DOI https://doi.org/10.24144/2307-3322.2021.69.44
УДК: 336.7:340.5:347.7

АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ПРОТИДІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ОПЕРАЦІЯМ НА СТРАТЕГІЧНОМУ РІВНІ

Дахно О.Ю.,
Навчально-науковий інститут інформаційної безпеки
та стратегічних комунікацій,
кандидат політичних наук
ORCID: 0000-0003-0542-1544

Дахно О. Ю. Адміністративно-правове регулювання протидії інформаційно-психологічним операціям на стратегічному рівні.

Статтю присвячено дослідженню адміністративно-правового регулювання у сфері протидії інформаційно-психологічним операціям на стратегічному рівні. Визначено поняття та сутність інформаційно-психологічних операцій. Автором проведено аналіз негативних наслідків та небезпеки інформаційно-психологічних операцій; з'ясовано механізм впливу інформаційно-психологічних операцій на населення, військовослужбовців та інші об'єкти впливу.

Охарактеризовано стратегічний рівень протидії інформаційно-психологічним операціям. Обґрунтовано, що особливістю стратегічного рівня протидії інформаційно-психологічним операціям є те, що інструменти публічного управління, які застосовуються на цьому рівень, спрямовані на досягнення стратегічної мети, яка полягає у створенні стійкого стану інформаційної безпеки та інформаційного суверенітету держави.

Проведено аналіз актів законодавства у сфері адміністративно-правового регулювання протидії інформаційно-психологічним операціям на стратегічному рівні. Визначено зміст та охарактеризовано інструменти протидії інформаційно-психологічним операціям на стратегічному рівні.

На підставі аналізу адміністративного законодавства у сфері регулювання протидії інформаційно-психологічним операціям на стратегічному рівні визначено, що основними інструментами такої протидії є розробка, прийняття та оновлення актів стратегічного характеру, які визначають довгострокове планування у сфері захисту інформаційної безпеки держави як складової національної безпеки, формування адекватної та ефективної у довгостроковій перспективі інформаційної політики у сфері оборони, налагодження публічних комунікацій сектору оборони, удосконалення системи підготовки відповідних фахівців, а також модернізація та запровадження у діяльність державних органів цифрових технологій. Автором обґрунтовано необхідність визначення місця Стратегії інформаційної безпеки та інших актів стратегічного характеру у сфері забезпечення інформаційної безпеки в ієрархії актів планування у сферах національної безпеки та оборони України.

Ключові слова: інформаційно-психологічна операція, протидія, адміністративно-правове регулювання, стратегічний рівень.

Dakhno O. Administrative and legal regulation of counteraction to information and psychological operations at the strategic level.

The article is devoted to the study of administrative and legal regulation in the field of counteraction to information and psychological operations at the strategic level. The concept and essence of information-psychological operations are defined. The author analyzes the negative consequences and dangers of information and psychological operations; the mechanism of influence of information and psychological operations on the population, servicemen and other objects of influence is clarified.

The strategic level of counteraction to information and psychological operations is characterized. It is substantiated that the peculiarity of the strategic level of counteraction to information and psychological

operations is that the tools of public administration used at this level are aimed at achieving the strategic goal of creating a stable state of information security and information sovereignty of the state.

The analysis of legislative acts in the field of administrative and legal regulation of counteraction to information and psychological operations at the strategic level is carried out. The content and tools of counteraction to information-psychological operations at the strategic level are determined and characterized.

Based on the analysis of administrative legislation in the field of regulation of counteraction to information and psychological operations at the strategic level, it is determined that the main tools of such counteraction are development, adoption and updating of strategic acts defining long-term planning. and long-term effective information policy in the field of defense, establishing public communications in the defense sector, improving the training of relevant specialists, as well as modernization and implementation of digital technologies in government agencies. The author substantiates the need to determine the place of the Information Security Strategy and other acts of strategic nature in the field of information security in the hierarchy of planning acts in the spheres of national security and defense of Ukraine.

Key words: information-psychological operation, counteraction, administrative-legal regulation, strategic level.

Постановка проблеми. В умовах постійно зростаючої напруги гібридної війни з Росією на фоні стрімкого розвитку новітніх інформаційних технологій усе більшої актуальності набуває проблема протидії інформаційно-психологічним операціям (далі – ІПСО), які стають одним з головних інструментів деструктивного інформаційного впливу на свідомість, систему цінностей, психологічні установки населення, військовослужбовців, правоохоронних органів та інших об'єктів цільового впливу. Небезпека ІПСО зумовлює необхідність розробки комплексного організаційно-правового механізму протидії цьому явищу. Обов'язковим складовим елементом такого механізму є акти адміністративно-правового регулювання, що визначають правові засади, мету та завдання протидії ІПСО, рівні, суб'єкти та об'єкти, методи та засоби такої протидії тощо.

