального зв’язку та захисту інформації

України : Закон України від 23.02.2006 р. № 3475-IV / Відомості Верховної Ради України. 2006. № 30. Ст. 258.

228. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України : Постанова Кабінету Міністрів України від 03.09.2014 р. № 411. URL. http://zakon3.rada.gov.ua/laws/show/411-2014-%D0%BF (дата звернення 28.08.2018).

229. Державний Стандарт України. Захист інформації. Технічний захист інформації. Основні Положення. ДСТУ 3396.0-96. URL. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=38836 (дата звернення 28.08.2018).

230. Державний Стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96. URL. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=38836 (дата звернення 28.08.2018).

231. Державний Стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97. URL. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=38836 (дата звернення 28.08.2018).

232. Про затвердження Положення про Міністерство оборони України : Постанова Кабінеті Міністрів України від 26.11.2014 р. № 671. URL. zakon.rada.gov.ua/go/671-2014-п (дата звернення 28.08.2018).

233. Про затвердження Положення про Генеральний штаб Збройних Сил України: Указ Президента України від 30.01.2019 р. № 23/2019. URL. https://zakon.rada.gov.ua/laws/show/ru/23/2019 (дата звернення 10.02.2019).

234. Про затвердження Положення про Міністерство внутрішніх справ України : Постанова Кабінеті Міністрів України від 28.10.2015 р. № 878. URL. http://zakon3.rada.gov.ua/laws/show/878-2015-%D0%BF (дата звернення 28.08.2018).

235. Про затвердження Положення про орган військового управління

оперативно-територіального об'єднання Національної гвардії України : Наказ МВС України від 16.07.2014 р. № 681. URL. http://zakon5.rada.gov.ua/laws/show/z0890-14 (дата звернення 28.08.2018).

236. Про Службу зовнішньої розвідки України : Закон України від 01.12.2005 р. № 3160-IV / Відомості Верховної Ради України. 2006. № 8. Ст. 94.

237. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII / Відомості Верховної Ради України. 1992. № 27. Ст. 382.

238. Климчук О. Інформаційна та кібербезпека в сучасному світі: досвід СБУ. 12.07.2018. Ліга net. URL. http://ua.news.liga.net/politics/opinion/informatsiyna-ta-kiberbezpeka-vsuchasnomu - sviti-dosvid-sbu (дата звернення 28.08.2018).

239. Актуальні проблеми управління інформаційною безпекою держави: збірник тез наукових доповідей науково-практичної конференції (Київ, 30 березня 2018 р.). Київ: Національна академія СБУ, 2018. 408 с

240. Про затвердження. Положення про Департамент кіберполіції Національної поліції : Наказ Національної поліції України від 10.11.2015 р. № 85. URL. http://tranzit.ltd.ua/nakaz/ (дата звернення 28.08.2018).

241. Харебава Т. Відмінність IT-бізнесу від кіберзлочинності. Не слід плутати. Київ: Spenser & Kauffmann, 2017. 20 с.

242. Про деякі питання інформаційної безпеки України : Наказ МВС України від 19.08.2014 р. № 840. URL. http://document.ua/pro-dejaki-pitannja-informaciinoyi-bezpeki-ukrayini-doc200231.html

243. Єсімов С. С. Діяльність Національної поліції з забезпечення інформаційної безпеки у контексті діяльності засобів масової інформації. Актуальні проблеми управління інформаційною безпекою держави: збірник тез наукових доповідей науково-практичної конференції (Київ, 30 березня 2018 р.). Київ: Національна академія СБУ, 2018. С. 211-213.

244. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII / Відомості Верховної Ради України. 2015. № 40-41. Ст. 379.

245. Про Національну раду України з питань телебачення і радіомовлення

: Закон України від 23.09.1997 р. № 538/97-ВР / Відомості Верховної Ради України. 1997. № 48. Ст. 296.

246. Про затвердження Положення про Державний комітет телебачення і радіомовлення України : Постанова Кабінеті Міністрів України від 13.08.2014 р. № 341. URL. http://zakon0.rada.gov.ua/laws/show/341-2014-%D0%BF (дата звернення 29.08.2018).

247. Про затвердження Положення про Міністерство культури України : Постанова Кабінеті Міністрів України від 03.09.2014 р. № 495. URL. http://zakon2.rada.gov.ua/laws/show/495-2014-%D0%BF (дата звернення 29.08.2018).

248. Єсімов С. С. Електронні документи як докази у справах про адміністративні правопорушення. Вісник Національного університету «Львівська Політехніка». Серія: юридичні науки. 2016 № 845. С.69-76.

249. Сірант О. Р. Нові види доказів у провадженні у справах про адміністративні правопорушення: проблеми теорії та практики: дис. … канд. юрид. наук: спец.: 12.00.07. Кривий Ріг, 2018. 254 с.

250. Участь громадських об'єднань у протидії інформаційній агресії РФ. Доповідна записка. Вересень 2016 року. Національний інститут стратегічних досліджень при Президенті України. URL. http://www.niss.gov.ua/content/articles/files/AZ-Protid-ya--nformagres---166e3.pdf (дата звернення 30.08.2018).

251. Мінка Т. П. Правовий режим у теорії адміністративного права. Адміністративне право і процес 2013. № 2. URL. http://applaw.knu.ua/index.php/arkhiv-nomeriv/2-4-2013/item/177-pravovyy-rezhym-u-teoriyi-administratyvnoho-prava-minka-t-p (дата звернення 30.08.2018).

