

УДК: 65.012.8:007+32(477)

*Р. Ю. Прав,  
аспірант, Міжрегіональна академія управління персоналом, м. Київ*

## **ДІЯЛЬНІСТЬ СУБ'ЄКТІВ ФОРМУВАННЯ І РЕАЛІЗАЦІЇ ПОЛІТИКИ ДЕРЖАВНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СФЕРІ УКРАЇНИ**

*R. Yu. Prav  
Postgraduate Student, Interregional Academy of Personnel Management, Kyiv*

### **Activity of the subjects of formation and implementation of the policy of state security in the information sphere of Ukraine**

*У статті автором визначено роль суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері.*

*Систематизовано класифікацію суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері: відносно рівня вироблення та реалізації державної політики інформаційної безпеки (державні суб'єкти різних рівнів та недержавні); відносно функціонального навантаження (суб'єкти, що виконують дослідницько-інформаційні, організуючі та реалізуючі функції); відносно статусу суб'єктів (органи влади та організації, що не пов'язані з державним управлінням). Визначено, що суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері можна розділити на дві основні категорії: органи державної влади України (різних рівнів та сфер життєдіяльності, органи місцевого самоврядування); 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. Встановлено, що спеціалізовані органи влади, що формують і реалізують політику національної безпеки, а саме Рада національної безпеки і оборони України, і її профільний комітет здійснюють моніторинг та дослідження загального рівня загроз інформаційної безпеки, вивчення стану та ефективності реалізації стратегій та програм, метою яких є підвищення рівня інформаційної безпеки, подають пропозиції щодо нейтралізації загроз інформаційного характеру. Верховна Рада України, а саме Комітет з питань інформації та зв'язку, формують та розглядають пропозиції внесення законодавчих змін у сферах: електронного обігу, телекомунікацій, розвитку інформаційного суспільства, національної програми інформатизації, захисту системи електронних інформаційних ресурсів.*

*Сформовано визначення системи інформаційної безпеки як сукупності взаємовідносин між суб'єктами інформаційного простору, які здійснюють цілеспрямований вплив на об'єкти інформаційної інфраструктури на основі комплексу заходів у вигляді стратегічних, урядових та кризових комунікацій. Доведено провідну роль суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері. Запропоновано системний підхід формування системи інформаційної безпеки. Зазначено, що інформаційно-психологічна війна, приниження української мови і культури, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу виступають одними з актуальних загроз інформаційної безпеки України.*

*In the article the author defined the role of the subjects of formation and implementation of the policy of state security in the information sphere.*

*The classification of the subjects of formation and implementation of the state security policy in the information sphere is systematized: regarding the level of development and implementation of the state policy of information security (state entities of different levels and non-state actors); relative to the functional load (subjects performing research and information, organizing and implementing functions); with regard to the status of subjects (authorities and organizations not associated with public administration). It is determined that the subjects of formation and implementation of the state security policy in the information sphere can be divided into two main categories: the bodies of state power of Ukraine (different levels and spheres of vital activity, bodies of local self-government); entities operating outside the system of public administration: enterprises and organizations of various forms of ownership and management, public associations, associations and other organizations of civil society. It has been established that the specialized authorities that form and implement the national security policy, namely the National Security and Defense Council of Ukraine, and its specialized committee monitor and study the general level of information security threats, study the status and effectiveness of the implementation of strategies and programs aimed at increase the level of information security, submit proposals on the neutralization of threats of informational character. The Verkhovna Rada of Ukraine, namely the Committee on Information and Communication, forms and considers proposals for introducing legislative changes in the areas of electronic circulation, telecommunications, information society development, national information programs, and the protection of the electronic information resources system.*

*The definition of the information security system as a set of relationships between the subjects of the information space, which has a purposeful influence on the objects of information infrastructure on the basis of a set of measures in the form of strategic, government and crisis communications, has been formed. The leading role of the subjects of formation and implementation of the state security policy in the information sphere is proved. A systematic approach to the formation of an information security system is proposed. It was pointed out that information-psychological warfare, humiliation of the Ukrainian language and culture, the formation of Russian media by the alternative to the reality of the distorted information picture of the world are one of the topical threats to Ukraine's information security.*

**Ключові слова:** *інформаційна безпека, інформаційна політика, суб'єкти інформаційної безпеки, інформаційна інфраструктура, інформаційна сфера, інформаційний простір.*

**Key words:** *information security, information policy, subjects of information security, information infrastructure, information sphere, information space.*

**Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями.** Загрози інформаційній безпеці України, зокрема системна інформаційна війна, поширення неправдивої, видозміненої інформації, що впливає на розвиток суспільства, несформованість інформаційної концепції та стратегії поширення інформації та протидії інформаційним загрозам, недостатній рівень медіа-культури суспільства, потребують формування системи інформаційної безпеки, в якій відбуватиметься ефективна та злагоджена взаємодія суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері. Впродовж 2015-2017 років в Україні активно розвивається та вдосконалюється правова база (ухвалено Стратегію національної безпеки України (2015 р.) [18], Стратегію кібербезпеки (2016 р.) [19], Доктрину інформаційної безпеки України (2016 р.) [17], Закон України «Про основні засади забезпечення кібербезпеки України» (2017 р.) [15], Закон України «Про національну безпеку України» (2017 р.) [14] тощо). У зазначених нормативно-правових актах визначено основних суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері, проте на разі не забезпечено високий рівень ефективності їх взаємодії.

**Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми, виділення не вирішених раніше частин загальної проблеми.** Державній політиці безпеки в інформаційній сфері присвячено праці науковців, таких як: В. В. Антонюк [1], І. Р. Березовська, Д. М. Русак [2], О. Д. Довгань [4], В. В. Зайцев [5], В. О. Негодченко [7], О. В. Олійник [8], В. Г. Пилипчук [9], Д. І. Федченко [21], В. П. Шеломенцев [22] та інші науковці.

У своїй праці В. В. Зайцев визначає суб'єктів забезпечення інформаційної безпеки України. Зокрема, автор робить висновок про те, що забезпечення окремих питань інформаційної безпеки покладаються на велику кількість різних державних органів, компетенція яких стосується різних сфер державного управління, вони мають різну підпорядкованість [5]. У роботі В. О. Негодченко вперше проведено класифікацію суб'єктів інформаційної політики [7]. Забезпечення системного покращення державної політики у інформаційній сфері,

реформування ключових напрямків підвищення рівня безпеки та протидії інформаційних загроз ускладнює роботу суб'єктів управління.

**Формулювання цілей статті (постановка завдання).** Визначення ролі суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері.

**Виклад основного матеріалу дослідження з обґрунтуванням отриманих наукових результатів.**

Інформаційно-психологічна війна, приниження української мови і культури, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу виступають одними з актуальних загроз інформаційної безпеки України. Несформованість сектору безпеки і оборони України в інформаційній сфері як цілісного функціонального об'єднання, керованого з єдиного центру; інституційна слабкість, непрофесійність, структурна незбалансованість органів сектору інформаційної безпеки і оборони; неефективне використання ресурсів у секторі інформаційної безпеки і оборони та ряд інших проблем зумовлюють неефективність системи забезпечення національної безпеки і оборони України в інформаційній сфері [18]. Зазначені проблеми потребують ефективної, злагодженої взаємодії суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері.

На сьогодні в Україні відбувається активне формування системи інформаційної безпеки – система взаємовідносин між суб'єктами інформаційного простору, які здійснюють цілеспрямований вплив на об'єкти інформаційної інфраструктури на основі комплексу заходів у вигляді планових, оперативних, кризових та ризик-комунікацій. Таким чином, з поданого визначення, що найбільш повно відображає цілі дослідження, випливає, що суб'єкти інформаційної політики є головним елементом системи національної безпеки в інформаційній сфері України, від дій якого залежить стан, тенденції та ефективність реалізації політики.

У роботі Д. І. Федченко подано наступне визначення системи забезпечення інформаційної безпеки – це комплексна та узгоджена діяльність спеціально уповноважених міжнародними та національними нормами суб'єктів забезпечення інформаційної безпеки, покликана запобігти виникненню та реалізації загроз інформаційного простору, а у відповідних випадках – усунути їх негативний вплив [21, с. 654].

В. О. Негодченко наводить загальну характеристику суб'єктів забезпечення державної інформаційної політики, особливого значення автор надає органам Національної поліції України. Крім того, у дослідженні доведено складність процесу забезпечення державної інформаційної політики, що зумовлюється значною кількістю суб'єктів, які беруть у ньому участь (окремі суб'єкти виступають одночасно як суб'єкти формування та суб'єкти реалізації такої політики) [7]. Саме тому, у Стратегії кібербезпеки України від 15 березня 2016 року № 96/2016 визначено, що національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури [19]. Отже, проблематика забезпечення взаємодії суб'єктів є одним з пріоритетних завдань інформаційної політики, адже від цього залежить ефективність її реалізації.

