УДК 342.9
DOI https://doi.org/10.32782/2524-0374/2024-6/53

АДМІНІСТРАТИВНО-ПРАВОВІ ФОРМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

ADMINISTRATIVE AND LEGAL FORMS OF INFORMATION SECURITY IN UKRAINE

Крупнова А.О., адвокат,
аспірант кафедри кримінально-правових та адміністративно-правових дисциплін
Міжнародний економіко-гуманітарний університет імені Степана Дем'янчука

У статті, на основі аналізу чинного законодавства, наявних наукових, публіцистичних та методичних джерел, з'ясовано зміст адміністративно-правових форм забезпечення інформаційної безпеки в Україні. Запропоновано під адміністративно-правовою формою забезпечення інформаційної безпеки розуміти зовнішнє вираження впливу суб'єкта адміністративно-правового забезпечення інформаційної безпеки на відповідний об'єкт з метою створення та збереження стану захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Встановлено, що діяльність суб'єктів адміністративно-правового забезпечення інформаційної безпеки в Україні може виражатися як у правових, так і неправових формах. Правові форми тягнуть за собою юридичні наслідки і за змістом поділяються на: правотворчі (видання нормативно-правових актів) і правозастосовні (ухвалення рішень у конкретних справах і правових суперечках, що виникають у процесі функціонування системи забезпечення інформаційної безпеки). Неправові форми адміністративно-правового забезпечення інформаційної безпеки не спричиняють юридичних наслідків і, найчастіше, є результатом вчинення правових дій, тобто застосовуються на підставі вже наявних правових актів, договорів і документів, що мають юридичне значення. Їх ми поділили на дві основні групи: організаційні та матеріально-технічні. Організаційні заходи не пов'язані безпосередньо з виникненням, зміною та припиненням конкретних правовідносин. Вони здійснюються в процесі поточної діяльності зі створення та підтримання необхідного рівня інформаційної безпеки відповідного об'єкта захисту. За допомогою матеріально-технічних дій забезпечується можливість здійснення всіх інших форм, у яких виражається діяльність цих суб'єктів. Вони є передумовою для правових та організаційних форм забезпечення інформаційної безпеки.

Ключові слова: адміністративно-правове забезпечення, адміністративно-правова форма, інформаційна безпека, захист інформації, інформаційні відносини.

Based on the analysis of current legislation, available scientific, journalistic and methodological sources, the article clarifies the content of administrative and legal forms of information security in Ukraine. The author proposes to understand the administrative and legal form of information security as an external expression of the influence of the subject of administrative and legal provision of information security on the relevant object with a view to creating and maintaining the state of protection of State sovereignty, territorial integrity, democratic constitutional order and other vital interests of a person, society and the State, under which the constitutional rights and freedoms of a person to collect, store, use and disseminate information are duly ensured.

The author establishes that the activities of the subjects of administrative and legal support of information security in Ukraine may be expressed in both legal and non-legal forms. Legal forms entail legal consequences and are divided into lawmaking (issuance of regulatory legal acts) and law enforcement (decision-making in specific cases and legal disputes arising in the course of functioning of the information security system). Non-legal forms of administrative and legal support for information security do not entail legal consequences and are most often the result of legal actions, i.e., they are applied on the basis of existing legal acts, contracts and documents of legal significance. We have divided them into two main groups: organizational and logistical. Organizational measures are not directly related to the emergence, change and termination of specific legal relations. They are carried out in the course of ongoing activities to create and maintain the required level of information security of the respective object of protection. With the help of material and technical actions, it is possible to carry out all other forms in which the activities of these subjects are expressed. They are a prerequisite for legal and organizational forms of information security.

Key words: administrative and legal support, administrative and legal form, information security, information protection, information relations.

Постановка проблеми. Адміністративно-правове забезпечення інформаційної безпеки, як і будь-яка інша діяльність в Україні, неминуче знаходить своє вираження в певних формах і здійснюється різними методами. Адміністративно-правові форми забезпечення інформаційної безпеки показують, як і за допомогою чого реалізуються цілі, завдання і функції, що стоять перед системою адміністративно-правового забезпечення інформаційної безпеки.

Адміністративно-правова форма забезпечення інформаційної безпеки є зовнішнім вираженням впливу суб'єкта адміністративно-правового забезпечення інформаційної безпеки на відповідний об'єкт з метою створення та збереження стану захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [1]. Специфіка завдань і функцій у царині забезпечення інформаційної безпеки породжує різноманіття форм цієї діяльності, які будуть розглянуті нами в цьому науковому дослідження.

