УДК 327.5:911.3]:316.776.23
DOI https://doi.org/10.32782/2524-0374/2023-2/2

ПРОБЛЕМАТИКА ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА В НОРМАТИВНО-ПРАВОВИХ Й ДОКТРИНАЛЬНИХ ДОКУМЕНТАХ СФЕРИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

PROBLEMS OF INFORMATION WARFARE IN NORMATIVE-LEGAL AND DOCTRINE DOCUMENTS OF THE SPHERE OF NATIONAL SECURITY OF UKRAINE

Вєдєнєєв Д.В., д.і.н.,
головний науковий співробітник
Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при Раді Національної безпеки і оборони України

Семенюк О.Г., д.ю.н.,
перший заступник керівника
Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при Раді Національної безпеки і оборони України

Стаття присвячена формуванню нормативно-правових та доктринальних засад державної політики й діяльності сектору безпеки і оборони України із забезпечення інформаційної безпеки та провадження інформаційного протиборства. Йдеться про базові елементи державної політики інформаційної безпеки України, серед яких створення системи забезпечення інформаційної безпеки (включаючи її правові засади та організаційно-функціональну структуру), реалізацію планової та оперативної діяльності із запобігання та усунення загроз та дестабілізуючих чинників супроти національних інтересів в інформаційній сфері, налагодження міжнародного співробітництва в сфері інформаційної безпеки. Розкриваються положення стосовно відсічі загрозам безпеці України в інформаційній сфері таких документів як «Доктрина інформаційної безпеки України», введена в дію Указом Президента України (2017 р.), Стратегія національної безпеки України «Безпека людини – безпека країни» (2020 р.), «Концепція забезпечення національної системи стійкості» (2021 р.), Стратегія воєнної безпеки України «Воєнна безпека – всеохоплююча оборона» (2021 р.).

Розглядається управлінське-координаційний механізм протистояння загрозам в інформаційній сфері на загальнодержавному рівні, оснований на розподілі компетентності у цій області між уповноваженими відомствами в «силовому блоці» держави. Аналізується Закон України «Про оборону України», «Концепція стратегічних комунікацій Міністерства оборони України та Збройних Сил України». Висвітлюється унормування відповідних функцій Служби безпеки України із протидії проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету України, розвідувальних органів України із сприяння захисту національних інтересів в інформаційній сфері за кордоном.

Ключові слова: національна безпека, інформаційна безпека, інформаційне протиборство, законотворчість, стратегічне планування, безпекові доктрини.

The article is devoted to the formation of normative-legal and doctrinal foundations of state policy and activities of the security and defense sector of Ukraine to ensure information security and the implementation of information warfare. These are the basic elements of the state information security policy of Ukraine, including the creation of a system for ensuring information security (including its legal basis and organizational and functional structure), implementation of planned and operational activities to prevent and eliminate threats and destabilizing factors against national interests in the information sphere, international cooperation in the field of information security. The provisions regarding countering threats to the security of Ukraine in the information sphere of such documents as the «Doctrine of Information Security of Ukraine», put into effect by the Decree of the President of Ukraine (2017), the National Security Strategy of Ukraine «Human Security – the Security of the Country» (2020), «The concept of ensuring the national stability system» (2021), the military security strategy of Ukraine «Military security – comprehensive defense» (2021).

The management and coordination mechanism for countering threats in the information sphere at the national level is considered, based on the distribution of competence in this area between the authorized departments in the «power block» of the state. The Law of Ukraine «On the Defense of Ukraine», «Concept of Strategic Communications of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine» is analyzed. The normalization of the relevant functions of the Security Service of Ukraine to counteract the conduct of special information operations against Ukraine, aimed at undermining the constitutional order, violation of Ukraine's sovereignty, and intelligence agencies of Ukraine to assist in the protection of national interests in the information sphere abroad is highlighted.

Key words: national security, information security, information warfare, law-making, strategic planning, security doctrines.

