ВИДИ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ХАРАКТЕРИСТИКА ЇХ ПОВНОВАЖЕНЬ[1]

ДУМЧИКОВ Михайло Олександрович - кандидат юридичних наук, старший викладач кафедри кримінально-правових дисциплін та судочинства Навчально-наукового інституту права Сумського державного університету
ORCID: https://orcid.org/0000-0002-4244-2419,
e-mail: m.dumchykov@yur.sumdu.edu.ua
УДК 342.841
DOI 10.32782/EP.2023.3.31

Стаття присвячена комплексному системному аналізу та еволюційному підходу до вивчення однієї з актуальних теоретико-правових проблем адміністративного та інформаційного права, зокрема – види органів державної влади в сфері забезпечення інформаційної безпеки та визначення їх основних повноважень. Зазначається, що у зв'язку з військовою агресією Російської Федерації питання інформаційної безпеки держави та підвищення рівня ефективності забезпечення інформаційної безпеки особи та захисту її інформаційних прав стає актуальною в умовах розвитку цифрових технологій.

В статті здійснено аналіз чинної нормативно-правової бази системи забезпечення інформаційної безпеки України та структури органів державної влади, що беруть участь у реалізації державної інформаційної політики. Розглянуті напрями діяльності у сфері прав особи на інформаційну безпеку Верховної Ради України, Президента України, Кабінету Міністрів України, Міністерства цифрової трансформації України, Служби безпеки України, Державної спеціальної служби спеціального зв'язку та захисту інформації України, Міністерства культури та інформаційної політики та інших центральних органів виконавчої влади з метою розробки та удосконалення нормативно-правової бази і практичної реалізації заходів, спрямованих на забезпечення прав людини на інформаційну безпеку. Суб'єкти формування та реалізації політики державної безпеки в інформаційній сфері можна систематизувати за декількома критеріями. Перш за все, це відносний рівень участі у виробленні та втіленні державної політики інформаційної безпеки, що включає як державні суб'єкти на різних рівнях управління, так і недержавні структури. Другий критерій - функціональне навантаження, оскільки суб'єкти можуть виконувати дослідницько-інформаційні, організаторські та реалізаційні завдання в контексті інформаційної безпеки. І, нарешті, важливим аспектом є врахування статусу суб'єктів, що може відображати їхнє приналежність до органів влади або організацій, які не пов'язані з державним управлінням.

Ключові слова: інформаційна безпека, кібербезпека, національна безпека, національна інформаційна безпека, суб'єкти забезпечення інформаційної безпеки, національна оборона.

Постановка проблеми

Сьогодні безпека всієї держави, суспільства та конкретної особи, в тому числі і інформаційна, представляє собою складне та багаторівневе явище, яке одночасно може виступати як процес і показник стану реалізації національних інтересів. Важливим елементом для ефективного функціонування системи забезпечення інформаційної безпеки держави є її суб'єктний склад, компетенція суб'єктів забезпечення інформаційної безпеки та належна організація взаємодії між ними.

[1] «Виконання завдань перспективного плану розвитку наукового напряму «Суспільні науки» Сумського державного університету» (номер державної реєстрації БФ/24-2021, термін виконання 2021-2025 роки).

Стан дослідження проблеми

Питання сучасного стану суб'єктів забезпечення інформаційної безпеки держави та визначенням спектру їх повноважень було предметом наукового інтересу багатьох вчених. Зокрема, Малашко О.Є., Єсімов С.С., Прав Р.Ю., Олійник О.В., Кормич Б.А., Федченко Д. І., Довгань О.Д. та інших. Водночас, враховуючи швидкі темпи цифровізації, діджиталізації та власне перенесення більшості загроз у кіберпростір, постали виклики, щодо модернізації системи забезпечення інформаційної безпеки та визначення основних повноважень субєктів забезпечення інформаційної безпеки.