Стан опрацювання проблематики. Різні аспекти проблематики адміністративно-правового забезпечення інформаційної безпеки в Україні **розкривали в своїх працях:** І. Арістова, О. Баранов, В. Брижко, О. Довгань, О. Золотар, І. Корж, Р. Калюжний, Б. Кормич, В. Ліпкан, А. Марущак, В. Пилипчук, В. Рубан, Г. Сащук, Я. Собків, С. Феденько, Л. Харченко, В. Шамрай та ін. Визнаючи всю важливість виконаної вченими роботи, водночас необхідно відзначити, що попередні наукові праці, у тому числі на рівні дисертаційних досліджень, головним чином, були присвячені проблемам правового регулювання сфери забезпечення інформаційної безпеки в Україні.

Метою статті є з'ясування на основі аналізу чинного законодавства, наявних наукових, публіцистичних та мето-

дичних джерел, сутності та змісту адміністративно-правових форм забезпечення інформаційної безпеки в Україні.

Виклад основного матеріалу. Традиційно форми адміністративної діяльності залежно від породжуваних ними наслідків поділяють на: правові та неправові. Такий поділ властивий і для адміністративно-правових форм забезпечення інформаційної безпеки. При цьому вид конкретної форми визначається характером дій суб'єктів адміністративно-правового забезпечення інформаційної безпеки щодо здійснення покладених на них функцій. Форма забезпечення інформаційної безпеки може бути віднесена до числа правових тільки в тому разі, якщо в діях, що здійснюються відповідним суб'єктом, чітко проявляється його юридичне волевиявлення.

1. Правові форми тягнуть за собою юридичні наслідки і можуть бути класифіковані за різними підставами. Так, за змістом адміністративно-правові форми забезпечення інформаційної безпеки поділяють на: правотворчі та правозастосовні.

Правотворча форма забезпечення інформаційної безпеки полягає у виробленні суб'єктами адміністративно-правового забезпечення інформаційної безпеки правових норм, правил поведінки, що регулюють різні сторони суспільних відносин, що складаються з приводу забезпечення інформаційної безпеки, тобто, з позиції законодавця, адміністративно-правове регулювання у сфері інформаційної безпеки являє собою прийняття органами державної влади правових актів у сфері інформаційної безпеки.

Правотворчість являє собою складний процес, який складається з низки логічно послідовних стадій, що змінюють одна одну за результатом проміжного результату. Процес творення нормативно-правового акта не є одномоментним, а триває в часі, тобто є послідовною зміною визначених стадій. Стадії правотворчої діяльності можна визначити як самостійні фази процедурних дій щодо формування державної волі або як організаційно відокремлені комплекси тісно пов'язаних між собою дій, спрямованих на створення нормативно-правового акта. На кожній стадії виникає нова якість створюваного нормативно-правового акта (прийняття рішення про підготовку проекту нормативно-правового акта, внесення на розгляд правотворчого органу, прийняття рішення правотворчим органом щодо проекту нормативно-правового акта, оприлюднення та введення в дію нормативно-правового акта) [2, с. 4]. Застосування правотворчої форми більшою мірою притаманне державним суб'єктам адміністративно-правового забезпечення інформаційної безпеки, зокрема, органам законодавчої та виконавчої влади, оскільки вони наділені відповідними повноваженнями.

Органи законодавчої влади України здійснюють адміністративно-правове забезпечення інформаційної безпеки у формі ухвалення законів, пов'язаних з інформаційною безпекою, що регулюють відповідні суспільні відносини.

Президент України є главою держави і в межах своєї компетенції видає укази та розпорядження. Тому видання Президентом України правових актів, що регулюють суспільні відносини, які виникають у сфері інформаційної безпеки, також слід відносити до правових форм її забезпечення. Крім правових актів, спрямованих на безпосереднє забезпечення інформаційної безпеки, Президент України видає акти, що за своєю природою не мають такої конкретної спрямованості, проте регулюють окремі питання, пов'язані зі здійсненням суб'єктами адміністративно-правове забезпечення інформаційної безпеки покладених на них функцій і спрямовані на ефективне функціонування деяких підсистем забезпечення інформаційної безпеки (наукової, інформаційної, освітньої, кадрової тощо).

Правотворчість суб'єктів виконавчої влади здійснюється на основі та на виконання правових актів, що мають вищу юридичну силу, які видаються органами законодавчої влади, Президентом України, і, відповідно, не може їм суперечити. Специфіка цієї групи правових актів полягає в тому, що вони можуть мати як галузевий відомчий характер, так і міжгалузевий надвідомчий характер, тобто встановлювати правові норми для суб'єктів суспільних відносин, які не перебувають із цими органами в субординаційному підпорядкуванні.