Важливо зазначити, що в Україні протидія ІПСО реалізується на різних рівнях, кожен з яких включає власну систему засобів та методів. Одним з таких є стратегічний рівень, метою якого є досягнення у довгостроковій перспективі стійкого стану інформаційної безпеки та попередження негативного інформаційно-психологічного впливу на цільові об'єкти.

Разом з тим, існуюча на сьогодні система адміністративно-правового регулювання протидії ІПСО на стратегічному рівні потребує подальшого удосконалення.

Тому, основною **метою** цього дослідження є проведення аналізу адміністративно-правового регулювання протидії ІПСО на стратегічному рівні та визначення інструментів такої протидії.

Стан дослідження. Питання щодо методів та засобів протидії ІПСО широко обговорюється у наукових та правових колах. Зокрема, проблеми протидії ІПСО висвітлювалась у роботах таких науковців, як Н. Волошина, І. В. Воробйова, М. Дзюба, В. В. Заборовський, Я. В. Мацегора, Ю. Мороз, І. І. Приходько, Ю. М. Твердохліб, І. Ю. Юзова та ін.

Водночас, наукові дослідження у цій сфері присвячені, головним чином, засобам протидії ІПСО в окремих сферах або умовах, зокрема: в умовах ведення гібридних війн (Ю. Мороз, Ю. М. Твердохліб, І. Ю. Юзова та ін.), у середовищі військовослужбовців або у правоохоронних органах (Н. Волошина, І. В. Воробйова, М. Дзюба, Я. В. Мацегора, І. І. Приходько та ін.) тощо. Однак, комплексних наукових досліджень, присвячених адміністративно-правовим засадам регулювання протидії ІПСО на стратегічному рівні, в Україні не достатньо.

Викладення основного матеріалу. Дослідження адміністративно-правового регулювання протидії ІПСО на стратегічному рівні передбачає окреслення основних інструментів публічного управління, а також засобів, за допомогою яких досягається стратегічна мета протидії ІПСО та реалізація яких урегульована актами адміністративно-правового законодавства.

Визначаючи стратегічну мету протидії ІПСО, важливо з'ясувати напрямки негативного впливу цих операцій.

У науковій літературі під ІПСО розуміють комплекс заздалегідь спланованих, узгоджених та реалізованих дій та заходів професійно підготовленими агентами держави-супротивника, що застосовують для захоплення та абсолютного контролю над свідомістю суспільства та здійснення подальших впливів на нього методом психологічних тисків та маніпуляцій із застосуванням істинної та/або не-

правдивої інформації задля його дестабілізації, дезорієнтації та підготовки до успішного проведення політичних або військових дій [1, с. 98].

У Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України, затвердженій наказом Міністерства оборони України від 22 листопада 2017 р. № 612, інформаційні операції визначаються, як узгоджені за метою, завданнями, місцем і часом з іншими діями військ (сил) інтегроване використання можливостей з інформаційного впливу для порушення, зриву, перехоплення або іншого деструктивного впливу на процеси прийняття рішень противником при одночасному захисті власного інформаційного простору [2].

У свою чергу, інформаційно-психологічний вплив являє собою цілеспрямоване розроблення і поширення спеціальної актуальної інформації, здатної безпосередньо або непрямо впливати на суспільну свідомість, психологію і поведінку населення, військовослужбовців. При цьому інформація психологічного і пропагандистського характеру може бути не тільки усного, друкованого, письмового, аудіо і візуального походження, але й екстрасенсорного, телепатичного й іншого типу, розрахована, насамперед, на підсвідомість реципієнта впливу [3, с. 62].

Зважаючи на те, що інформаційно-психологічний вплив здійснюється, головним чином, на емоційну сферу свідомості на основі некритичного сприйняття інформації особистістю, то, на відміну від пропагандистського впливу, він базується на дещо нижчому рівні критичності й свідомості психіки індивіда. Зниження рівня усвідомленості є однією з умов ефективності цього впливу, оскільки у процесі прийняття інформації функціонує тільки сприйняття й запам'ятовування, діяльність мислення «випадає» або дуже послаблюється [4, с. 35].

Отже, ІПСО є сучасним та ефективним інструментом підриву інформаційного суверенітету держави, створення загрози національній безпеці, передусім, такої її складової, як інформаційна безпека, та досягнення сприятливої емоційно-психологічної ситуації для реалізації відповідних політичних, військових чи інших заходів, спрямованих на досягнення цілей суб'єктів ІПСО.