В оборонно-безпековому будівництві доводиться враховувати сутність сучасних війн (по відношенню до яких використовується ціла лінійка близьких за змістом понять: «безконтактні», «нетрадиційні», «асиметричні», «гібридні», «мережевоцентричні»), котрі в комплексі використовують усі інструменти: політичні, економічні, інформаційні, воєнні тощо. Сучасні «поведінкові» війни ведуться з акцентом на дезорієнтацію свідомості населення противника за рахунок множини узгоджених впливів різної природи, включаючи інформаційно-психологічний чинник [див.: 1–4].

Захист інформаційного суверенітету України, національного інформаційного простору та конституційних прав і свобод громадян, суспільства і держави у цій сфері виступає одним із пріоритетних напрямів оборонно-безпекової політики держави, що потребує активізації нормативно-правового та концептуального забезпечення цих зусиль. Серед основних здобутків наріжних ознак (елементів) державної політики щодо інформаційної безпеки України, яка сформувалася за період незалежності, дослідники виокремлюють:

створення системи забезпечення інформаційної безпеки (включаючи її правові засади, цілепокладання, організаційно-функціональну структуру тощо);

реалізацію планової та оперативної діяльності щодо забезпечення інформаційної безпеки;

запобігання та усунення загроз та дестабілізуючих чинників супроти національних інтересів в інформаційній сфері;

локалізацію та ліквідацію наслідків інформаційних конфліктів або впливу дестабілізуючих чинників;

налагодження міжнародного співробітництва в сфері інформаційної безпеки, із входженням в існуючі та утворенням нових профільних двосторонніх і багатосторонніх структур (організацій), діяльність яких спрямована на вирішення проблем інформаційної безпеки тощо [5–6].

Зазначимо, що від 2015 року для доктринальних документів України у сфері воєнної безпеки властивими стали підвищення уваги до інформаційних чинників загроз безпеці держави та визначення форм протидій у цій царині [7–8]. Розглянемо процес формування нормативно-правових та доктринальних засад державної політики й діяльності сектору безпеки і оборони України із забезпечення інформаційної безпеки та провадження інформаційного протиборства.

Стаття 17 Конституції України віднесла забезпечення інформаційної безпеки до найважливіших функцій держави та справи всього Українського народу. Стратегія національної безпеки України «Безпека людини – безпека країни» від 2020 року серед існуючих та прогнозованих загроз національній безпеці та національним інтересам України визначила стрімке зростання ролі інформаційних технологій у всіх сферах суспільного життя, розробку систем озброєнь із використанням нових інформаційних технологій, посилення міжнародної конкуренції із застосуванням інформаційно-психологічних «інструментів національної сили». Підкреслювалася небезпека зовнішньої деструктивної пропаганди та внутрішніх гуманітарних проблем, що призводило до розпалення суспільної ворожнечі та національної єдності, ускладнених відсутністю продуманої інформаційної політики держави та незадовільним станом системи стратегічних комунікацій. З-поміж стратегічних завдань висувалася настанова про розробку пакету документів щодо планування у сферах національної безпеки і оборони, включаючи Стратегії інформаційної та кібернетичної безпеки України [9].

Одне із чільних місць відводилося проблематиці заисту національного інформаційного простору у запровадженій у вересні 2021 р. «Концепції забезпечення національної системи стійкості», яка спрямовувалася на забезпечення здатності держави і суспільства своєчасно ідентифікувати загрози, вразливості та ризики національній безпеці, запобігати або мінімізувати їх негативні впливи, ефективно реагувати й відновлюватися після виникнення загроз або настання надзвичайних та кризових ситуацій усіх видів, включаючи загрози гібридного типу. Самі загрози гібридного типу трактувалися як «різновид загроз національній безпеці, реалізація яких спричиняє синергетичний ефект від одночасного застосування комбінованих методів впливу, які часто мають прихований характер або маскуються під інші процеси у рамках правового поля», що само по собі мало на увазі і загрози інформаційно-комунікаційній сфері життєдіяльності держави [10–11]. Серед базових елементів національної системи стійкості (по суті – наріжних підвалин життєдіяльності держави і суспільства) передбачалися – суспільна стійкість до інформаційних впливів, захищеність та безперебійне функціонування інформаційних та комунікаційних послуг, кібербезпека.