Правові акти, що регулюють питання забезпечення інформаційної безпеки, які видаються різними органами державної влади, у своїй сукупності, становлять законодавство України щодо інформаційної безпеки.

Правозастосовна форма забезпечення інформаційної безпеки являє собою діяльність суб'єктів адміністративно-правового забезпечення інформаційної безпеки з реалізації правових норм щодо конкретних питань. Фактично, вона полягає в діях уповноважених на те органів і посадових осіб щодо підведення конкретного факту, що має юридичне значення, під відповідну правову норму для ухвалення індивідуального акта з метою розв'язання на основі правових норм певних питань, які виникають у процесі функціонування системи адміністративно-правового забезпечення інформаційної безпеки.

Правозастосовний процес складається з декількох послідовних стадій, результати кожної з яких відображаються у відповідному акті застосування права. До основних стадій правозастосовного процесу належать такі: встановлення фактичних обставин юридичної справи та їх оцінювання. На цій стадії застосування права проводяться збирання, систематизація й аналіз інформації (доказів), які мають стосунок до розглянутої юридичної справи та можуть вплинути на владне правозастосовне рішення, що виноситься; встановлення фактичних обставин справи (юридична кваліфікація), що полягає у виборі й аналізі правового припису, який підлягає застосуванню й відповідає встановленим фактичним обставинам у розглянутій юридичній справі; прийняття (винесення) владного рішення у справі та його документальне оформлення. На третій стадії суб'єкт правозастосування конкретизує виявлену правову норму в рішенні, що виноситься, з урахуванням наявних у справі обставин [3, с. 11]. На останній стадії відбувається видання правозастосовником такого юридичного документа, як акт застосування права, у якому відображаються основні результати правозастосовної діяльності, здійсненої в рамках розгляду конкретної юридичної справи. Акт застосування права не містить у собі правових норм, він лише визначає механізм вирішення виниклого питання. Акти застосування права мають обов'язковий характер для всіх суб'єктів відповідних суспільних відносин, яким вони адресовані. При цьому ефективність і якість подальшого виконання таких актів істотно впливає на функціонування різних підсистем і всієї системи адміністративно-правового забезпечення інформаційної безпеки загалом.

Правозастосування здійснюють переважно державні суб'єкти системи адміністративно-правового забезпечення інформаційної безпеки, зокрема, Президент України, органи виконавчої та судової влади. За допомогою правозастосовної діяльності компетентні державні органи та їхні посадові особи реалізують покладені на них владні повноваження: в процесі управління системою адміністративно-правового забезпечення інформаційної безпеки; в процесі розв'язання в адміністративному або судовому порядку індивідуально-конкретних справ чи спорів, що виникають у цій сфері.

Очевидно, що застосування правових форм, як правотворчих, так і правозастосовних, властиве здебільшого державним суб'єктам системи адміністративно-правового забезпечення інформаційної безпеки. Однак, у випадках, встановлених законодавством, а також у разі делегування владних повноважень органами державної влади, правотворчість і правозастосування у сфері інформаційної безпеки, у межах наданої їм компетенції, можуть здійсню-

вати посадові особи органів місцевого самоврядування, громадські об'єднання (корпоративні норми), адміністрація підприємств та установ (локальні норми). Водночас до правотворчої діяльності, здійснюваної недержавним суб'єктами системи адміністративно-правового забезпечення інформаційної безпеки можна віднести: видання локальних інструкцій у сфері інформаційної безпеки; встановлення додаткових правил і вимог інформаційної безпеки, що не суперечать відповідним правовим актам, які мають вищу юридичну силу; встановлення заходів соціального й економічного стимулювання забезпечення інформаційної безпеки тощо.

До правозастосовної ж діяльності зазначених суб'єктів у галузі забезпечення пожежної безпеки слід відносити: видання в межах наданої компетенції індивідуальних актів (усних і письмових розпоряджень, наказів) з питань функціонування системи адміністративно-правового забезпечення інформаційної безпеки; призначення відповідальних за інформаційну безпеку на підприємствах і в установах; винесення рішень про заохочення співробітників, які беруть активну участь у забезпеченні інформаційної безпеки, про притягнення винних у недотриманні та неналежному виконанні вимог і правил інформаційної безпеки до дисциплінарної відповідальності тощо.

До правових форм адміністративно-правового забезпечення інформаційної безпеки слід також відносити укладення договорів і вчинення інших юридично-значущих дій, оскільки вони можуть слугувати підставою виникнення різного роду правовідносин (адміністративних, цивільних, трудових та ін.), тобто спричинити певні юридичні наслідки. За допомогою вчинення такого роду дій суб'єкти системи адміністративно-правового забезпечення інформаційної безпеки реалізують права і виконують обов'язки, встановлені чинним законодавством України щодо інформаційної безпеки, а також договорами, що регулюють суспільні відносини в цій сфері. Тому їх можна подати як різновид правових форм адміністративно-правового забезпечення інформаційної безпеки та позначити як правореалізуючі.