В. О. Негодченко пропонує класифікувати вказані суб'єкти на державні та недержавні [7]. З такою класифікацією можна погодитися, адже недержавні суб'єкти володіють більшою часткою інформаційної інфраструктури, а тому суттєво впливають на державну інформаційну політику.

О. Д. Довгань у своїй роботі класифікує суб'єктів на:

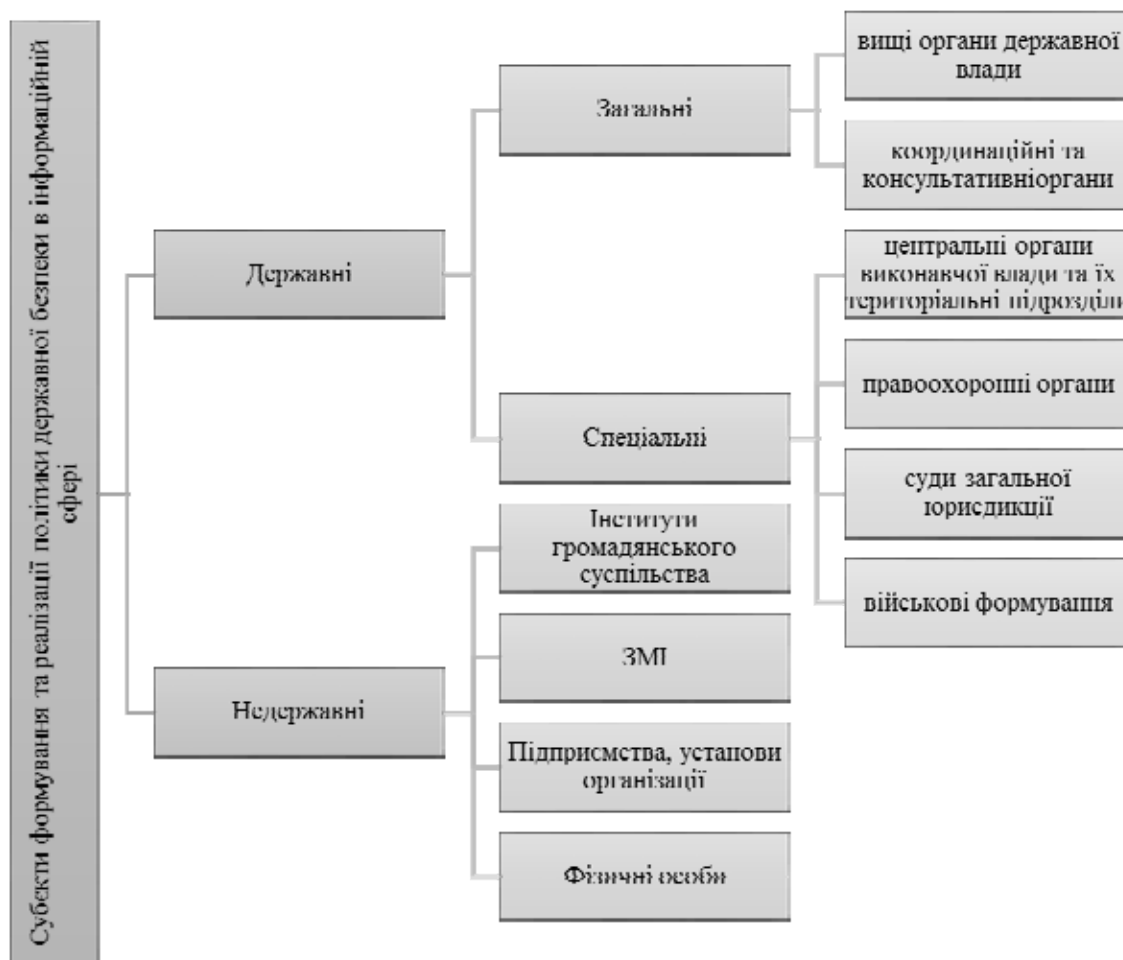
1. Суб'єкти з інформаційно-аналітичними функціями щодо аналізу загроз [4, с. 15].

2. Суб'єкти з організаційно-управлінськими функціями (прийняття рішень, програмування й планування) [4, с. 15].

3. Суб'єкти з безпосередньо виконавчими функціями [4, с. 15].