252. Коваленко Н. В. Адміністративно-правові режими: дис. … д-ра юрид. наук: спец.: 12.00.07. Запоріжжя, Запорізький національний університет, 2017. 529 с.

253. Галунько В. В., Курило В. І., Короєд С. О. Адміністративне право України. Т.1. Загальне адміністративне право: навчальний посібник. Херсон:

Грінь Д.С., 2015. 272 с.

254. Вакарюк Л. Основні підходи до розуміння поняття «правовий режим». Підприємництво, господарство і право. 2016. № 12. С. 196-201.

255. Адабаш О. В. Поняття, сутність та ознаки адміністративно-правових режимів. Європейські перспективи. 2013. № 12. С. 36-40.

256. Мальцев В. Особливості забезпечення правового режиму антитерористичної операції органами внутрішніх справ в Україні. Вісник Харківського національного університету імені В. Н. Каразіна. Серія Право. 2015. № 20. 266-270.

257. Кузніченко С. О. Становлення та розвиток інституту надзвичайних адміністративно-правових режимів в Україні: автореф. дис. … д-ра. юрид. наук: спец.: 12.00.07. Харків, 2010. 34 с.

258. Середа В. В. Надзвичайні правові режими у сфері публічного права. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. 2017. № 3. С. 101-112.

259. Ковалів М. В., Рутар А. І., Павлишин Ю. В. Порядок і підстави введення правового режиму надзвичайного стану. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. 2015. № 2. С. 180–188.

260. Про правовий режим надзвичайного стану : Закон України від 16.03.2000 р. № 1550-III / Відомості Верховної Ради України. 2000. № 23. Ст. 176.

261. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. № 389-VIII / Відомості Верховної Ради України. 2015. № 28. Ст. 250

262. Чистоклетов Л., Хитра О., Остапенко Л., Скриньковський Р. Поняття, ознаки та зміст правових режимів, що запроваджуються під час виникнення кризових ситуацій. Traektoriâ Nauki. Path of Science. 2018. Vol. 4, № 3. С.6001-6006.

263. Настюк В. Я., Бєлєвцева В. В. Адміністративно-правові режими в Україні. Харків: Право, 2009. 128 с.

264. Про затвердження Порядку вжиття тимчасових надзвичайних заходів з подолання наслідків тривалого порушення нормальної роботи ринку електричної енергії : Постанова Кабінету Міністрів України від 13.08.2014 р. № 372. URL. http://zakon2.rada.gov.ua/laws/show/372-2014-%D0%BF (дата звернення 30.08.2018).

265. Про затвердження Правил здійснення діяльності у сфері телекомунікацій (діяльність з надання послуг доступу до Інтернет) : Рішення Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації від 10.12.2013 р. № 803. URL. http://zakon5.rada.gov.ua/laws/show/z0207-14 (дата звернення 30.08.2018).

266. Державні будівельні норми України Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва ДБН А.2.2-2-96. URL. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38938&cat_id=38836 (дата звернення 30.08.2018).

267. Орел О. В., Мідіна А. С. Адміністративно-правові засади оцінки рівня ризиків безпеки інформації в процесах службово-бойової діяльності Національної гвардії України. Journal «ScienceRise: Juridical Science». 2018. № 1 (3). С. 45-49.

268. Основи управління інформаційною безпекою на базі міжнародних стандартів серії ISO. Київський національний університет імені Т. Шевченко. URL. https://studfiles.net/preview/2265905/ (дата звернення 30.08.2018).

269. Коваленко Н. В. Окремі складові адміністративно-правового режиму конфіденційної інформації. Вісник Національного університету «Львівська політехніка». Юридичні науки. 2016. № 845. С. 75-82

270. Лісовська Ю. П. Адміністративно-правове забезпечення інформаційної безпеки в Україні: автореф. дис. … канд. юрид. наук: спец. 12.00.07. Київ, 2017. 21 с.

271. IT-індустрія: тренди та прогнози розвитку. Інформаційна довідка. Європейський інформаційно-дослідницький центр. Київ: UASID, 2018. 12 с.

272. Аведян Л. Й. Державне регулювання сфери сучасних інформаційних технологій та інновацій: закордонний досвід. Актуальні проблеми державного управління. 2017. 2 (52). С. 1-6.

273. Ковалів М., Єсімов С., Крамар Р., Скриньковський Р. Перспективи реформування організаційно-правового механізму забезпечення прав і свобод людини та громадянина. Traektoriâ Nauki. Path of Science. 2017. Vol. 3. № 10. P. 6001-6008.

274. Про запровадження Національної системи індикаторів розвитку інформаційного суспільства : Постанова Кабінету Міністрів України від 28.11.2012 р. № 1134. URL. http://zakon2.rada.gov.ua/laws/show/1134-2012-%D0%BF (дата звернення 01.09.2018).

275. Про затвердження Методики формування індикаторів розвитку інформаційного суспільства : Наказ Міністерство освіти і науки України від 06.09.2013 р. № 1271. URL. http://zakon2.rada.gov.ua/laws/show/z1664-13/paran13#n13 (дата звернення 01.09.2018).