Договори в галузі забезпечення інформаційної безпеки, залежно від учасників і характеру цих відносин, можуть мати міжнародний, адміністративно-правовий та цивільно-правовий характер.

Міжнародні договори є міжнародними угодами, які можуть укладатися уповноваженими державними органами України з іноземною державою (або державами) чи з міжнародною організацією в письмовій формі з різних питань співробітництва в галузі забезпечення інформаційної безпеки. Залежно від органів, які укладають міжнародні договори, розрізняють договори міждержавні, міжурядові та міжвідомчі.

Адміністративний договір є спільним правовим актом суб'єктів владних повноважень або правовим актом за участю суб'єкта владних повноважень та іншої особи, що ґрунтується на їх волеузгодженні, має форму договору, угоди, протоколу, меморандуму тощо, визначає взаємні права та обов'язки його учасників у публічно-правовій сфері і укладається на підставі закону [4]. Зазначені правові акти в галузі адміністративно-правового забезпечення інформаційної безпеки можуть укладатися між: державними органами; державними органами та недержавними суб'єктами системи адміністративно-правового забезпечення інформаційної безпеки. У випадках застосування державними органами договору як правової форми діяльності, спрямованої на здійснення завдань і функцій, що стоять перед ними, порядок укладення та чинність договору регулюється нормами не тільки цивільного, а й адміністративного права.

Законодавець також встановлює, що виробництво товарів із забезпечення інформаційної безпеки в Україні здійснюється на основі державного замовлення, однією з правових форм реалізації якого є державні контракти. Державний контракт є договором, укладеним державним замовником від імені держави з суб'єктом господарювання – виконавцем державного замовлення, в якому визначаються економічні та правові зобов'язання сторін і регулюються їх господарські відносини [5]. Такі договори укладаються в інтересах держави і не переслідують комерційних цілей.

Цивільно-правові договори в галузі інформаційної безпеки можуть укладатися між різними суб'єктами адміністративно-правового забезпечення інформаційної безпеки з метою реалізації цими суб'єктами цивільних прав та обов'язків, що складаються в цій сфері суспільних відносин. Більшість таких договорів укладається з приводу виконання робіт і надання послуг у сфері інформаційної безпеки, до яких відносяться: виробництво, проведення випробувань, закупівля і поставка продукції щодо забезпечення інформаційної безпеки; монтаж, технічне обслуговування і ремонт систем і засобів, що відносяться до цієї сфери тощо. Крім укладення договорів, до дій, які тягнуть за собою певні юридичні наслідки, слід відносити видачу ліцензій, сертифікатів, а також інші дії посадових осіб, спрямовані на створення і збереження необхідного рівня інформаційної безпеки. Такі дії здійснюють переважно державні суб'єкти адміністративно-правового забезпечення інформаційної безпеки під час реалізації покладених на них прав та обов'язків, завдань і функцій.

Ліцензування являє собою процес проходження процедури отримання ліцензії на види господарської діяльності, що підлягають підвищеному контролю з боку держави або спеціальних органів. Завданням цього процесу є досконала перевірка суб'єкта підприємницької діяльності або іншої організації на предмет того, чи є вона достатньо кваліфікованою, відповідальною та обізнаною для надання певних послуг чи виготовлення певних товарів. Такі послуги або товари за замовчуванням мають підвищений ризик негативного впливу на навколишнє середовище та здоров'я громадян. Недостатній рівень кваліфікації суб'єкта, що має справу з постачанням таких товарів, послуг чи виконанням робіт підвищеного ризику може призвести до невідворотних наслідків, збитків. Ліцензія є документом, який готується за визначеними державою стандартами та є офіційним дозволом для ліцензіата здійснювати зазначені в ліцензії види господарської діяльності [6]. Власне кажучи, ліцензія несе в собі правонадільну функцію, оскільки надає конкретним суб'єктам певні права та обов'язки в галузі інформаційної безпеки, тобто наділяє їх спеціальною адміністративною правосуб'єктністю. Порушення умов ліцензування або здійснення цього виду діяльності в галузі інформаційної безпеки без ліцензії тягне за собою юридичну відповідальність.