Державну інформаційну політику та політику національної безпеки визначає Верховна Рада України, у складі якої діють такі профільні комітети: з питань свободи слова та інформаційної політики; з питань інформатизації та зв'язку; з питань національної безпеки і оборони [9, с. 25].

Ще у 2002 році при РНБО України було утворено Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки [12], до складу якої за посадою входять керівники чи заступники міністерств, відомств, правоохоронних органів, представники Генерального штабу Збройних Сил України, державних комітетів, комітетів Верховної Ради України, наукових та дослідних установ, діяльність яких пов'язана з проблематикою інформаційної безпеки [22, с. 302].



**Рис. 1. Система суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері**

*Джерело: складено та доповнено автором на основі [7]*

Враховуючи наведені дослідниками системи класифікації суб'єктів управління, що розподілені на державних та недержавних суб'єктів та інші різновидності класифікації, узагальнено ці класифікації.

Суб'єкти формування та реалізації політики державної безпеки в інформаційній сфері можна розділити на дві основні категорії:

- органи державної влади України (різних рівнів та сфер життєдіяльності, органи місцевого самоврядування);
- 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.

При цьому, якщо суспільство може здійснювати як позитивний, так і негативний вплив на об'єкти інформаційного простору на національному та регіональному рівнях, що має прояв у поширенні та пропагуванні війни, національної, релігійної ворожнечі, то органи виконавчої влади здатні впливати на дії суспільства шляхом формування та реалізації державної інформаційної політики на національному та міжнародному рівнях. Як зазначає О. Д. Довгань для вжиття дієвих «заходів на загальнодержавному рівні пріоритетами забезпечення інформаційної безпеки є виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності» [4, с. 11].

Таким чином, між визначеними суб'єктами формування та реалізації політики державної безпеки в інформаційній сфері існує тісний зв'язок: якщо суспільство має можливість сприяти реалізації інформаційної політики, то органи виконавчої влади є єдиним суб'єктом, що забезпечує її формування та від якого залежить ефективність її реалізації. Крім того, органи державної влади можуть забезпечити участь суспільства у реалізації державної політики безпеки в інформаційній сфері. Останнє набуває вагомому значення, адже підприємства, установи та організації володіють об'єктами інформаційної інфраструктури, є її власниками та розпорядниками, а тому повинні сприяти реалізації інформаційної політики.

Як зазначає В. В. Антонюк «центральні органи державного управління в ході реалізації функцій щодо виявлення загроз інформаційній безпеці держави можуть залучати ОДВ та МС, засоби масової інформації, політичні партії та рухи, громадські організації та професійні спілки, неурядові дослідницькі організації, а також інші організації та установи, що здійснюють діяльність в інформаційній сфері» [1].

Зважаючи на тісний зв'язок між суб'єктами формування та реалізації політики державної безпеки в інформаційній сфері, в Україні потрібно здійснювати інформаційну політику на основі системного підходу, де кожен суб'єкт повинен розуміти власну відповідальність за дії та комунікації в інформаційному просторі, наслідки таких дій для національної безпеки країни. Як зазначають І. Р. Березовська, Д. М. Русак [2], «в рамках державної інформаційної політики важливо зосередитись на формуванні в середовищі користувачів таких загальнообов'язкових норм поведінки, як інформаційна культура та відповідальне ставлення до використання інформаційного простору». Такої позиції також дотримується: «побудова системи інформаційної безпеки та подальша її реалізація має виходити не лише з норм національного законодавства та можливостей кожної окремої держави, а й ґрунтуватися на нормах міжнародного права та узгодженості дій суб'єктів даної системи, неухильного виконання взятих на себе зобов'язань» [21, с. 654].

Органи державної влади здійснюють формування системи інформаційної безпеки на декількох рівнях:

- законодавчому;
- адміністративному;
- процедурному;
- програмно-технічному [4].

В Україні було прийнято рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [17]. Крім цього, прийнято Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 08.07.2017 [9]. Основними суб'єктами національної системи інформаційної безпеки відповідно Доктрині є: Кабінет Міністрів України, Міністерство інформаційної політики України, Міністерство закордонних справ України, Міністерство оборони України, Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, розвідувальні органи України [17]. Ці суб'єкти забезпечують розробку та реалізацію заходів, визначають обсяги фінансування відповідно напрямку інформаційної безпеки України.

Крім цього, відповідно Доктрині суб'єктами урядових комунікацій в інформаційній сфері є уповноважені представники Кабінету Міністрів України, які реалізують комплекс заходів, що передбачають діалог з цільовою аудиторією з метою роз'яснення урядової позиції та/або політики з певних проблемних питань [17], див. табл. 1.