У свою чергу, протидія ІПСО реалізується за допомогою відповідної системи інструментів та засобів, вибір яких залежить від рівня, на якому здійснюється така протидія.

Досліджуючи психологічний аспект інформаційно-психологічної протидії в Національній гвардії України, І. В. Воробйова, Я. В. Мацегора та інші виокремлюють таку систему засобів запобігання інформаційно-психологічному впливу протидіючої сили: своєчасне визначення початку ІПСО з боку протидіючих сил; безперервне і психологічно доцільне суспільно-політичне та бойове інформування особового складу, роз'яснення цілей і завдань ведення протидіючою стороною підривних дій; перекриття або встановлення повного контролю над каналами інформаційно-психологічного впливу протидіючої сторони; розвідку, придушення та знищення сил і засобів ІПСО з боку протидіючих сил; виховання в особового складу переконань в справедливості боротьби, вірності присязі, віри у командирів та начальників, упевненості в силі й надійності власної зброї; нарощування матеріально-технічної бази інформаційно-психологічного впливу на свої війська і населення [5, с. 37].

Протидія ІПСО на стратегічному рівні спрямована, головним чином, на формування відносно стійкого стану інформаційної безпеки держави із використанням механізму стратегічного планування та загальнонаціонального стратегічного регулювання.

Адміністративно-правовою основою протидії ІПСО на стратегічному рівні є: Конституція України [6], закони України «Про національну безпеку України» [7], «Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях» [8], «Про основні засади забезпечення кібербезпеки України» [9], Указ Президента України «Питання Центру протидії дезінформації» [10] та ін.

Аналіз цих законодавчих актів свідчить про те, що одним з інструментів протидії ІПСО на стратегічному рівні є розробка, прийняття та оновлення актів стратегічного характеру, які визначають довгострокове планування у сфері захисту інформаційної безпеки держави як складової національної безпеки, окреслюють завдання та строки їх реалізації, а також засоби, необхідні для цього ресурси та очікувані результати. Притім суб'єктами стратегічного планування в Україні є Президент України, Кабінет Міністрів України, Міністерство оборони України, Рада національної безпеки і оборони України, а також робочий орган останнього – Центр протидії дезінформації та ін.

Зокрема, на сьогодні діють: укази Президента України від 14 вересня 2020 р. № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 р. «Про Стратегію національної безпеки України» [11], від 28 грудня 2021 р. № 685/2021 «Про рішення Ради національної без-

пеки і оборони України від 15 жовтня 2021 р. «Про Стратегію інформаційної безпеки» [12], Доктрина публічного спілкування, затверджена Головнокомандувачем Збройних Сил України від 19 вересня 2020 р. № ВКП-18(00).01 [13], наказ Міністерство оборони України від 22 листопада 2017 р. № 612 «Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України» [2], розпорядження Кабінету Міністрів України від 27 грудня 2018 р. № 1100-р «Про схвалення Стратегії інформаційної реінтеграції Автономної Республіки Крим та м. Севастополя» [14] та ін.

Як слідує зі змісту положень ч. 1 ст. 26 Закону України «Про національну безпеку України», основним документом довгострокового планування, яким визначаються основні напрями державної політики у сфері національної безпеки, є Стратегія національної безпеки України, яка розробляється за дорученням Президента України протягом шести місяців після його вступу на пост [7].

Водночас аналіз положень Розділу V «Планування у сферах національної безпеки і оборони» Закону України «Про національну безпеку України» свідчить про те, що у ньому не визначено місце Стратегії інформаційної безпеки України в ієрархії актів стратегічного характеру сектору оборони. Проте, така Стратегія затверджена рішенням Ради національної безпеки і оборони України від 15 жовтня 2021 р. та уведена у дію Указом Президента України від 28 грудня 2021 р. № 685/2021.

Стратегією інформаційної безпеки України визначено сім стратегічних цілей, серед яких, зокрема й протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу тощо; інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, до загальноукраїнського інформаційного простору; створення ефективної системи стратегічних комунікацій та ін. [12].