«Доктрина інформаційної безпеки України», введена в дію Указом Президента України від 25 лютого 2017 р. [12] неоднозначно вказувала на перетворення інформаційної сфери на ключову арену міждержавного протиборства. Підкреслювалося, що інформаційні технології впливу на свідомість громадян здатні провокувати насильницьке повалення державного ладу, порушення суверенітету і територіальної цілісності України, розпалювання національної і релігійної ворожнечі. Завданням держави поставало «визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації».

Захист держави та українського суспільства від руйнівних інформаційно-психологічних впливів та агресивної деструктивної пропаганди відносився до життєве важливих інтересів України в інформаційній сфері. Серед актуальних загроз національним інтересам в інформаційній сфері називалися, зокрема, проведення спеціальних інформаційних операцій, скерованих на підрив обороноздатності й деморалізацію особового складу військових формувань, провокування екстремістських проявів, дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів, формування негативного іміджу України на міжнародній арені.

До числа пріоритетів державної політики в інформаційній сфері (у частині забезпечення інформаційної безпеки та інформаційного протиборства) згаданий документ відносив:

створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; розбудову структур, що відповідають за інформаційно-психологічну безпеку (передовсім – у ЗС України), з урахуванням стандартів і досвіду держав-членів НАТО;

розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України;

побудову ефективної системи стратегічних комунікацій;

«посилення спроможностей сектору безпеки і оборони щодо протидії спеціальним інформаційним операціям, спрямованим на зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності, підрив обороноздатності України, деморалізацію особового складу Збройних Сил України та інших військових формувань, загострення суспільно-політичної ситуації»;

діяльність розвідувальних органів України із сприяння захисту національних інтересів в інформаційній сфері, нейтралізації зовнішніх загроз інформаційній безпеці держави за межами України.

Положення Доктрини значно удосконалили управлінське-координаційний механізм протистояння загрозам в інформаційній сфері на загальнодержавному рівні, визначили розподіл компетентності у цій області між відомствами. Зокрема, визначився подібний розподіл і в силовому блоці держави.

До відповідних функцій *Міністерства оборони України* віднесли:

інформаційне забезпечення антитерористичної операції в Донецькій та Луганській областях;

протидію спеціальним інформаційним операціям, спрямованим проти Збройних Сил, інших військових формувань України;

супроводження інформаційними засобами виконання завдань оборони України;

донесення достовірної інформації до військовослужбовців Збройних Сил України, інших військових формувань.

Служба безпеки України у зобов'язувалася здійснювати:

моніторинг спеціальними методами вітчизняних та іноземних ЗМІ, мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері;

протидію проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій.

Розвідувальні органи України мали б сприяти захисту національних інтересів України в інформаційній сфері за кордоном, протидіяти зовнішнім загрозам інформаційній безпеці держави.

Оскільки розгортання сучасної інформаційної боротьби та перетворення кіберпростору в можливий театр воєнних дій нерозривно пов'язані із протиборством в кіберпросторі, важливим стало ухвалення у 2021 р. «*Стратегії кібербезпеки України*» [13] задля «посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому серед-

овищі». Документ підкреслював значущість ескалації кіберзагроз в світовому контексті розвитку інформаційних технологій та технологій штучного інтелекту, здатну створити нову безпекову ситуацію для дієздатності функціонування національних і транснаціональних структур управління (на фоні конфронтації у міждержавних стосунках з приводу поділу сфер впливу у кіберпросторі). Констатувалися можливості кібервійськ із проведення превентивних наступальних операцій у кіберпросторі шляхом виведення з ладу критично важливих об'єктів інфраструктури противника через руйнування інформаційних систем.

В контексті проблематики нашого дослідження доцільно звернути увагу на констатацію у документі посилення тенденції із «використання кібератак як інструменту спеціальних інформаційних операцій, маніпулювання суспільною думкою», появи нової моделі інформаційного протиборства, основаної на «поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій», застосування кіберзброї терористичними угрупованнями. Слушно йшлося про ескалацію міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі, формування цілих служб кіберрозвідки у все більшого кола держав, продукування сучасних технологій розвідувально-підривної діяльності у кіберпросторі, включаючи інструментарій з накопичення масивів інформації щодо поведінки людини, соціальних груп та використання сучасних досягнень у сфері штучного інтелекту та залучення спецслужбами міжнародних хакерських угруповань для протизаконного кібервпливу. Висувався комплекс заходів щодо поліпшення й централізації управління захистом кіберсфери України.