**Таблиця 1.**

**Органи державного управління, що беруть участь у формуванні і реалізації політики державної безпеки в інформаційній сфері**

№	Суб'єкт	Функції, повноваження у сфері інформаційної безпеки
<b>Загальнодержавні</b>		
1	Президент України, зокрема Рада з питань національної єдності (консультативно-дорадчий орган при Президентові України)	подолання існуючих стереотипів та пропагандистських міфів, спрямованих на руйнування єдності Українського народу; зміцнення існуючих і налагодження нових взаємозв'язків між регіонами у питаннях інформаційних комунікацій [16].
2	Кабінет Міністрів України	урядові комунікації в інформаційній сфері уповноважених представників КМУ, що реалізують комплекс заходів та забезпечують діалог з цільовою аудиторією з метою роз'яснення урядової позиції та/або політики з певних проблемних питань [19]. здійснення інформаційної політики держави, фінансування програм, пов'язаних з інформаційною безпекою, спрямовуватиме і координуватиме роботу міністерств, інших органів виконавчої влади у цій сфері [8].
3	Верховна Рада України	орган законодавчої влади, що виконує повноваження з питань забезпечення інформаційної безпеки, що постають із конституційних повноважень [8].
4	Рада національної безпеки і оборони України Комісія з інформатизації Ради національної безпеки й оборони України	аналіз стану і можливих загроз національній безпеці України в інформаційній сфері; аналіз здійснення галузевих програм і виконання заходів, пов'язаних із реалізацією міністерствами та іншими центральними органами виконавчої влади державної політики в інформаційній сфері; розроблення і внесення Президентові України та Раді національної безпеки і оборони України пропозицій в інформаційній сфері; удосконалення системи оперативного інформаційно-аналітичного забезпечення Президента України (в тому числі альтернативною інформацією) у сфері національної безпеки і оборони та інші функції [12].
<b>Спеціальні або організаційно-функціональні (центральні й місцеві органи виконавчої влади)</b>		
5	Органи прокуратури України	здійснюють свої повноваження у сфері інформаційної безпеки відповідно до Конституції України і законів України, у встановленому порядку забезпечують нагляд за дотриманням чинного законодавства в цій сфері діяльності [8].

6	Органи судової влади	здійснюють правосуддя у справах про злочини у сфері інформаційної безпеки, пов'язаної із замахом на законні інтереси особи, суспільства, держави, забезпечують судовий захист прав суб'єктів у цій сфері діяльності [17].
7	Міністерство інформаційної політики України	головний орган у системі центральних органів виконавчої влади у сфері забезпечення інформаційного суверенітету України, зокрема, з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів. Основні функції: моніторинг ЗМІ та загальнодоступних ресурсів вітчизняного сегмента мережі Інтернет з метою виявлення інформації, поширення якої заборонено в Україні; моніторинг загроз в інформаційній сфері; сприяння Міністерству закордонних справ України щодо донесення офіційної позиції України до іноземних засобів масової інформації; формування поточних пріоритетів державної інформаційної політики, контролю їх реалізації; координації діяльності центральних та місцевих органів виконавчої влади у сфері забезпечення інформаційного суверенітету України; урядові комунікації; кризові комунікації; вжиття заходів в інформаційній сфері, пов'язаних із запровадженням правових режимів надзвичайного чи воєнного стану; розроблення стратегічного нарративу і його імплементація; вироблення і впровадження стратегії інформаційного забезпечення процесу звільнення та реінтеграції тимчасово окупованих територій; розроблення та впровадження єдиних стандартів підготовки фахівців у сфері урядових комунікацій для потреб державних органів [17].
8	Міністерство закордонних справ	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 [17].
9	Міністерство оборони України, Генеральний штаб Збройних Сил України, зокрема відділ стратегічних комунікацій та інші суб'єкти	забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахисту власної інформаційної інфраструктури [19]. зв'язки з українськими та іноземними ЗМІ; протидія спеціальним інформаційним операціям; супроводження інформаційними засобами виконання завдань оборони України; донесення достовірної інформації до військовослужбовців Збройних Сил України, інших військових формувань, зокрема через ЗМІ Збройних Сил України [17].
10	Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України	забезпечення захисту українського інформаційного простору від пропагандистської аудіовізуальної та друкованої продукції держави-агресора; розробка пріоритетів і стимулів розвитку українського кіно, телевізійного контенту, книгодрукування, зокрема висвітлення героїчного спротиву Українського народу російській агресії [17].
11	Служба безпеки України	моніторинг вітчизняних та іноземних ЗМІ та мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері; протидія проведенню проти України спеціальних інформаційних операцій. розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури [17].
12	Державна служба спеціального зв'язку та захисту інформації України	формування і реалізація державної політики у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом України [17]; формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів

		та інформації; кіберзахист критичної інформаційної інфраструктури, державний контроль у цих сферах; проведення аудиту захищеності об'єктів критичної інформаційної інфраструктури на вразливість [19].
13	Національний банк України	формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері [17];
14	Національна поліція України	забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі [17]
15	Національний інститут стратегічних досліджень	забезпечення науково-аналітичного та експертного супроводження процесу формування і реалізації державної інформаційної політики [17].

*Джерело: складено автором.*

Крім цього, при міністерствах функціонують Департаменти стратегічних комунікацій, зокрема при Міністерстві закордонних справ України, Міністерстві оборони та Збройних сил України.

Основними суб'єктами системи стратегічних комунікацій Міністерства оборони та Збройних сил України є керівний склад, прес-секретар, помічник начальника Генерального штабу, Управління комунікацій та преси, Управління інформаційних технологій, відділ стратегічних комунікацій, управління зав'язків з громадськістю, відділ координації стратегічних комунікацій та моніторингу та інші суб'єкти [11]. Управління комунікацій та преси здійснює реалізацію державної інформаційної політики в Міністерстві оборони та Збройних Силах України, ведення інформаційно-роз'яснювальної роботи з питань підвищення престижу військової служби, формування в українському суспільстві позитивної громадської думки щодо Збройних Сил та висвітлення їх діяльності, виконання завдань в інформаційній сфері, забезпечення ефективної діяльності системи інформування громадськості та взаємодії із засобами масової інформації [20].

При Міністерстві інфраструктури України функціонує Департамент забезпечення комунікації та аналітичної роботи, що відповідає за забезпечення висвітлення в засобах масової інформації діяльності керівництва та Міністерства в цілому, взаємодію з органами державної влади та місцевого самоврядування, налагодження ефективної взаємодії з прес-службами центральних органів виконавчої влади, Укрзалізниці, підприємств галузі [3].

При міських радах функціонують Департаменти комунікацій, які забезпечують комунікації влади з громадськістю, боротьбі з дезінформацією, формування суспільної довіри.

Діяльність суб'єктів досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, та повинна базуватися на принципах: забезпечення поваги до прав та свобод громадянина; забезпечення національних інтересів України в сфері інформаційної безпеки; відкритості, стабільності, доступності, захищеності кіберпростору; державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту; невідворотного покарання за вчинення злочинів у сфері інформаційної безпеки; пріоритетного розвитку, підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу [19].

Забезпечення кібербезпеки покладено на такі органи Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи [19].

Отже, на сьогодні існує сформована система суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері. Потребує оптимізації їх взаємодія, контроль кількості елементів цієї системи та контроль їх функцій з метою уникнення дублювання обов'язків. Потребує також вдосконалення механізм взаємодії суб'єктів в частині розвитку електронного урядування та автоматизації процедур взаємодії.

**Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі.** Враховуючи результати дослідження виділено декілька основних ознак класифікації суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері: відносно рівня вироблення та реалізації державної політики інформаційної безпеки (державні суб'єкти різних рівнів та недержавні); відносно функціонального навантаження на суб'єктів щодо формування і реалізації політики (суб'єкти, що виконують дослідницько-інформаційні, організуючі та реалізуючі функції); відносно статусу суб'єктів (органи влади та організації, що не пов'язані з державним управлінням). Перспективними з точки зору подальших досліджень та напрацювань можуть стати вивчення питань функціонального впливу тих чи інших суб'єктів на інформаційну безпеку.