276. Про затвердження Типового положення про управління організаційно-аналітичного забезпечення та оперативного реагування головних управлінь Національної поліції України в Автономній Республіці Крим та м. Севастополі, областях, м. Києва : Наказ МВС України від 22.01.2016 р. № 39. URL. http://zakon5.rada.gov.ua/laws/show/z0216-16/paran7#n7 (дата звернення 01.09.2018).

277. Про створення міжвідомчої робочої групи Адміністрації Державної служби спеціального зв'язку та захисту інформації України і Міністерства внутрішніх справ України : Спільний наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Міністерства внутрішніх справ України від 08.05.2015 р. № 256/545. URL. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=E26EA615EF01E8A00DDF183B87CE5FE9.app2?art_id=148413&cat_id=121207 (дата звернення 01.09.2018).

278. Про затвердження Положення про Департамент інформатизації

Міністерства внутрішніх справ України : Наказ МВС України від 31.01.2018 р. № 70. URL. http://parusconsultant.com/?doc=0AZG0FB928&abz=KB7HR (дата звернення 01.09.2018).

279. Про затвердження Інструкції про взаємодію правоохоронних та інших державних органів України у боротьбі із злочинністю : Наказ МВС України, Служби безпеки України, Державного комітету у справах охорони Державного кордону України, Державного митного комітету України, Національної гвардії України, Міністерства оборони України, Міністерства юстиції України від 10.08.1994 р. № 4348/138/151/11-2-2870/172/148-407/2-90-442. URL. http://zakon2.rada.gov.ua/laws/show/z0225-94 (дата звернення 01.09.2018).

280. Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків : Постанова Кабінету Міністрів України від 12.02.2016 р. № 92. URL. http://zakon5.rada.gov.ua/laws/show/92-2016-%D0%BF (дата звернення 01.09.2018).

281. Бугайчук К. Функції публічного адміністрування в органах Національної поліції України: поняття та класифікація. Підприємництво, господарство і право. 2018. № 5. С.112-117.

282. Єсімов С. С. Юридична відповідальність суб'єктів публічного управління за порушення інформаційного законодавства України. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. 2017. Вип. 3. С. 82-92.

283. Перун Т. Значення адміністративної відповідальності в системі заходів забезпечення інформаційної безпеки. Право України. 2017. № 10. С. 202-209.

284. Лошицький М. В. Адміністративно-правові засоби в механізмі охорони навколишнього природного середовища. Митна справа. 2015. № 1 (97). С. 79-85.

285. Бортник Н. П., Пєтков С. В. Загрози інформаційному ресурсу

держави в контексті інформаційної та національної безпеки. IT право: проблеми і перспективи розвитку в Україні Збірник матеріалів науково-практичної конференції (Львів, 18 листопада 2016 р). Львів, 2016. С.34-36.

286. Серков П. П. Административная ответственность: автореф. дис. … д-ра юрид. наук: спец. 12.00.14. Москва, 2010. URL. http://www.dissercat.com/content/administrativnaya-otvetstvennost#ixzz2qpUMlYp (дата звернення 20.07.2018).

287. Процессуально-исполнительный кодекс Республики Беларусь об административных правонарушениях. Официальное издание. Минск.: Высшая школа, 2015. 116 с.

288. Банчук О. А. Адміністративне деліктне законодавство: Зарубіжний досвід та пропозиції реформування в Україні. Київ: Книги для бізнесу, 2007. 912 с.

289. Стратегія розвитку МВС до 2020 року: детально про відхід від міліції. 15.11.2017. URL. https://www.5.ua/suspilstvo/stratehiia-rozvytku-mvs-do-2020-roku-detalno-pro-vidkhid-vid-militsii-159349.html

290. Пашковська Т. Cybercrime: системи захисту «нарощують м'язи». Юридична газета online. 14 березня 2017 року. URL. http://yur-gazeta.com/publications/practice/inshe/sybercrime-sistemi-zahistu-naroshchuyut-myazi.html (дата звернення 20.08.2018).

291. Федченко Д. І. Система забезпечення кібербезпеки: проблеми формування та ефективної діяльності. Young Scientist. 2018. № 5 (57). С. 653-658.

292. Адміністративні правопорушення у 2016 році. Статистичний бюлетень. Київ: Державна служба статистики України. 2017. 205 с.

293. Стан злочинності у 2016 році. Доповідь. Київ Державна служба статистики України. 2017. 2 с.

294. Задорожна Я. В. Спосіб вчинення протиправного діяння як ознака об'єктивної сторони адміністративного проступку: автореф. дис. … канд. юрид. наук спец.: 12.00.07. Запоріжжя, 2016. 22 с.

295. Навроцький В. О. Основи кримінально-правової кваліфікації: навчальний посібник. Київ: Юрінком Інтер, 2006. – 704 с.

296. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ: ДУТ, 2015. 288 с.

297. Ковалів М. В. Основи управління в органах внутрішніх справ України: навчально-практичний посібник. Львів: Львівський державний університет внутрішніх справ, 2010. 340 с.

298. Повторева С. М. Структурний підхід – структуралізм – постструктуралізм (еволюція методології та її поширення у гуманітарних студіях). Львів: Видавництво «Львівська політехніка», 2010. 336 с.