Поважне місце проблематиці інформаційного протиборства відводилося у концептуальних документах військового відомства та Збройних Сил України [14]. Так, *Закон України «Про оборону України»* [15] визначав «оборону України» як систему політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних заходів держави з підготовки до збройного захисту та її захист у разі збройної агресії або збройного конфлікту. Підготовка держави до оборони мала включати, зокрема, «захист інформаційного простору України та її входження у світовий інформаційний простір, створення розвинутої інфраструктури в інформаційній сфері». Під час відсічі збройній агресії проти України, її Збройні Сили на підставі рішення Президента України Збройні Сили України, повинні разом з іншими військовими формуваннями, розпочати воєнні дії, включаючи проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі.

Закон України «Про Збройні Сили України» [16] серед функцій ЗС визначив і «проведення військових інформаційно-психологічних операцій».

Нова *Стратегія воєнної безпеки України* «Воєнна безпека – всеохоплююча оборона» [17] говорячи про макрозагрози міжнародній та національній безпеці, неодноразово вказує саме на інформаційні фактори «підвищення рівня невизначеності і непередбачуваності безпекового середовища», у тому числі – посилення міждержавної конкуренції із застосуванням «…інформаційних, воєнних і гібридних інструментів», конкуренцією держав у сфері, в т.ч., інформаційних, кібернетичних та інших технологій.

Визначаючи завдання реалізації державної політики у воєнній сфері, сфері оборони і військового будівництва, Стратегія передбачала і низку позицій, прямо пов'язаних із діяльністю в інформаційно-комунікаційній сфері, як от: «розвиток спроможностей сил оборони України щодо стратегічних комунікацій у сфері оборони», впровадження сучасних інформаційних технологій, досягнення належного рівня захищеності інформаційної сфери, «розвиток спроможностей щодо забезпечення кібербезпеки, кіберзахисту та кібероборони». Ведучи мову про *нарощування спроможностей Збройних Сил України, документ підкреслює значення* оновлення змісту доктринальний х та інших розпорядчих документів щодо підготовки та застосування сил оборони для ведення превентивних, непередбачуваних, асиметричних та інноваційних дій для нівелювання чисельної і технологічної переваги противника» з використанням єдиного інформаційного простору.

В процесі творення перспективної моделі організації оборони України, розробки стратегії досягнення спільних оборонних спроможностей, документ знов таки висунув завдання проведення спеціальних операцій, забезпечення спроможностей Збройних Сил України та інших складових сил оборони щодо, у т.ч., ведення асиметричних, мережецентричних, багатосферних і непрямих дій з метою нейтралізації чисельної та технологічної переваги противника «на суші, в повітрі, на морі, в інформаційному просторі та кіберпросторі».

У мірі розвитку сучасних нормативно-правових, доктринальних засад та появи нових структур сектору безпеки і оборони держави, розширюється коло сфер оборонно-безпекової діяльності та їх відповідних структур, до компетенції яких включається і завдання інформаційного протиборства. У цьому відношенні, показовим є приклад унормування й розвитку Сил територіальної оборони (ТрО) Збройних Сил України. *Закон України «Про основи національного спротиву»* [18] включив до функцій руху опору участь у проведенні спеціальних (розвідувальних, інформаційно-психологічних тощо) операцій, а до завдань ТрО – «участь в інформаційних заходах, спрямованих на підвищення рівня обороноздатності держави та на протидію інформаційним операціям агресора (противника)».

Особливе значення для унормування та визначення змісту діяльності сил і засобів інформаційного протиборства у військовій сфері мала «*Концепція стратегічних комунікацій Міністерства оборони України та Збройних Сил України*», затверджена наказом Міністра оборони України від 22 листопада 2017 р. № 612 [19]. Документ визначав стратегічні комунікації (СТК) як «скоординоване і належне використання комунікативних можливостей держави: публічної дипломатії, зв'язків із громадськістю, військових зв'язків інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави», а їх основними складовими стратегічних комунікацій МО та ЗС України – зв'язки з громадськістю, зв'язки з громадськістю у воєнній сфері, публічну дипломатію, інформаційні та психологічні операції.