При цьому, зазначається, що протидія ІПСО, дезінформації та іншим заходам, спрямованим на створення загроз інформаційній безпеці, здійснюватиметься шляхом виконання таких завдань: визначення системи протидії дезінформації та інформаційним операціям, спрямованої на запобігання, максимально швидке виявлення та реагування держави і суспільства на інформаційні загрози; ужиття заходів щодо запобігання та протидії поширенню дезінформації та деструктивної пропаганди стосовно європейської та євроатлантичної інтеграції України; розвиток спроможностей складових сил оборони щодо протидії загрозам в інформаційному просторі; посилення відповідальності за поширення недостовірної інформації (дезінформації); запровадження дієвих механізмів виявлення, фіксації, обмеження доступу та/або видалення з українського сегмента мережі Інтернет інформації, розміщення якої обмежено або заборонено законом тощо [12].

Важливим інструментом протидії ІПСО на стратегічному рівні є формування адекватної сучасним умовам та ефективної у довгостроковій перспективі інформаційної політики Міністерства оборони України, яка відповідно до Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України є складовою державної інформаційної політики, спрямованої на вирішення комплексу питань, які стосуються: формування інформаційної політики відповідно до функцій і завдань Міністерства оборони та Збройних Сил; взаємодії із засобами масової інформації; висвітлення діяльності Міністерства оборони; забезпечення інформаційної безпеки та інформаційного забезпечення в Міністерстві оборони та Збройних Силах; впровадження нових інформаційних технологій у діяльність Міністерства оборони [2].

Реалізація Стратегії інформаційної безпеки України, Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України спрямовано на: запобігання, виявлення та припинення проявів сепаратизму, тероризму, екстремізму, припинення діяльності незаконних збройних формувань, політично мотивованого насильства та інших зазіхань на конституційний лад; отримання повної і достовірної інформації про ситуацію в Україні та світі, протидія зовнішнім загрозам національній безпеці України, сприяння реалізації національних інтересів України та ін. [11].

З цього приводу важливо також зазначити, що 19 вересня 2020 р. Головнокомандувачем Збройних Сил України затверджено Доктрину публічного спілкування, в якій окреслено методи публічного спілкування використовується для розповсюдження думок, ідей, що базуються на стратегічних наративах, серед загальної або цільової, зовнішньої або внутрішньої аудиторії. При цьому формами публічного спілкування визначені такі, як: публічні виступи, відкриті публічні заходи, участь у телевізійних та радіо-програмах, публікації в друкованих та електронних ЗМІ, рекламні щити та інші інформаційно-комунікаційні продукти, спрямовані на досягнення основної мети публічного спілкування [13].

Таким чином, Доктрина публічного спілкування спрямована на визначення стратегічних наративів, формування соціально-політичних, державотворчих та інших цінностей, які потребують утвердження у суспільній свідомості та відповідно до яких має відбуватися подача інформації в усіх формах публічного спілкування.

Необхідно також погодитись із думкою В. В. Заборовського про те, що впровадження інформаційних технологій у збройних силах є нагальною вимогою сучасності, оскільки перевага у часі та ступені інформованості стає неодмінною умовою перемоги у війні, що переконливо доводить досвід останніх збройних конфліктів і локальних війн [15, с. 31].

З метою удосконалення інформаційно-технологічного оснащення сектори оборони та національної безпеки Указом Президента України від 22 жовтня 2021 р. № 544/2021 введено у дію рішення Ради національної безпеки і оборони України від 22 жовтня 2021 р. «Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України». Реалізація Концепції розрахована на період до 2025 року та складається з двох етапів. Результатом першого етапу має стати актуалізація законодавства України з питань організації та діяльності Державної служби спеціального зв'язку та захисту інформації України, реалізація пріоритетних проектів у сфері спеціального зв'язку.

За результатами другого етапу має бути модернізовано державну систему урядового зв'язку та впроваджено ключові новації у сфері захисту інформації, завершено оптимізацію організаційних структур органів та підрозділів Державної служби спеціального зв'язку та захисту інформації України [16].

Крім того, протидія ІПСО на стратегічному рівні потребує підвищення кваліфікації військовослужбовців та інших працівників сектору оборони та національної безпеки у частині формування вмінь та навичок щодо використання цифрових технологій у своїй діяльності, тобто удосконалення цифрової грамотності військовослужбовців, підвищення їх інформаційної культури тощо.

Висновки. За результатами проведеного дослідження можна зробити наступні висновки.

1. ІПСО передбачає здійснення інформаційно-психологічного впливу на емоційно-вольову сферу людини, а також суспільну свідомість, що у підсумку призводить до негативних наслідків, які можуть виражатися у спотвореному сприйнятті змісту та сутності певних явищ та подій, дезорієнтації у цих подіях, формуванні хибних уявлень та орієнтирів тощо; ІПСО є сучасним та ефективним інструментом підриву інформаційного суверенітету держави, створення загрози національній безпеці, передусім, такої її складової, як інформаційна безпека, та досягнення сприятливої емоційно-психологічної ситуації для реалізації відповідних політичних, військових чи інших заходів, спрямованих на досягнення цілей суб'єктів ІПСО.