299. Сергій Князєв: Найближчим часом до МВС на затвердження подадуть критерії оцінки. Веб-сайт МВС України 27.01.2018. URL. http://mvs.gov.ua/ua/news/11884_Sergiy_Knyazv_Nayblizhchim_chasom_do_MVS_na_zatverdzhennya_podadut_kriterii_ocinki_efektivnosti_roboti_policii_FOTO.htm (дата звернення 22.08.2018).

300. Про затвердження Концепції (нова редакція) програми інформатизації системи Міністерства внутрішніх справ України на 2018–2020 роки : Рішення колегії МВС від 05.11.2018 р. № 18 КМ. URL. https://mvs.gov.ua/upload/file/koncepc_ya_nformatizac_mvs_12.12.2018.pdf

(дата звернення 20.12..2018).

301. Остапенко О. І. Адміністративна деліктологія: соціально-правовий феномен і проблеми розвитку. Львів: Львівський інститут внутрішніх страв, 1995. 312 с.

302. Остапенко О. І. Хитра О. Л. Юрисдикційна діяльність органів, що уповноважені розглядати справи про адміністративні правопорушення. Навчальний посібник. Львів, Растр-7. 2017. 220 с.

303. Денисенко В. В. Деликтология: от конфронтации к интеграции административной деликтологии и криминологии. Москва, 2011.URL. http://www.juristlib.ru/book_9045.html (дата звернення 20.12..2018).

304. Поляков Е. М. Кибернетика, меметика и теория массовой коммуникации: обзор естественнонаучных подходов к проблемам социологии. Человек. Сообщество. Управление. 2009. № 3. С. 33-41. URL. http://chsu.kubsu.ru/arhiv/2009_3/CHSU2009-3.pdf (дата звернення 20.12.2018).

305. Грищук В. К. Філософсько-правове розуміння відповідальності людини: 2 видання перероблене і доповнене. Хмельницький: Хмельницький університет управління і права, 2013. 768 с.

306. Ортинський В. Новітні методи дослідження адміністративно-правових явищ. Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2014. № 782. С. 5–9.

307. Ортинський В. Л. Реформування правоохоронної системи у контексті соціально-правового механізму забезпечення прав особистості. Вісник Національного університету «Львівська політехніка». Юридичні науки. 2014. № 810. С. 38-42.

308. Єсімов С. С. Правове регулювання застосування інформаційних технологій для формування довіри до органів державної влади. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. 2015. Вип. 1. С. 173-184.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Перун Т. С. Історія розвитку права на інформацію. *Митна справа*. 2013. № 2 (86). Ч. 2. К. 1. С. 417–422.

2. Перун Т. Загальна характеристика правовідносин у сфері забезпечення інформаційної безпеки в Україні. *Вісник Національного університету «Львівська політехніка»*. Серія: Юридичні науки. 2017. № 861. С. 328–332.

3. Перун Т. Методологічні засади дослідження механізму забезпечення інформаційної безпеки в Україні. *Вісник Національного університету «Львівська політехніка»*. Серія: Юридичні науки. 2017. № 865. С. 303–307.

4. Перун Т. С. Принципи забезпечення інформаційної безпеки України в умовах євроінтеграції. *Eurasian Academic Research Journal*. 2017. № 11 (17). С. 108–114. (Вірменія).

5. Перун Т. Значення адміністративної відповідальності в системі заходів забезпечення інформаційної безпеки. *Право України*. 2017. № 10. С. 202–209.

6. Перун Т. С. Шляхи покращення взаємодії між Україною та ЄС у сфері забезпечення інформаційної безпеки. *Наукові записки Інституту законодавства Верховної Ради України*. 2018. № 5. С. 26–30.

які засвідчують апробацію матеріалів дисертації:

7. Перун Т. С. Адміністративна відповідальність в системі заходів забезпечення інформаційної безпеки. *ІТ-право: проблеми і перспективи розвитку в Україні*: збірник матеріалів ІІ Міжнародної науково-практичної конференції (Львів, 17 листопада 2017 р.) Львів, Національний університет «Львівська політехніка». 2017. С. 155–160.

8. Перун Т. С. Адміністративно-правова відповідальність за правопорушення у сфері інформаційної безпеки. *Адміністративне право і процес: проблеми та перспективи розвитку: тези* Всеукраїнської заочної науково-

практичної конференції. (м. Львів, 30 березня 2018 р.). [у 2 ч.]. Київ: МП «Леся». Ч. 1 С. 166–170.

9. Перун Т. Провайдер як суб'єкт інформаційного права. *Політичні, соціальні, економічні, психологічні та правові механізми регулювання міграційних процесів у сучасних умовах:* матеріали Міжнародної заочної науково-практичної конференції. (м. Львів, 17 травня 2018 р.). Київ: МП «Леся». С. 82–84.

10. Перун Т. Інформаційна безпека країн ЄС: проблеми та перспективи правового регулювання. *Правові засади європейської та євроатлантичної інтеграції України: досягнення та перспективи*: матеріали учасників ІІ заочної науково-практичної конференції (Львів, 23 листопада 2018 р.). Львів, 2018. С. 140–143.

Додаток Б

Опитування

думки представників Головного управління Національної поліції у Львівській області та Карпатського управління кіберполіції Департаменту кіберполіції Національної поліції за темою «Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні»

1. . Чи, на Вашу думку, норми чинного законодавства, спрямовані на забезпечення інформаційної безпеки, можна вважати ефективними?