У документі містилося визначення *інформаційних операцій* як «узгоджених 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». Відповідно, під *психологічними операціями* розумілася «сукупність узгоджених і взаємопов'язаних за метою, завданнями, місцем і часом психологічних акцій (дій) та інших дій суб'єктів психологічних операцій, які проводяться за єдиним замислом і планом для здійснення впливу на емоційний стан, мотивацію, раціональне мислення визначених цільових аудиторій та зміни моделей їх поведінки у спосіб, що сприятиме досягненню політичних і військових цілей України».

Передбачалося, що оперативне планування та управління інформаційними операціями здійснюють Головне оперативне управління Генерального штабу Збройних Сил України та Об'єднаний оперативний штаб Збройних Сил України. Психологічні операції відносили до компетенції Командування Сил спеціальних операцій Збройних Сил України. Розвідувальне забезпечення про-

ведення інформаційних заходів покладалося на Головне управління розвідки МО України. Метою розвідувального супроводження інформбезпеки визначалося «глибоке та повне розуміння» можливостей (намірів, дій) ключових суб'єктів середовища інформаційного протиборства, забезпечення органів військового управління та командирів необхідною інформацією для участі у проведенні МО та ЗС відповідних контрпропагандистських заходів та інформаційно-психологічних операцій.

Серед шляхів реалізації СТК (в частині інформбезпеки) йшлося про систематизацію виявлення та реагування на виклики та загрози в інформаційному просторі із залученням підрозділів, на які покладено проведення інформаційних, психологічних операцій та дій в кіберпросторі, протидію інформаційним операціям проти України, маніпуляціям масовою свідомістю і поширенню сфабрикованої інформації. По суті, йшлося про запровадження всеохоплюючої участі всіх військово-управлінських рівнів ЗС України у СТК, адже передбачалася участь за єдиним замислом в організації дій в інформаційному просторі в мирний час та при проведення операцій (бойових дій) органів військового управління, командних кадрів та штабів всіх рівнів.

Завдання національної спецслужби в царині інформаційного протиборства передбачалися «*Стратегією забезпечення державної безпеки*», затвердженою Президентом України 16 лютого 2022 р. [20]. Документ містив визначення інформаційної безпеки як складової національної безпеки України, розуміючи під нею стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, за якого унеможливлено завдання шкоди державним інтересам, у тому числі, через «проведення іноземними спецслужбами, окремими організаціями, групами, особами спеціальних інформаційних операцій та деструктивних інформаційних впливів».

В комплексі основних завдань державної політики у сфері забезпечення державної безпеки визначалися протидія спеціальним інформаційним операціям, спрямованим на повалення (зміну) конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної ситуації в державі, підрив обороноздатності, завершення створення і посилення спроможності національної системи кібербезпеки.

Отже, виходячи із законодавчо визначених небезпек державному й суспільному ладу, в Україні з 1991 року розроблено й імплементовано в практику оборонно-безпекового будівництва концептуальні засади та нормативно-правову базу захисту інформаційної безпеки та діяльності вітчизняних сил інформаційного протиборства. Відповідно, створено багаторівневу (міжвідомчу) систему державних органів та структур (передовсім – у складі Збройних Сил та СБ України) із забезпечення інформаційної безпеки та ведення інформаційно-психологічної боротьби як складової захисту державного суверенітету й національної безпеки. Активно розвивається синтетична модель інформаційно-гуманітарного впливу – стратегічні комунікації, куди віднесено й мистецтво проведення спеціальних інформаційно-психологічних операцій. Відповідні організаційно-функціональні та концептуальні елементи СТК впроваджуються у відомствах та органах державного управління (передовсім – МО, МЗС, МВС України, ГШ ЗС України, НГУ тощо).