Видача ліцензії являє собою «офіційне схвалення» органом виконавчої влади певної діяльності суб'єкта права в галузі інформаційної безпеки, що оформляється відповідним індивідуально-правовим актом. Так, питання ліцензування послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України перебуває в компетенції Державної служби спеціального зв'язку та захисту інформації України. Що стосується ліцензування діяльності, пов'язаної з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації, то воно знаходиться в компетенції Служби безпеки України [7]. Усі дії Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України та інших органів щодо видачі ліцензії є юридичними фактами і тягнуть за собою, відповідно, виникнення, зміну або припинення адміністративних правовідносин дозвільного характеру

щодо реалізації прав і виконання обов'язків, передбачених ліцензією.

Сертифікація в сфері інформаційної безпеки є підтвердженням того, що інформаційна система, продукт чи фахівець відповідає певним визначеним стандартам і вимогам безпеки. Стандарти з інформаційної безпеки являють собою критерії, яким повинна відповідати система захисту цифрового контенту. Сертифікація відповідності стандартам кібербезпеки важлива не тільки для забезпечення безпеки власних цифрових систем, але й для відповідності законодавству, яке регулює захист інформації. Сертифікація продукції для захисту комп'ютерних систем визначає, наскільки безпечною є конкретна продукція, така як антивірусне програмне забезпечення, фаєрволи, апаратне забезпечення тощо. Сертифікація мереж стосується локальних мереж, цифрових носіїв інформації. Сертифікація фахівців вказує на те, що фахівець має необхідні знання та навички для контролю за безпекою цифрових мереж та інших вебпродуктів [8]. Після закінчення терміну дії сертифіката або в разі, коли дію сертифіката призупинено чи скасовано, виробники продукції із забезпечення інформаційної безпеки, яка підлягає обов'язковій сертифікації та реалізується на території України, зобов'язані призупинити або припинити її реалізацію, якщо вона не відповідає вимогам інформаційної безпеки. Без чинного сертифіката, використання інформаційних систем у сфері інформаційної безпеки також стає неприпустимим. Аналогічно, фахівці, чиї сертифікати втратили чинність, втрачають право займатися контролем за безпекою цифрових мереж та інших вебпродуктів. Ця вимога запобігає можливим ризикам, пов'язаним із використанням несертифікованих або застарілих методів захисту інформації, що є критично важливим для підтримання високого рівня інформаційної безпеки.

2. Неправові форми адміністративно-правового забезпечення інформаційної безпеки не призводять до юридичних наслідків і, найчастіше, є результатом вчинення правових дій, тобто застосовуються на підставі вже наявних правових актів, договорів і документів, що мають юридичне значення. Як правило, їх поділяють на дві групи: організаційні та матеріально-технічні. Здійснення тих чи інших дій та заходів, спрямованих на забезпечення інформаційної безпеки, що не тягнуть за собою правових наслідків, залежить від конкретного суб'єкта, його компетенції, завдань і цілей. Однак, на відміну від правових, неправові форми можуть застосовуватися як державними так і недержавними суб'єктами адміністративно-правового забезпечення інформаційної безпеки.

Організаційні заходи не пов'язані безпосередньо з виникненням, зміною та припиненням конкретних правовідносин. Вони здійснюються в процесі поточної діяльності зі створення та підтримання необхідного рівня інформаційної безпеки відповідного об'єкта захисту. Організаційні заходи щодо забезпечення інформаційної безпеки також можна поділити на дві групи:

1. Заходи, спрямовані на забезпечення інформаційної безпеки, що проводяться до виникнення інцидентів з інформаційною безпекою, включають:

– організацію захисту інформаційних систем і даних до моменту можливого порушення, включно з розробленням і впровадженням політик інформаційної безпеки;

– моніторинг та аудит дотримання стандартів інформаційної безпеки в проектуванні та функціонуванні інформаційних систем;

– створення комісій з інформаційної безпеки, відповідальних за реалізацію та дотримання заходів захисту даних;

– розробку планів реагування на інциденти інформаційної безпеки та проведення тренувань з персоналом;

– проведення аудитів інформаційної безпеки, технічних інспекцій інформаційних систем та інформаційної інфраструктури;

– проведення навчань і тренувань з інформаційної безпеки для підрозділів, що відповідають за захист даних;

– перевірку та обслуговування систем захисту даних, включно з кібербезпекою та антивірусним захистом;

– організацію та підтримку волонтерських груп з кібербезпеки тощо.

2. Заходи, спрямовані на забезпечення інформаційної безпеки, що проводяться після інцидентів, пов'язаних із порушеннями інформаційної безпеки, включають:

– оцінку шкоди, заподіяної порушеннями інформаційної безпеки, і виявлення причин цих порушень;

– організацію статистичного обліку інцидентів та їх наслідків;

– аналіз дій реагування на інциденти та оптимізацію процесів гасіння «пожеж» в інформаційних системах;

– проведення занять з персоналом з аналізу інцидентів і тактик їх усунення;

– організацію відшкодування збитків суб'єктам, які постраждали від порушень безпеки тощо.