Відповідь	Кількість	%
Так	30	60%
Ні	11	22%
Не відповіли	9	18%

2. У науковій літературі забезпечення інформаційної безпеки визначають як:

Відповідь	Кількість	%
Визначені нормативно-правовими актами заходи захисту інформаційного простору	1	2%
Технічний захист інформації	1	2%
Комплекс правових і технічних заходів	1	2%
Сукупність прийомів і засобів захисту інформаційно-комунікаційних систем	1	2%
Не зустрічав вказаних визначень у науковій літературі	46	92%

3. Чи доцільне, на Вашу думку, державно-приватне партнерство у забезпеченні інформаційної безпеки?

Відповідь	Кількість	%
Так	8	16%
Ні	3	6%
Складно визначити	28	56%
Не відповіли	11	22%

4. Чи Ви вважаєте доцільним внесення доповнень до нормативно-правових актів щодо державно-приватного партнерства у забезпеченні інформаційної безпеки?

Відповідь	Кількість	%
Так	21	42%
Ні	25	50%
Не відповіли	4	8%

5. Чи Ви вважаєте документи, що рівень адміністративно-правого забезпечення інформаційної безпеки є задовільним

Відповідь	Кількість	%
Доцільно	17	34%
Не доцільно	17	34%
Не знаю	3	6%
Не відповіли	13	26%

6. Чи доцільно, на Вашу думку, адміністративні правопорушення у інформаційній сфері чи пов’язаних з інформацією звести у одну главу Кодексу України про адміністративні правопорушення?

Відповідь	Кількість	%
Доцільно	6	12%
Не доцільно	5	10%
Не знаю	22	44%
Інші відповіді	2	4%
Не відповіли	15	30%

7. Чи, на Вашу думку, норми чинного законодавства, спрямовані на боротьбу з правопорушеннями в сфері забезпечення інформаційної безпеки, можна вважати ефективними?

Відповідь	Кількість	%
Так	2	4%
Ні	8	16%
Не відповіли	40	80%

8. Чи на Вашу думку, доцільно контрольно-наглядові процедури у сфері забезпечення інформаційної безпеки включити у Адміністративний процесуальний кодекс?

Відповідь	Кількість	%
Так	20	40%
Ні	20	40%
Не відповіли	10	20%

9. Чи доцільно доповнити Кодекс України про адміністративні правопорушення норми процесуальні норми, що визначають порядок проведення контрольно-наглядових заходів у сфері забезпечення інформаційної безпеки?

Відповідь	Кількість	%
Так	6	12%
Ні	29	58%
Не відповіли	15	30%

10. Чи достатньо, на Ваш погляд, методичних рекомендацій щодо адміністративно-юрисдикційної діяльності у сфері забезпечення інформаційної безпеки?

Відповідь	Кількість	%
Так	20	40%
Ні	20	40%
Не відповіли	10	20%

Надіслано 80 анкет. Отримано 50. Для аналізу вибрано 50.

25 анкет працівників апарату Головного управління Національної поліції у Львівській області.

25 анкет працівників Карпатського управління кіберполіції Департаменту кіберполіції Національної поліції.

Опитування

думки представників управління Державної служби спеціального зв'язку і захисту інформації України у Львівській області

1. Чи, на Вашу думку, норми чинного законодавства, спрямовані на забезпечення інформаційної безпеки, можна вважати ефективними?

Відповідь	Кількість	%
Так	4	8%
Ні	46	92%
Не відповіли	0	0%

2. У науковій літературі забезпечення інформаційної безпеки визначають як:

Відповідь	Кількість	%
Визначені нормативно-правовими актами заходи захисту інформаційного простору	0	0%
Технічний захист інформації	0	0%
Комплекс правових і технічних заходів	0	0%
Сукупність прийомів і засобів захисту інформаційно-комунікаційних систем	0	0%
Не зустрічав вказаних визначень у науковій літературі	50	100%

3. Чи доцільне, на Вашу думку, державно-приватне партнерство у забезпеченні інформаційної безпеки?

Відповідь	Кількість	%
Так	50	100%
Ні	0	0%
Не відповіли	0	0%

4. Чи Ви вважаєте доцільним внесення доповнень до нормативно-правових актів щодо державно-приватного партнерства у забезпеченні інформаційної безпеки?

Відповідь	Кількість	%
Так	49	98%
Ні	0	0%
Не відповіли	1	2%

5. Чи Ви вважаєте документи, що рівень адміністративно-правого забезпечення інформаційної безпеки є задовільним?

Відповідь	Кількість	%
Доцільно	40	80%
Не доцільно	0	0%
Не знаю	0	0%
Не відповіли	10	20%

6. Чи доцільно, на Вашу думку, адміністративні правопорушення у інформаційній сфері чи пов’язаних з інформацією звести у одну главу Кодексу України про адміністративні правопорушення?

Відповідь	Кількість	%
Так	50	100%
Ні	0	0%
Не відповіли	0	0%

7. Чи, на Вашу думку, норми чинного законодавства, спрямовані на боротьбу з правопорушеннями в сфері забезпечення інформаційної безпеки, можна вважати ефективними?

Відповідь	Кількість	%
Так	22	44%
Ні	20	40%
Не відповіли	8	16%

8. Чи на Вашу думку, доцільно контрольно-наглядові процедури у сфері забезпечення інформаційної безпеки включити у Адміністративний процесуальний кодекс?