В Україні продуктивного розвитку набула низка наукових напрямів у царині інформаційного протиборства, сформувалися відповідні спеціалізовані наукові, науково-аналітичні та науково-педагогічні установи (підрозділи), у тому числі – недержавного характеру. Серед тематики науково-практичних досліджень виокремилися і такі напрями як розробка концептуальних та організаційно-правових основ забезпечення інформаційної безпеки та інформаційного протиборства в інтересах розвитку (удосконалення) цього сегменту сектору безпеки і оборони України, студіювання та адаптація до національного законодавства та оборонно-безпекового будівництва властивих країнам – членам НАТО та ЄС правових норм, доктринальних поглядів, форм і методів забезпечення інформаційної безпеки та ведення інформаційно-психологічного протиборства (зокрема – досвіду творення системи стратегічних комунікацій).

Водночас, до кінця не вирішеним в організаційно-правовому відношенні залишається завдання розбудови (як у рамках сектору безпеки и обороні, так і на загальнодержавному рівні) централізованого органу координації забезпечення інформаційної безпеки та виконання завдань з інформаційно-психологічного протиборства.

ЛІТЕРАТУРА

1. Війни інформаційної епохи: міждисциплінарний дискурс: монографія/за ред. В.А. Кротюка. Харків: ФОП Федорко М.Ю., 2021. 558 с.
2. Левченко О.В., Міхєєв Ю.І. Інформаційні загрози як різновид воєнних загроз державі. Наука і техніка Повітряних Сил Збройних Сил України. 2018. № 3. С. 14–19.
3. Пунда Ю.В., Мінєєв П.А., Шепіцен О.І. Деякі особливості підготовки держави до відсічі збройній агресії з урахуванням змін у характері збройних конфліктів. Наука і оборона. 2020 № 3. С. 3–7.
4. Вєдєнєєв Д. «Вишукана» гібридна зброя: ураження свідомості керманичів та інтелігенції. Виклики і ризики. Безпековий огляд Центру дослідження армії, конверсії та роззброєння. 2020. № 9. С. 20–32; № 10. С.14–26.
5. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення : монографія. Львів : Сполом, 2020. С. 265–266.
6. Законодавчі основи забезпечення інформаційної безпеки України: наукова доповідь / Пилипчук В.Г., Корж І.Ф., Петришин О.В. та інші. К: НДІІП НАПрН України, 2014. 60 с.
7. Гаврильців М.Т. Інформаційна безпека держави у системі національної безпеки України. *Юридичний науковий електронний журнал*. 2020. № 2. С. 200–203.
8. Дзюба М. Т. Обґрунтування концептуальних положень інформаційної безпеки України. Наука і оборона. 2021. № 3.С. 41–46.
9. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України». Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037.
10. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості». Указ Президента України від 27 вересня 2021 року № 479/2021. URL: https://www.president.gov.ua/documents/4792021-40181.
11. Пирожков С.І., Божок Є.В., Хамітов Н.В. Національна стійкість (резильєнтність) країни: стратегія і тактики випередження гібридних загроз. *Вісник* НАН України. 2021. № 8. С. 74–82.
12. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Указ Президента України від 25 лютого 2017 р. №47/2017. URL: https://www.president.gov.ua/documents/472017-21374.
13. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013
14. Фурашев В.М. Інформаційна складова оборони України: роль та місце. Розвиток законодавства України у сфері оборони: проблеми адаптації до стандартів НАТО та шляхи їх вирішення: матеріали науково-практичної конференції, 23 квітня 2021 р., м. Київ, 2021. С. 86–90.

15. «Про оборону України». Закон України. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text
16. «Про Збройні Сили України». Закон України. URL: https://zakon.rada.gov.ua/laws/show/1934-12#Text
17. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України». Указ Президента України від 25 березня 2021 року № 121/2021. URL: https://www.president.gov.ua/documents/1212021-37661
18. Про основи національного спротиву. Закон України. URL:https://ips.ligazakon.net/document/view/T211702?an=1
19. Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України. Наказ Міністра оборони України від 22 листопада 2017 р. № 612. URL: https://zakon.rada.gov.ua/rada/show/v0612322-17#Text
20. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки». Указ Президента України від 16 лютого 2022 року № 56/2022.