Такий підхід дає змогу не тільки запобігти можливим порушенням інформаційної безпеки, а й ефективно реагувати на інциденти, що сталися, мінімізуючи їхні можливі негативні наслідки.

Матеріально-технічні дії суб'єктів адміністративно-правового забезпечення інформаційної безпеки мають допоміжне значення. Однак, за їх допомогою матеріально забезпечується можливість здійснення всіх інших форм, у яких виражається діяльність цих суб'єктів. Вони є передумовою для правових та організаційних форм забезпечення інформаційної безпеки. Матеріально-технічні дії в галузі забезпечення інформаційної безпеки включають у себе:

– розробку документів з попереднього планування – створення планів і політик інформаційної безпеки, спрямованих на запобігання, виявлення та реагування на загрози в інформаційній сфері;

– складання довідок, звітів та оглядів – підготовка документації, що відображає рівень інформаційної безпеки, аналіз інцидентів і підготовка рекомендацій щодо поліпшення захисту;

– технічне обслуговування та ремонт – регулярне обслуговування та оновлення інформаційних систем, антивірусного програмного забезпечення, фаєрволів тощо;

– ведення статистичної звітності – збір та аналіз даних щодо інцидентів, що сталися, та їхніх наслідків, моніторингу загроз, ефективності вжитих заходів тощо;

– ведення діловодства – заповнення журналів, карток та інших документів для обліку конкретних дій, пов'язаних з інформаційною безпекою, та забезпечення їх відповідності нормативним вимогам;

– заповнення бланків документів з юридичним значенням – правильне оформлення всіх документів, що стосуються інформаційної безпеки, які можуть мати юридичні наслідки, такі як угоди про нерозголошення, політики безпеки тощо;

– складання планів – планування ресурсів, задіяних у забезпеченні інформаційної безпеки, розробка планів на випадок інцидентів тощо.

Діяльність, пов'язана із забезпеченням інформаційної безпеки, виражена в тій чи іншій формі, регулюється правовими нормами. Однак, необхідно враховувати, що не всяка правова форма цієї діяльності, регулюється адміністративним правом. Адміністративно-правовим регулюванням охоплюється діяльність, яку здійснюють у сфері інформаційної безпеки, переважно органи виконавчої влади, виконавчі органи місцевого самоврядування (під час впливу на поведінку людей і діяльність юридичних осіб, які не перебувають із ними в субординаційному підпорядкуванні), а також посадові особи державних органів, органів місцевого самоврядування, адміністрації підприємств та установ (під час впливу на своїх підлеглих)

та громадські об'єднання (щодо осіб, які не є членами їхньої родини), та громадські організації (щодо осіб, які не є членами їхньої родини). Зазначена діяльність спрямована на підтримання нормального функціонування різних підсистем забезпечення інформаційної безпеки і має виконавчо-розпорядчий, управлінський характер. Відповідно, форми вираження цієї діяльності слід називати формами управління (у тому числі державного управління) забезпечення інформаційної безпеки. Останні відносяться до форм забезпечення інформаційної безпеки як часткове до загального. Власне кажучи, з усього різноманіття форм забезпечення інформаційної безпеки, адміністративно-правовому регулюванню піддаються тільки форми управління системою забезпечення інформаційної безпеки.

Важливими складовими адміністративно-правового забезпечення інформаційної безпеки, що здійснюється у проаналізованих нами формах, є технологічне, кадрове, матеріальне, фінансове, інформаційне та наукове забезпечення.

Технологічне забезпечення являє собою сукупність методичного забезпечення та технологічного інструментарію, які використовуються суб'єктами адміністративно-правового забезпечення інформаційної безпеки в інтересах виконання покладених на них функцій з протидії загрозам інформаційній безпеці. Методичне забезпечення інформаційної безпеки являє собою комплекс технічних норм і стандартів, що регулюють захист інформаційної інфраструктури, включно з інформаційно-телекомунікаційними системами, мережами зв'язку та системами автоматизованого управління різними галузями, підприємствами і технологічними процесами. Ці стандарти безпеки розробляються для забезпечення узгодженої взаємодії між виробниками, споживачами, а також експертами з кваліфікації та сертифікації сучасних інформаційних технологій. Вони формують загальні вимоги та керівництва з оцінки та забезпечення безпеки, створюючи надійну основу для захисту від потенційних загроз. Технологічний інструментарій, який використовується для захисту інформаційної безпеки, містить широкий спектр технічних і програмних засобів. Ці інструменти призначені для забезпечення захисту інформаційно-телекомунікаційних систем, систем зв'язку та інших систем обробки інформації від несанкціонованого доступу та дій. Застосування цих засобів дає змогу контролювати й управляти доступом до ресурсів, а також запобігати неавторизованим операціям із критично важливою інформацією. Розроблення та застосування цих стандартів і технологій не тільки зміцнюють захист інформаційних систем, а й сприяють підвищенню рівня довіри до інформаційних технологій, поліпшенню їхньої якості та безпеки.