#### **Список використаних джерел.**

1. Антонюк В. В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці / В. В. Антонюк // Державне управління: удосконалення та розвиток. – Випуск 8(10). – 2014. – с. 1-5.
2. Березовська І. Р., Русак Д. М. Державна інформаційна політика та основні напрями її вдосконалення / І. Р. Березовська, Д. М. Русак // Міжнародні відносини. Серія «Економічні науки». – Випуск 4. – 2014. [Електронний ресурс]. – Режим доступу: [http://journals.iir.kiev.ua/index.php/ec\\_n/article/view/2488](http://journals.iir.kiev.ua/index.php/ec_n/article/view/2488)
3. Департамент забезпечення комунікації та аналітичної роботи. [Електронний ресурс]. – Режим доступу: <https://mtu.gov.ua/content/departament-zabezpechennya-komunikacii-ta-analitichnoi-roboti.html>

4. Довгань О. Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки / О. Д. Довгань // Інформаційна безпека людини, суспільства, держави. – 2015. – Випуск 3 (19). – с. 6-17.
5. Зайцев В. В. Суб'єкти забезпечення інформаційної безпеки України / В. В. Зайцев // Форум права. – Випуск 3. – 2013. – с. 231-238.
6. Комітет з питань інформатизації та зв'язку. Електронний ресурс. – Режим доступу: [Електронний ресурс]. – Режим доступу: <http://komit.rada.gov.ua/>
7. Негодченко, В. О. Адміністративно-правове забезпечення державної інформаційної політики органами Національної поліції України : автореф. дис. ... д-ра юрид. наук : 12.00.07 / В. О. Негодченко; МВС України, Харк. нац. ун-т внутр. справ. - Харків, 2017. - 40 с.
8. Олійник О. В. Структура суб'єктів забезпечення інформаційної безпеки в Україні // Актуальні проблеми держави і права. – Випуск 68. – 2016. – с. 485-491.
9. Пилипчук В. Г. Забезпечення інформаційної безпеки України: сучасні тенденції та проблеми: матеріали наук.-практ. конф. / 06 жовт. 2016 р. / Упоряд. : В. М. Фурашев. – Київ : НТУУ «КПІ імені Ігоря Сікорського», Вид-во «Політехніка». – 2016. – С. 24-28.
10. Предмети відання Комітету з питань інформатизації та зв'язку. [Електронний ресурс]. – Режим доступу: [http://komit.rada.gov.ua/news/pro\\_komitet/72756.html](http://komit.rada.gov.ua/news/pro_komitet/72756.html)
11. Про затвердження концепції стратегічних комунікацій Міністерство оборони України та Збройних Сил, Наказ МОУ № 612 від 22.11.2017. [Електронний ресурс]. – Режим доступу: [http://www.mil.gov.ua/content/mou\\_orders/612\\_nm\\_2017.pdf](http://www.mil.gov.ua/content/mou_orders/612_nm_2017.pdf)
12. Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України : Указ Президента України від 22 січ. 2002 р. № 63/2002 // Офіц. вісн. України. – 2002. – № 4. – С. 17. – Ст. 132. – Код акту 21253/2002. – 8 лют.
13. Про Міністерство інформаційної політики України. [Електронний ресурс]. – Режим доступу: <https://mip.gov.ua/content/pro-ministerstvo.html>
14. Про національну безпеку України, Закон України № 2469-VIII, поточна редакція від 21 червня 2017. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2469-19?lang=en>
15. Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII від 08.07.2017. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2163-19/conv>
16. Про Раду з питань національної єдності. Указ Президента України № 697/2015, чинний, поточна редакція від 08.10.2016. [Електронний ресурс]. – Режим доступу: <https://zakon2.rada.gov.ua/laws/show/697/2015>
17. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», Указ Президента України 47/2017, поточна редакція від 25.02.2017. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/47/2017>
18. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», Указ Президента України. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/287/2015#n14>
19. Стратегія кібербезпеки України, Указ Президента України від 15 березня 2016 року № 96/2016. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/96/2016#n11>
20. Управління комунікацій та преси Міністерства оборони України. [Електронний ресурс]. – Режим доступу: <http://www.mil.gov.ua/ministry/struktura-aparatu-ministerstva/upimou.html>
21. Федченко Д. І. Система забезпечення кібербезпеки: проблеми формування та ефективної діяльності / Д. І. Федченко // Молодий вчений. – Випуск 5 (57). 2017. – с. 653-658.
22. Шеломенцев В. П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення / В. П. Шеломенцев // Випуск 2 (28). – 2012. – с. 299-309.