Відповідь	Кількість	%
Так	4	8%
Ні	44	88%
Не відповіли	2	4%

9. Чи доцільно доповнити Кодекс України про адміністративні правопорушення норми процесуальні норми, що визначають порядок проведення контрольно-наглядових заходів у сфері забезпечення інформаційної безпеки?

Відповідь	Кількість	%
Так	16	32%
Ні	14	28%
Не відповіли	20	40%

10. Чи достатньо, на Ваш погляд, методичних рекомендацій щодо адміністративно-юрисдикційної діяльності у сфері забезпечення інформаційної безпеки?

Відповідь	Кількість	%
Так	48	96%
Ні	0	0%
Не відповіли	2	4%

Надіслано 60 анкет. Отримано 50. Для аналізу вибрано 50.

Опитування
представників кафедр адміністративного та інформаційного права
вищих навчальних юридичних закладів
(Львівський національний університет імені Івана Франка, Інститут права і психології Національного університету «Львівська політехніка», Львівський державний університет внутрішніх справ, Ужгородський національний університет)

1. Чи, на Вашу думку, норми чинного законодавства, спрямовані на забезпечення інформаційної безпеки, можна вважати ефективними?

Відповідь	Кількість	%
Так	10	20%
Ні	40	80%
Не відповіли	0	0%

2. У науковій літературі забезпечення інформаційної безпеки визначають як:

Відповідь	Кількість	%
Визначені нормативно-правовими актами заходи захисту інформаційного простору	6	12%
Технічний захист інформації	3	6%
Комплекс правових і технічних заходів	38	76%
Сукупність прийомів і засобів захисту інформаційно-комунікаційних систем	3	6%
Не зустрічав вказаних визначень у науковій літературі	0	0%

3. Чи доцільне, на Вашу думку, державно-приватне партнерство у забезпеченні інформаційної безпеки?

Відповідь	Кількість	%
Так	46	92%
Ні	3	6%
Не відповіли	1	2%

4. Чи Ви вважаєте доцільним внесення доповнень до нормативно-правових актів щодо державно-приватного партнерства у забезпеченні інформаційної безпеки?

Відповідь	Кількість	%
Так	25	50%
Ні	25	50%
Не відповіли	0	0%

5. Чи Ви вважаєте документи, що рівень адміністративно-правого забезпечення інформаційної безпеки є задовільним?

Відповідь	Кількість	%
Доцільно	25	50%
Не доцільно	24	48%
Не знаю	1	2%
Не відповіли	0	0%

6. Чи доцільно, на Вашу думку, адміністративні правопорушення у інформаційній сфері чи пов’язаних з інформацією звести у одну главу Кодексу України про адміністративні правопорушення?

Відповідь	Кількість	%
Доцільно	50	100%
Не доцільно	0	0%
Не відповіли	0	0%

7. Чи, на Вашу думку, норми чинного законодавства, спрямовані на боротьбу з правопорушеннями в сфері забезпечення інформаційної безпеки, можна вважати ефективними?

Відповідь	Кількість	%
Так	2	4%
Ні	48	96%
Не відповіли	0	0%

8. Чи на Вашу думку, доцільно контрольно-наглядові процедури у сфері забезпечення інформаційної безпеки включити у Адміністративний процесуальний кодекс?

Відповідь	Кількість	%
Так	10	20%
Ні	40	80%
Не відповіли	0	0%

9. Чи доцільно доповнити Кодекс України про адміністративні правопорушення норми процесуальні норми, що визначають порядок проведення контрольно-наглядових заходів у сфері забезпечення інформаційної безпеки?

Відповідь	Кількість	%
Так	4	8%
Ні	36	72%
Не відповіли	10	20%

10. Чи достатньо, на Ваш погляд, методичних рекомендацій щодо адміністративно-юрисдикційної діяльності у сфері забезпечення інформаційної безпеки?

Відповідь	Кількість	%
Так	30	60%
Ні	20	40%
Не відповіли	0	0%

Надіслано 60 анкет. Отримано 50. Для аналізу вибрано 50.

Примітка: *опитування здійснювали на кафедрах:*

– адміністративного та інформаційного права Інституту права та психології Національного університету «Львівська політехніка» – 10 анкет;

– адміністративного права і процесу факультету № 4 (з підготовки працівників для кадрових і патрульних підрозділів) Львівського державного університету внутрішніх справ – 10 анкет;

– адміністративно-правових дисциплін факультету № 6 (юридичного) Львівського державного університету внутрішніх справ –10 анкет;

– адміністративного та фінансового права юридичного факультету Львівського національного університету імені Івана Франка – 10 анкет;

– адміністративного права юридичного факультету Ужгородського національного університету – 10 анкет.

Узагальнення

опитування за темою «Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні»

1. Чи, на Вашу думку, норми чинного законодавства, спрямовані на забезпечення інформаційної безпеки, можна вважати ефективними?

Відповідь	Кількість	%
Так	44	29%
Ні	97	65%
Не відповіли	9	6%

2. У науковій літературі забезпечення інформаційної безпеки визначають як:

Відповідь	Кількість	%
Визначені нормативно-правовими актами заходи захисту інформаційного простору	7	5%
Технічний захист інформації	4	3%
Комплекс правових і технічних заходів	39	25%
Сукупність прийомів і засобів захисту інформаційно-комунікаційних систем	50	33%
Не відповіли	50	33%

3. Чи доцільне, на Вашу думку, державно-приватне партнерство у забезпеченні інформаційної безпеки?