Кадрове забезпечення інформаційної безпеки являє собою інтегровану систему освітніх і професійних процесів, спрямованих на підготовку, перепідготовку та ефективне використання фахівців для реалізації завдань із захисту інформаційних ресурсів. Ця система включає в себе не тільки нормативно-правові акти, що регулюють процес навчання, а й навчально-методичні матеріали, а також мережу освітніх установ, які здійснюють підготовку кваліфікованих кадрів у цій сфері. В Україні підготовка фахівців з інформаційної безпеки проводиться відповідно до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого Постановою Кабінету Міністрів України від 29.04.2015 р. № 266 (в редакції Постанови Кабінету Міністрів України від 07.07.2021 р. № 762) [9]. Спеціалізація в галузі інформаційних технологій, виділена в окремий напрям («12 Інформаційні технології»), що підкреслює стратегічну важливість та актуальність розвитку компетенцій у сфері інформаційної безпеки. Система кадрового забезпечення не обмежується лише здобуттям особою базової освіти, вона також включає програми по стажуванню, перекваліфікації, підвищенню кваліфікації тощо, що дає змогу фахівцям у галузі інформаційної безпеки постійно підтримувати та розвивати свої навички відповідно до мінливих технологій і загроз у цій сфері. Такий підхід забезпечує не лише теоретичну підготовку, а й практичні навички, необхідні для ефективного реагування на сучасні виклики в галузі захисту інформації.

Матеріальне, фінансове та інформаційне забезпечення є компонентами ресурсного забезпечення в рамках протидії загрозам інформаційній безпеці. Ці види забезпечення формуються на основі систематичного розподілу та використання відповідних ресурсів, які необхідні для ефективної роботи із захисту інформаційних систем і даних. Здебільшого матеріальні, фінансові та інформаційні ресурси зосереджені переважно в ключових органах виконавчої влади, на які покладається основна відповідальність за здійснення конкретно-предметної діяльності у сфері протидії загрозам інформаційній безпеці. Адекватне ресурсне забезпечення таких органів критично важливе для спроможності держави ефективно реагувати на інформаційні виклики сьогодення.

Наукове забезпечення інформаційної безпеки охоплює комплекс наукових теорій, методологій і технік, що дають змогу систематично аналізувати й розуміти природу загроз інформаційній безпеці, їхні джерела та механізми розвитку, а також розробляти стратегії та методи для їхньої нейтралізації. Цей процес включає застосування передових наукових підходів, отриманих з різних дисциплін, таких як інформатика, кібернетика, соціологія, психологія та ін., для глибокого аналізу і розуміння комплексних взаємодій в інформаційній сфері. Наукове забезпечення у сфері інформаційної безпеки спрямоване на розроблення та вдосконалення теоретичних засад захисту інформації, методів виявлення та протидії кібератакам, а також на формування ефективних політик і практик, здатних знизити ризики та мінімізувати потенційний збиток від інформаційних загроз. Важливою частиною цього процесу є дослідження й адаптація нових наукових знань для підвищення стійкості інформаційної інфраструктури та забезпечення цілісності й доступності даних. Наукові дослідження в цій царині включають комплексний аналіз поточного стану інформаційної безпеки, виявлення нових загроз і векторів атак, а також розробку і тестування нових технологій захисту інформації. Це забезпечує базу для формування стратегічного бачення і практичної реалізації заходів зі зміцнення інформаційної безпеки на національному та міжнародному рівнях.

Висновки. Отже, діяльність суб'єктів адміністративно-правового забезпечення інформаційної безпеки в Україні може виражатися як у правових, так і неправових формах. Правові форми тягнуть за собою юридичні наслідки і за змістом поділяються на: правотворчі (видання нормативно-правових актів) і правозастосовні (ухвалення рішень у конкретних справах і правових суперечках, що виникають у процесі функціонування системи забезпечення інформаційної безпеки). Неправові форми адміністративно-правового забезпечення інформаційної безпеки не спричиняють юридичних наслідків і, найчастіше, є результатом вчинення правових дій, тобто застосовуються на підставі вже наявних правових актів, договорів і документів, що мають юридичне значення. Їх ми поділили на дві основні групи: організаційні та матеріально-технічні. Організаційні заходи не пов'язані безпосередньо з виникненням, зміною та припиненням конкретних правовідносин. Вони здійснюються в процесі поточної діяльності зі створення та підтримання необхідного рівня інформаційної безпеки відповідного об'єкта захисту. За допомогою матеріально-технічних дій забезпечується можливість здійснення всіх інших форм, у яких виражається діяльність цих суб'єктів. Вони є передумовою для правових та організаційних форм забезпечення інформаційної безпеки.