#### References.

1. Antoniuk V. V. (2014) “Mechanisms of state response to modern challenges and threats to information security”, *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, vol. 8, pp. 1-5.
2. Berezovska I. R., Rusak D. M. (2014), “State information policy and the main directions of its improvement”, *Mizhnarodni vidnosyny. Seriya «Ekonomiczni nauky»*, [Online], vol. 4, available at: [http://journals.iir.kiev.ua/index.php/ec\\_n/article/view/2488](http://journals.iir.kiev.ua/index.php/ec_n/article/view/2488) (Accessed 8 September 2017).
3. Ministry of Infrastructure of Ukraine, “Department for communication and analytical work”, available at: <https://mtu.gov.ua/content/departament-zabezpechennya-komunikacii-ta-analitichnoi-roboti.html> (Accessed 8 September 2017).
4. Dovhan O. D (2015) “Legal principles of formation and development of information security system”, *Informatsijna bezpeka liudyny, suspil'stva, derzhavy*, vol. 3, pp. 6-17.
5. Zajtsev V. V. (2013) “Subjects of information security of Ukraine”, *Forum prava*, vol. 3, pp. 231-238.
6. Verkhovna Rada of Ukraine, “Committee on Informatization and Communications”, available at: <http://komit.rada.gov.ua/> (Accessed 9 September 2017).
7. Nehodchenko, V. O. (2017), “Administrative and legal support of the state information policy by the bodies of the National Police of Ukraine”, Ph.D. Thesis, legal science, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine.
8. Olijnyk O. V. (2016) “The structure of the subjects of providing information security in Ukraine”, *Aktualni problemy derzhavy i prava*, vol. 68, pp. 485-491.



9. Pylypchuk V. H. (2016) "Providing of information security of Ukraine: current trends and problems", *Politekhnik*, pp. 24-28.
10. Verkhovna Rada of Ukraine, "Subjects of the Committee on Informatization and Communications", available at: [http://komit.rada.gov.ua/news/pro\\_komitet/72756.html](http://komit.rada.gov.ua/news/pro_komitet/72756.html) (Accessed 9 September 2017).
11. MoD of Ukraine (2017), "On approval of the concept of strategic communications, the Ministry of Defense of Ukraine and the Armed Forces", available at: [http://www.mil.gov.ua/content/mou\\_orders/612\\_nm\\_2017.pdf](http://www.mil.gov.ua/content/mou_orders/612_nm_2017.pdf) (Accessed 8 September 2017).
12. Decree of the President of Ukraine (2002), "On the Interdepartmental Commission on Information Policy and Information Security under the National Security and Defense Council of Ukraine", *Ofitsijnyj visnyk Ukrainy*, vol. 4., p. 17.
13. Ministry of Information Policy of Ukraine (2016) "About the Ministry of Information Policy of Ukraine", available at: <https://mip.gov.ua/content/pro-ministerstvo.html> (Accessed 8 September 2017).
14. The Verkhovna Rada of Ukraine (2017), The Law of Ukraine "On National Security of Ukraine", available at: <https://zakon.rada.gov.ua/laws/show/2469-19?lang=en> (Accessed 8 September 2017).
15. The Verkhovna Rada of Ukraine (2017), The Law of Ukraine "About the basic principles of providing cybersecurity of Ukraine", available at: <https://zakon.rada.gov.ua/laws/show/2163-19/conv> (Accessed 9 September 2017).
16. Decree of the President of Ukraine (2015), "On the Council on National Unity", available at: <https://zakon2.rada.gov.ua/laws/show/697/2015> (Accessed 8 September 2017).
17. Decree of the President of Ukraine (2017), "On the decision of the Council of National Security and Defense of Ukraine dated December 29, 2016 «On the Doctrine of Information Security of Ukraine»", available at: <https://zakon.rada.gov.ua/laws/show/47/2017> (Accessed 8 September 2017).
18. Decree of the President of Ukraine (2015), "On the decision of the National Security and Defense Council of Ukraine dated May 6, 2015 «On the Strategy of National Security of Ukraine»", available at: <https://zakon.rada.gov.ua/laws/show/287/2015#n14> (Accessed 8 September 2017).
19. Decree of the President of Ukraine (2016), "Strategy of cybersecurity of Ukraine", available at: <https://zakon.rada.gov.ua/laws/show/96/2016#n11> (Accessed 8 September 2017).
20. MoD of Ukraine (2013), "Office of Communications and Press of the Ministry of Defense of Ukraine", available at: <http://www.mil.gov.ua/ministry/struktura-aparatu-ministerstva/upimou.html> (Accessed 9 September 2017).
21. Fedchenko D. I. (2017) "Cybersecurity System: Problems of Creation and Effective Activities", *Molodyj vchenyj*, vol. 5, pp. 653-658.
22. Shelomentsev V. P. (2012) "The essence of organizational support of the system of cybernetic security of Ukraine and directions of its improvement", vol. 2, pp. 299-309.

*Стаття надійшла до редакції 20.09.2018 р.*