Відповідь	Кількість	%
Так	104	70%
Ні	6	4%
Складно визначити	28	18%
Не відповіли	12	8%

4. Чи Ви вважаєте доцільним внесення доповнень до нормативно-правових актів щодо державно-приватного партнерства у забезпеченні інформаційної безпеки?

Відповідь	Кількість	%
Так	96	69%
Ні	50	33%
Не відповіли	4	8%

5. Чи Ви вважаєте документи, що рівень адміністративно-правого забезпечення інформаційної безпеки є задовільним?

Відповідь	Кількість	%
Доцільно	92	61%
Не доцільно	41	27%
Не знаю	4	3%
Не відповіли	13	9%

6. Чи доцільно, на Вашу думку, адміністративні правопорушення у інформаційній сфері чи пов’язаних з інформацією звести у одну главу Кодексу України про адміністративні правопорушення?

Відповідь	Кількість	%
Доцільно	106	71%
Не доцільно	5	3%
Не знаю	22	15%
Інші відповіді	2	1%
Не відповіли	15	10%

7. Чи, на Вашу думку, норми чинного законодавства, спрямовані на боротьбу з правопорушеннями в сфері забезпечення інформаційної безпеки, можна вважати ефективними?

Відповідь	Кількість	%
Так	26	17%
Ні	76	51%
Не відповіли	48	32%

8. Чи на Вашу думку, доцільно контрольно-наглядові процедури у сфері забезпечення інформаційної безпеки включити у Адміністративний процесуальний кодекс?

Відповідь	Кількість	%
Так	34	23%
Ні	104	69%
Не відповіли	12	8%

9. Чи доцільно доповнити Кодекс України про адміністративні правопорушення норми процесуальні норми, що визначають порядок проведення контрольно-наглядових заходів у сфері забезпечення інформаційної безпеки?

Відповідь	Кількість	%
Так	26	17%
Ні	79	53%
Не відповіли	45	30%

10. Чи достатньо, на Ваш погляд, методичних рекомендацій щодо адміністративно-юрисдикційної діяльності у сфері забезпечення інформаційної безпеки?

Відповідь	Кількість	%
Так	98	65%
Ні	40	27%
Не відповіли	12	8%

Надіслано 200 анкет. Отримано 150. Для аналізу вибрано 150.

Додаток В

Закон України
«Про захист інформації
в інформаційно-телекомунікаційних системах»
(Відомості Верховної Ради 1994. № 31. Ст. 286)

Доповнити пункт 5 частини 2 статті 10 «Повноваження державних органів у сфері захисту інформації в системах» та викласти у редакції:

Стаття 10. Повноваження державних органів у сфері захисту інформації в системах

Вимоги до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

…

здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі, сприяє державно-приватному партнерству у сфері захисту інформації;

Далі за текстом.

Додаток Д

Закон України
«Про державно-приватне партнерство»
(Відомості Верховної Ради. 2010. № 40. Ст. 524)

1. Доповнити абзац перший частини першої статті 1 «Визначення та ознаки державно-приватного партнерства» та викласти у редакції:

Розділ І
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення та ознаки державно-приватного партнерства

1. Державно-приватне партнерство - співробітництво між державою Україна, Автономною Республікою Крим, територіальними громадами в особі відповідних державних органів та органів місцевого самоврядування (державними партнерами) та юридичними особами, крім державних та комунальних підприємств, або фізичними особами - підприємцями (приватними партнерами), що здійснюється на основі договору в порядку, встановленому цим Законом та іншими законодавчими актами, та відповідає ознакам державно-приватного партнерства, визначеним цим Законом.

Державно-приватна взаємодія у сфері кібербезпеки (інформаційної безпеки) специфічна форми взаємодії між державним і приватним секторами на основі принципу партнерства, створеної з метою реалізації заходів інформаційної безпеки визначених статтею 10 Державно-приватна взаємодія у сфері кібербезпеки Закону України від 5 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України» спрямованих на задоволення суспільних потреб, яка передбачає консолідацію ресурсів, а також поділ відповідальності і ризиків між сторонами.

2. Доповнити частину першу статті 4 «Сфери застосування державно-приватного партнерства» абзацом вісімнадцятим та викласти у редакції:

забезпечення інформаційної безпеки (кібербезпеки).

Далі за текстом.

Додаток Е

Закон України
«Про телекомунікації»
(Відомості Верховної Ради. 2004. № 12. Ст. 155)

Доповнити пункт 17 частини першої статті 18 «Повноваження Національної комісії, що здійснює державне регулювання у сфері зв’язку та інформатизації» та викласти у редакції:

Стаття 18. Повноваження Національної комісії, що здійснює державне регулювання у сфері зв’язку та інформатизації

1. Національна комісія, що здійснює державне регулювання у сфері зв’язку та інформатизації:

17) створює сприятливі організаційні та економічні умови для залучення інвестицій у сферу телекомунікацій; сприяє державно-приватній взаємодії у сфері інформаційної безпеки (кібербезпеки);

Далі за текстом.