ЛІТЕРАТУРА

1. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n5 (дата звернення: 11.06.2024).
2. Андрусів Л. М. Оприлюднення нормативно-правових актів як стадія правотворчості. *Актуальні проблеми вітчизняної юриспруденції*, 2017. № 3. С. 3–5.
3. Калєніченко Л., Слинько Д. Загальнотеоретична характеристика процесуальної підстави юридичної відповідальності. *Jurnalul juridic national: teorie şi practică = Национальный юридический журнал: теория и практика*, 2019. № 2. Ч. 2 (Martie). С. 9–12.
4. Кодекс адміністративного судочинства України від 06.07.2005 р. № 2747-IV. *Відомості Верховної Ради України (ВВР)*, 2005. № 35–36. № 37. Ст. 446.
5. Господарський кодекс України від 16.01.2003 р. № 436-IV. *Відомості Верховної Ради України (ВВР)*, 2003. № 18. № 19–20. № 21–22. Ст. 144.
6. Усе про ліцензування. Західна Консалтингова Група. URL: https://zkg.ua/yurydychni-posluhy-praktyky/pravo-intelektualnoji-vlasnosti/use-pro-litsenzuvannia/ (дата звернення: 14.06.2024).
7. Перелік органів ліцензування, затверджений Постановою Кабінету Міністрів України від 05.08.2015 р. № 609. URL: https://zakon.rada.gov.ua/laws/show/609-2015-%D0%BF#n13 (дата звернення: 14.06.2024).
8. Сертифікація в галузі інформаційної безпеки. URL: https://isocert.org.ua/2023/12/08/sertyfikatsiya-v-haluzi-informatsiynoyi-bezpeky/ (дата звернення: 15.06.2024.)
9. Перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затверджений Постановою Кабінету Міністрів України від 29.04.2015 р. № 266 (в редакції Постанови Кабінету Міністрів України від 07.07.2021 р. № 762). URL: https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF#Text (дата звернення: 17.06.2024).
10. Литвин Н. А., Ярош А. О. Вплив дезінформації на національну безпеку України в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2024. № 2. С. 208–210.
11. *Габрелян А. Ю. Адміністративна відповідальність в галузі охорони інформації. Матеріали конференцій МЦНД, 2021*. URL: https://doi.org/10.36074/mcnd-19.03.2021.law-gov.03 (дата звернення: 17.06.2024).
12. Габрелян А. Ю. Форми адміністративно-правового забезпечення державної політики. *Матеріали конференцій Молодіжної наукової ліги, 2021.* https://ojs.ukrlogos.in.ua/index.php/liga/article/view/9731 (дата звернення: 17.06.2024).
13. Габрелян А. Ю. Методи адміністративно-правового забезпечення державної політики. *Збірник наукових праць ΛΌГОΣ*, 2021 https://doi.org/10.36074/logos-19.03.2021.v1.41 (дата звернення: 17.06.2024).
14. Стрілецька О. В., Габрелян А. Ю. Реалізація принципу змагальності в ході проведення досудового розслідування. *Науковий вісник УжНУ. Серія «Право»*, 2024. Випуск 81(1). С. 168–179.
15. Стрілецька О. В., Габрелян А. Ю. Реалізація принципу змагальності під час судового розгляду. *Аналітично-порівняльне правознавство*, 2024. Випуск 2. С. 719–731.
16. Стрілецька О. В., Габрелян А. Ю. Організаційні проблеми реалізації принципу змагальності у кримінальному процесі. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*, 2024. № 1. С. 328–340.
17. Kreminskyi O., Omelchuk L., Habrelian A., Matsiuk A., Diakovskyi O. Legal regime of virtual currency in Ukraine: current state, problems and prospects of regulation. *Revista Relações Internacionais do Mundo Atual*, 2024. Vol. 1. № 43. P. 21–24.
18. Melnyk O., Artemenko O., Yarosh A., Lytvyn O., Gabrielyan A. Administrative and legal culture of driving a vehicle as a factor in the social consciousness of a road user. *Revista Relações Internacionais do Mundo Atual*, 2021. № 3(32). URL: http://dx.doi.org/10.21902/Revrima.v3i32.550 (дата звернення: 17.06.2024).