Мета і завдання дослідження

Метою дослідження є аналіз системи суб'єктів забезпечення інформаційної безпеки держави, окреслення їх основних компетенцій шляхом аналізу законодавства України.

Виклад основного матеріалу

Сучасні загрози інформаційній безпеці України, зокрема системна інформаційна війна, поширення дезінформації та інформації пропаганди, що впливає на розвиток суспільства, несформованість інформаційної концепції та стратегії поширення інформації та протидії інформаційним загрозам, а також низький рівень кібергігієни суспільства, стали каталізаторами створення системи інформаційної безпеки. В цій системі необхідна ефективна та згуртована взаємодія суб'єктів, що формують та реалізують політику державної безпеки в інформаційній сфері.

Варто зауважити, що з моменту анексії Криму та початку військових дій на сході держави, в Україні активно розвивається нормативно-правова база, щодо забезпечення інформаційної безпеки держави. Зокрема, в цей період було прийнято ряд ключових документів: 1) Стратегія національної безпеки; 2) Стратегія кібербезпеки; 3) Закон України «Про основні засади забезпечення кібербезпеки України»; 4) Доктрина інформаційної безпеки України; 5) Закон України «Про національну безпеку України»; 6) стратегія інформаційної безпеки. Особливістю вищезазначених нормативно-правових актів виступає і визначення кола суб'єктів, щодо формування та реалізації політики забезпечення інформаційної безпеки в державі. Водночас на наше переконання, прогресивних взаємодій між собою зазначені суб'єкти не мають [1, с. 50].

Основним суб'єктом в забезпеченні права особи на інформаційну безпеку виступає держава, водночас, така обставина зумовлюється наявністю в її компетенції відповідних прав і повноважень, щодо створення спеціальних органів, інститутів та служб, функціональна діяльність яких пов'язана з забезпечення інформаційної безпеки. Суб'єкти формування та реалізації політики державної безпеки в інформаційній сфері можна розділити на дві основні категорії: 1) органи державної влади України (різних рівнів та сфер життєдіяльності, органи місцевого самоврядування); 2) суб'єкти, що функціонують поза системою державного управління: підприємства та організації різних форм власності і господарювання, громадські об'єднання, асоціації та інші організації громадянського суспільства [2].

Відповідно до рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» Рада національної безпеки і оборони України відповідно до Конституції України та у встановленому законом порядку здійснює координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері, зокрема з використанням спроможностей Центру протидії дезінформації [3].

В свою чергу Кабінет Міністрів України відповідає за формування та реалізацію інформаційної політики держави, гарантує інформаційний суверенітет, фінансує програми, пов'язані з інформаційною безпекою, а також спрямовує та координує діяльність міністерств та інших органів виконавчої влади в цій сфері, розробляє та затверджує план заходів з реалізації Стратегії, на основі якого відповідні органи виконавчої влади впроваджують заходи щодо забезпечення інформаційної безпеки.

Органи державної влади спільно з органами місцевого самоврядування, Центром

протидії дезінформації та інститутами громадянського суспільства взаємодіють для забезпечення реалізації Стратегії відповідно до плану заходів, який отримує затвердження від Кабінету Міністрів України. Центральний орган виконавчої влади, що забезпечує формування та реалізацію державної політики в інформаційній сфері: 1) здійснює в межах компетенції нормативно-правове регулювання у сфері інформаційної безпеки України; 2) визначає перспективи та пріоритетні напрями розвитку у сфері інформаційної безпеки України; 3) разом із Міністерством закордонних справ України сприяє популяризації та формуванню позитивного іміджу України у світових інформаційних ресурсах та національних інформаційних ресурсах іноземних держав з метою захисту її політичних, економічних та соціально-культурних інтересів, зміцнення національної безпеки і відновлення територіальної цілісності України [3].