2. На стратегічному рівні протидії ІПСО реалізуються, головним чином, завдання щодо формування відносно стійкого стану інформаційної безпеки держави із використанням механізму стратегічного планування та загальнонаціонального стратегічного регулювання. Інструментами протидії ІПСО на стратегічному рівні є: розробка, прийняття та оновлення актів стратегічного характеру, які визначають довгострокове планування у сфері захисту інформаційної безпеки держави як складової національної безпеки, формування адекватної та ефективної у довгостроковій перспективі інформаційної політики у сфері оборони, налагодження публічних комунікацій сектору оборони, удосконалення системи підготовки відповідних фахівців, а також модернізація та запровадження у діяльність державних органів цифрових технологій.

3. Актами адміністративно-правового регулювання протидії ІПСО є Конституція та закони України, укази Президента України, розпорядження Кабінету Міністрів України, накази Міністерства оборони України, що визначають систему актів планування у сферах національної безпеки та оборони України, окреслюють стратегічну мету протидії ІПСО, методи та засоби досягнення цієї мети, суб'єктів протидії ІПСО, ресурси, необхідні для такої протидії. З метою удосконалення адміністративно-правового регулювання протидії ІПСО доцільно у Законі України «Про національну безпеку України» визначити місце Стратегії інформаційної безпеки та інших актів стратегічного характеру у сфері забезпечення інформаційної безпеки в ієрархії актів планування у сферах національної безпеки та оборони України.

Список використаних джерел:

1. Мороз Ю., Твердохліб Ю. Інформаційно-психологічні операції в умовах ведення гібридної війни. Вісник Львівського університету. Серія: Міжнародні відносини. 2016. Вип. 38. С. 97-105.

2. Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України: наказ Міністерство оборони України від 22.11.2017 № 612. URL : https://zakon.rada.gov.ua/rada/show/v0612322-17#Text.

3. Юзова І. Ю., Пацек П. Інформаційно-психологічний вплив противника та протидія йому в умовах ведення гібридних війн. Наука і техніка Повітряних Сил Збройних Сил України, 2020, № 3(40). С. 61-68.

4. Волошина Н., Дзюба М. Вироблення у майбутніх офіцерів імунітету проти негативного інформаційно-психологічного впливу. Вісник Київського національного університету ім. Тараса Шевченка. 2013. № 30. С. 34-37.

5. Воробйова І. В., Мацегора Я. В., Приходько І. І. та ін. Інформаційно-психологічна протидія в Національній гвардії України (психологічний аспект) : монографія; за заг. ред. проф. І.І. Приходька; 2-ге вид. Х. : Національна акад. НГУ, 2016. 265 с.

6. Конституція України від 28.06.1996 № 254к/96-ВР. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

7. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text.

8. Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях: Закон України від 18.01.2018 № 2268-VIII. URL : https://zakon.rada.gov.ua/laws/show/2268-19#Text.

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

10. Питання Центру протидії дезінформації: Указ Президента України від 7 травня 2021 року № 187/2021. URL : https://www.president.gov.ua/documents/1872021-38841.

11. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 № 392/2020. URL : https://zakon.rada.gov.ua/laws/show/392/2020#Text.

12. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 № 685/2021. URL : https://zakon.rada.gov.ua/laws/show/685/2021#n7.

13. Доктрина публічного спілкування: затверджено Головнокомандувачем Збройних Сил України від 19 вересня 2020 року № ВКП-18(00).01. URL : https://www.mil.gov.ua/content/standarts/doktryna_pyblick_spilk_20200919.pdf.

14. Про схвалення Стратегії інформаційної реінтеграції Автономної Республіки Крим та м. Севастополя: розпорядження Кабінету Міністрів України від 27 грудня 2018 р. № 1100-р. URL : https://zakon.rada.gov.ua/laws/show/1100-2018-%D1%80#Text.

15. Заборовський В. В. Інформаційно-психологічний вплив на супротивника у війнах: історичний досвід. Психологічні та педагогічні проблеми професійної освіти та патріотичного виховання персоналу системи МВС України. Харків, 2020. С. 29-32.

16. Про рішення Ради національної безпеки і оборони України від 22 жовтня 2021 року «Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України»: Указ Президента України від 22.10.2021 № 544/2021. URL : https://zakon.rada.gov.ua/laws/show/544/2021#Text.