Додаток Ж

Закон України
«Про Державну службу спеціального зв'язку
та захисту інформації України»
(Відомості Верховної Ради України. 2006. № 30. Ст. 258)

1. Доповнити частину першу статті 1 «Визначення термінів» та викласти у редакції:

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

1. У цьому Законі наведені нижче терміни вживаються в таких значеннях:

…

державна система урядового зв'язку - система спеціального зв'язку, що функціонує в державні інформаційні ресурси - систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень;

державно-приватна взаємодія у сфері кібербезпеки (інформаційної безпеки) специфічна форми взаємодії між державним і приватним секторами на основі принципу партнерства, створеної з метою реалізації заходів інформаційної безпеки визначених статтею 10 Державно-приватна взаємодія у сфері кібербезпеки Закону України від 5 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України» спрямованих на

задоволення суспільних потреб, яка передбачає консолідацію ресурсів, а також поділ відповідальності і ризиків між сторонами.

Далі за текстом.

2. Доповнити частину першу статті 14 «Обов’язки Державної служби спеціального зв’язку та захисту інформації України» пунктом 93 та викласти у редакції:

Розділ IV

ПОВНОВАЖЕННЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Стаття 14. Обов’язки Державної служби спеціального зв’язку та захисту інформації України

1. На Державну службу спеціального зв’язку та захисту інформації України відповідно до визначених завдань покладаються такі обов’язки:

93) координація державно-приватній взаємодії у сфері інформаційної безпеки та кібербезпеки.

Далі за текстом.

Додаток И

Положення
про Інтегровану інформаційно-пошукову систему МВС України
(Затверджено наказом Міністерства внутрішніх справ України від 12.10.2009 № 436. Зареєстровано в Міністерстві юстиції України 28 грудня 2009 року за № 1256/17272)

Доповнити розділ 3 «Інформаційні ресурси ІІПС» та викласти у редакції:

3.2. Джерелами формування інформаційних ресурсів ІІПС є:

зареєстровані заяви і повідомлення про кримінальні та адміністративні правопорушення, кримінальні провадження;

…

інформація, отримана від громадян і посадових осіб, про вчинені кримінальні правопорушення під час проведення слідчих (гласних) розшукових дій;

інформація про події зв’язані з інформаційною безпекою;

інформація, отримана від правоохоронних органів іноземних держав на підставі міжнародних договорів України, угод про співробітництво між МВС і відповідними органами іноземних держав у сфері боротьби із злочинністю зареєстровані заяви і повідомлення про злочини та адміністративні правопорушення, кримінальні справи;

повідомлення працівників ОВС у разі звернення до них громадян або службових осіб із заявою чи повідомленням про події, які загрожують особистій чи громадській безпеці, або у разі безпосереднього виявлення таких;

повідомлення про аварії, пожежі, катастрофи, стихійні лиха та інші надзвичайні події, які підлягають реєстрації в ОВС;

повідомлення засобів масової інформації, публічні виступи;

Далі за текстом.

Додаток К

Положення
про Міністерство внутрішніх справ України
(Затверджено постановою Кабінету Міністрів України від 28.10.2015 № 878)

Доповнити пункт 2 розділу 4 «МВС відповідно до покладених на нього завдань», викласти в редакції:

2) нормативно-правові акти, які регулюють суспільні відносини відповідно до компетенції визначеної законодавством та цим Положенням;

Доповнити пункт 5 розділу 4 «МВС відповідно до покладених на нього завдань»:

5) розробляє проекти державних програм з питань забезпечення інформаційної безпеки і порядку, протидії злочинності, безпеки дорожнього руху, охорони державного кордону, захисту об’єктів і територій на випадок виникнення надзвичайних ситуацій, а також з питань міграції;

Додаток Л

Регламент

Міністерства внутрішніх справ України

(Наказ Міністерства внутрішніх справ України від 20.11.2007 № 440)

Доповнити пункт 3 словами: у сфері забезпечення інформаційної безпеки є координатором юрисдикційної діяльності та викласти у редакції:

I. Загальні положення

1. Цей Регламент установлює порядок організації діяльності Міністерства внутрішніх справ України, пов'язаної зі здійсненням його повноважень.

2. Міністерство внутрішніх справ спрямовує свою діяльність на виконання Конституції і інших законів України, актів Президента України і Верховної Ради України, прийнятих відповідно до Конституції і інших законів України, актів Кабінету Міністрів України, Програми діяльності Кабінету Міністрів України, інших актів законодавства.

3. Міністерство внутрішніх справ, у межах своїх повноважень, на основі та на виконання актів законодавства видає накази, організовує і контролює їх виконання, а в разі потреби видає разом з іншими органами виконавчої влади спільні акти, у сфері забезпечення інформаційної безпеки є координатором юрисдикційної діяльності.

Далі за текстом.

Примітка: жирним шрифтом показано зміст пропозицій.

Додаток М

Структура
законопроекту «Про основи державної системи
профілактики правопорушень»

Структура законопроекту передбачає такі розділи:

I. Загальні положення.

II. Основні види та засоби профілактики правопорушень.

III. Система суб'єктів і учасників державної системи профілактики правопорушень, їх повноваження.

IV. Повноваження державних органів в сфері профілактики правопорушень

V. Порядок і засади застосування заходів профілактики правопорушень

VI. Забезпечення діяльності суб'єктів державної системи профілактики правопорушень

VII. Відповідальність за порушення законодавства України у галузі профілактики правопорушень

VIII. Нагляд і контроль у сфері профілактики правопорушень

IX. Прикінцеві положення.