Міністерство оборони України, а також сили оборони в межах компетенції забезпечують: 1) моніторинг інформаційного простору (аналіз та виявлення інформаційних загроз національній безпеці в сфері оборони, зокрема у воєнній сфері); 2) підготовка та проведення інформаційних заходів (розробка та координація заходів із забезпечення інформаційної безпеки держави, залучення суб'єктів забезпечення національної безпеки); 3) розвиток системи стратегічних комунікацій (створення та удосконалення системи передачі стратегічних повідомлень та комунікацій для сил оборони); 4) забезпечення інформаційної безпеки в сфері оборони (здійснення заходів щодо правового, організаційного, технічного та іншого характеру для забезпечення інформаційної безпеки, включаючи захист інформаційного середовища та зв'язків у військових частинах та дислокаційних місцях); 5) зв'язки з ЗМІ (взаємодія з українськими та іноземними ЗМІ для висвітлення ситуації та подій, пов'язаних із заходами національної безпеки та оборони, зокрема у зоні збройного конфлікту з Російською Федерацією); 6) протидія інформаційним операціям (заходи для запобігання та стримування інформаційних операцій, спрямованих проти Збройних Сил та інших військових формувань України); 7) достовірна інформація для військовослужбовців (передача достовірної інформації військовослужбовцям Збройних Сил України та іншим складовим сил оборони) [3].

Ключовими учасниками у системі стратегічних комунікацій Міністерства оборони та Збройних Сил України є керівництво, прес-секретар, помічник начальника Генерального штабу, а також ряд структурних підрозділів, таких як Управління комунікацій та преси, Управління інформаційних технологій, відділ стратегічних комунікацій, управління зав'язків з громадськістю, відділ координації стратегічних комунікацій та моніторингу, та інші [4].

Функції Управління комунікацій та преси полягають у впровадженні державної інформаційної політики в структурах Міністерства оборони та Збройних Сил України, організації інформаційно-роз'яснювальної діяльності для підвищення престижу військової служби, формування позитивної громадської думки щодо Збройних Сил, а також виконання завдань в інформаційній сфері. Це включає забезпечення ефективного функціонування системи інформування громадськості та взаємодію із засобами масової інформації [5].

СБУ комплексно забезпечує контррозвідувальний захист інформаційної та кібернетичної безпеки держави, зокрема здійснює моніторинг інформаційного простору за допомогою спеціальних методів і засобів, як вітчизняних, так і зарубіжних ЗМІ та Інтернету, спрямований на виявлення потенційних загроз національній безпеці України в інформаційній сфері. Паралельно, відбувається протидія проведенню спеціальних інформаційних операцій проти України, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності, а також на загострення суспільно-політичної та соціально-економічної ситуації у країні [6, с. 655].

Розвідувальні органи України у процесі провадження розвідувальної діяльності мають сприяти реалізації та захисту національних інтересів України в інформаційній сфері за кордоном, здійснювати виявлення та протидію зовнішнім інформаційним за-

грозам у сфері безпеки та оборони держави. Національна рада України з питань телебачення і радіомовлення відповідно до компетенції бере участь у забезпеченні захисту українського інформаційного простору від пропагандистської аудіовізуальної продукції держави-агресора, сприяє розповсюдженню українського телерадіомовлення на тимчасово окупованих територіях України [7].

Верховна Рада України, як орган законодавчої влади, активно сприяє забезпеченню інформаційної безпеки держави через прийняття та вдосконалення законодавчих актів, що регулюють інформаційну політику та здійснення заходів національної безпеки в інформаційному просторі.

Органи прокуратури України реалізують свої повноваження в сфері інформаційної безпеки відповідно до норм Конституції України та відповідних законодавчих актів. Здійснюють контроль з дотримання чинного законодавства у сфері інформаційної безпеки, сприяючи таким чином забезпеченню цілісності та безпеки інформаційного простору України відповідно до актуальних вимог та викликів цієї області [8, с. 487].

Міністерство культури та інформаційної політики України є головним органом в системі органів виконавчої влади з питань забезпечення інформаційного суверенітету держави, здійснює координацію з питань поширення суспільно важливої інформації в Україні та за її межами. Серед основних завдань Міністерства культури та інформаційної політики варто виділити саме моніторинг засобів масової інформації та ресурсів Інтернет мережі, зокрема щодо виявлення загроз у сфері інформаційної безпеки. Разом з Міністерством закордонних справ України сприяє у донесенні офіційної позиції держави до іноземних засобів масової інформації, формує пріоритет державної інформаційної політики на світовій арені. Він також відповідає за урядові та кризові комунікації, а також за впровадження стратегії інформаційного забезпечення процесу звільнення та реінтеграції тимчасово окупованих територій, розроблення та впровадження єдиних стандартів підготовки фахівців у сфері урядових комунікацій [9].

В свою чергу Міністерство закордонних справ здійснює формування та реалізація стратегії публічної та культурної дипломатії України; координація інформаційної діяльності державних органів у зовнішньополітичній сфері; забезпечення просування інтересів України за кордоном інформаційними засобами; забезпечення донесення позиції України до керівництва іноземних держав, парламентів та урядів, зовнішньополітичних відомств, представників бізнесу та експертних кіл, широкої громадськості, сприяння просуванню позитивного іміджу України; сприяння просуванню українських телеканалів у кабельні та супутникові мережі за кордоном; забезпечення налагодження взаємодії з міжнародними партнерами як на двосторонній, так і на багатосторонній основі з метою застосування міжнародного досвіду та найкращих практик у контексті протидії інформаційним загрозам.

Національний інститут стратегічних досліджень здійснює науково-аналітичне та експертне супроводження процесу формування та реалізації державної інформаційної політики [10, с. 9].

Варто відзначити, що перелік суб'єктів, які можуть брати участь у проведенні політики інформаційного захисту фактично не є вичерпним, і він не обмежується органами державної влади чи місцевого самоврядування. Таким чином, суб'єктами процесу забезпечення інформаційної безпеки є не лише органи державної влади, але й недержавні суб'єкти, відповідно до нормативно-правових актів, які регулюють відносини у галузі інформаційної безпеки в державі. Розуміння інституційного механізму, незалежно від того, чи є воно широким, чи вузьким, не охоплює суттєвого суб'єкта забезпечення інформаційної безпеки - громадян України, обмежуючи коло учасників виключно державними та недержавними інституціями. Тому вважаємо, що термін «інституційний механізм інформаційної безпеки» є більш вузьким поняттям порівняно з терміном «суб'єкти забезпечення інформаційної безпеки» [11, с. 166].

Можна в упевненістю констатувати факт, що на сьогодні вже існує впорядкована система суб'єктів, відповідальних за формуван-

ня та втілення політики державної безпеки в інформаційній сфері. Проте, ця система потребує оптимізації взаємодії, ретельного контролю за кількістю та функціями кожного її елементу для уникнення дублювання обов'язків. Додатково, є необхідність вдосконалити механізм взаємодії суб'єктів, зокрема, у сферах розвитку електронного урядування та автоматизації процедур для підвищення ефективності цієї системи.

Висновок

Сьогодні Україна крокує на шляху свого євроінтеграційного розвитку, навіть у контексті повномасштабної військової агресії з боку Російської Федерації. Ця війна активно використовується Росією у сфері інформаційної боротьби. З урахуванням зростання негативного зовнішнього впливу на інформаційний простір України, проблеми забезпечення інформаційної безпеки набувають особливого значення. Оптимізація правових та організаційних механізмів управління інформаційною безпекою, включаючи систему суб'єктів цієї області, стає важливою умовою для ефективної реалізації стратегічних пріоритетів, принципів та завдань державної політики інформаційної безпеки.

На сьогоднішній момент ефективне впровадження політики забезпечення інформаційної безпеки вимагає вдосконалення організаційно-функціонального забезпечення інформаційної безпеки, значної оптимізації системи державних органів, що відповідають за цю сферу. Це передбачає чітке визначення та розмежування повноважень цих органів, встановлення ефективної взаємодії та координації всіх суб'єктів забезпечення інформаційної безпеки, а також здійснення контролю за дотриманням чинного законодавства. Створення міжвідомчої структури з представництвом основних суб'єктів забезпечення інформаційної безпеки при Раді національної безпеки й оборони України або надання Службі безпеки України додаткових координуючих повноважень може слугувати запорукою для розроблення узгоджених рішень щодо напрямів і заходів забезпечення реалізації державної політики інформаційної безпеки.

Література

1. Малашко О.Є., Єсімов С.С. Зміст державної діяльності із забезпечення інформаційної безпеки. Міжнародний науковий журнал «Інтернаука». 2020. № 15 (95). Т. 1. С. 46–54.

2. Прав Р.Ю. Діяльність суб'єктів формування і реалізації політики державної безпеки в інформаційній сфері України. URL: http://www.dy.nayka.com.ua/pdf/9_2018/103.pdf

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

4. Про затвердження концепції стратегічних комунікацій Міністерство оборони України та Збройних Сил, Наказ МОУ № 612 від 22.11.2017. URL: http://www.mil.gov.ua/content/mou_orders/612_nm_2017.pdf

5. Управління комунікацій та преси Міністерства оборони України. URL: http://www.mil.gov.ua/ministry/struktura-aparatu-ministerstva/upimou.html

6. Федченко Д. І. Система забезпечення кібербезпеки: проблеми формування та ефективної діяльності. Молодий вчений. № 5 (57). 2017. С. 653-658.

7. Шеломенцев В. П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. № 2. С. 299-309. URL: http://nbuv.gov.ua/UJRN/boz_2012_2_36.

8. Олійник О. В. Структура суб'єктів забезпечення інформаційної безпеки в Україні. Актуальні проблеми держави і права. № 68. 2016. С. 485-491.

9. Указ Президента України: Про рішення Ради національної безпеки і оборони України № 47/2017 від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: https://zakon.rada.gov.ua/laws/show/47/2017

10. Довгань О. Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 3 (19). С. 6-17.

11. Кормич Б. А. Організаційноправові засади політики інформаційної безпеки України. Одеса, 2003. 472 с.

АНОТАЦІЯ

The article is devoted to a complex system analysis and an evolutionary approach to the study of one of the current theoretical and legal problems of administrative and information law, in particular - the types of state authorities in the field of ensuring information security and determining their main powers. It is noted that in connection with the military aggression of the Russian Federation, the issue of information security of the state and increasing the level of efficiency in ensuring the information security of a person and protecting his information rights is becoming relevant in the context of the development of digital technologies.

The article analyzes the current normative and legal framework of the information security system of Ukraine and the structure of state authorities participating in the implementation of the state information policy. The considered areas of activity in the field of individual rights on information security of the Verkhovna Rada of Ukraine, the President of Ukraine, the Cabinet of Ministers of Ukraine, the Ministry of Digital Transformation of Ukraine, the Security Service of Ukraine, the State Special Service for Special Communication and Information Protection of Ukraine, the Ministry of Culture and Information Policy and other central executive authorities with the aim of developing and improving the legal framework and practical implementation of measures aimed at ensuring human rights to information security. Subjects of formation and implementation of state security policy in the information sphere can be systematized according to several criteria. First of all, it is the relative level of participation in the development and implementation of the state information security policy, which includes both state entities at different levels of management and non-state structures. The second criterion is functional load, as subjects can perform research and informational, organizational and implementation tasks in the context of information security. And finally, an important aspect is taking into account the status of subjects, which may reflect their affiliation to authorities or organizations that are not related to public administration.

Keywords: information security, cyber security, national security, national information security, entities providing information security, national defense.