Ілона Клименко,
кандидатка фізико-математичних наук, доцентка, доцентка кафедри публічної політики Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка, Україна

РОЗДІЛ 4.3. ВИКЛИКИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ В УМОВАХ ПОВНОМАСШТАБНОГО РОСІЙСЬКОГО ВТОРГНЕННЯ

Анотація. *З початком повномасштабного вторгнення Російської Федерації на територію України, поряд зі стагнацією летальної зброї та кіберзброї – кібератаки на національні інформаційні ресурси, інформаційні системи та сайти органів державної влади, кіберзлочини, негативні поширився інформаційний вплив на всі сфери функціонування нашої держави і суспільства, завдавши їм значних втрат. Метою роботи є теоретичне обґрунтування та розробка практичних рекомендацій щодо забезпечення інформаційної безпеки України в умовах повномасштабної війни з Росією. Важливими завданнями є консолідація суспільства, створення єдиної стратегії і тактики боротьби з агресором, але сьогодні ми продовжуємо потужне посягання на інформаційну безпеку нашої держави, пов'язане переважно зі спробами інформаційних суб'єктів, у тому числі іноземних, свідомо прикривати змісту заходів за участю України, подавати в неправдивій формі інформацію про розвиток політичних, соціальних, економічних та інших подій, спрямованих на дискредитацію держави в очах міжнародної спільноти та власного народу, підвищення довіри до неї як надійний партнер і значущий суб'єкт міжнародного права. Методологія дослідження базується на загальнонаукових та спеціальних методах наукового пізнання суспільних явищ і процесів, зокрема системному, історичному, логічному, структурно-функціональному та інших методах наукового пізнання державного управління, які спрямовані на отримання об'єктивних і надійні результати. Результати. Пропаганда та дезінформація були викликом протягом десятиліть, але особливо небезпечними під час війни. Дезінформація як від державних, так і від недержавних структур намагається посіяти паніку, спотворити оперативну інформацію з дипломатичного, культурного, економічного, військового фронтів (особливо серед громадян у зоні бойових дій чи на тимчасово окупованих територіях), підірвати довіру до демократичних*

інституцій та представити авторитарні режими як найкращі для забезпечення якості життя громадян.

Таким чином, в умовах війни актуальним є розробка та прийняття Національного плану дій з кібербезпеки та інформаційної безпеки в умовах воєнного стану. Ключовими складовими якого мають стати: поєднання кіберспроможностей держав коаліції для проведення активних превентивних кібероперацій проти агресора; розгортання експертних аналітичних центрів для моделювання та прогнозування загроз, технологій та алгоритмів атак кіберугруповань агресора з метою їх попередження та мінімізації ризиків для держави та суспільства, зміцнення комплексної системи інформаційного забезпечення захист органів державної влади та об'єктів управління від місцевого до загальнодержавного рівнів, поінформованість посадових осіб та громадян про можливі кіберзагрози та заходи щодо їх запобігання, безпечна робота в середовищі інформаційних систем, соціальних мереж, розвиток критичного ставлення до інформації в Інтернет. Пріоритетом також є запровадження комплексної системи підготовки фахівців з інформаційно-психологічних операцій на основі європейських практик та з урахуванням українського досвіду, набутого під час проведення спеціальних операцій. Це допоможе створити відповідний професійний кадровий резерв. Практичні наслідки. Впровадження в державно-управлінську практику забезпечення інформаційної безпеки в умовах повномасштабної війни моделі системного впливу на інформаційну безпеку Української держави, яка включає: нестандартну системну, інституційну поведінку суб'єктів інформаційної безпеки з метою попередження негативних зовнішніх інформаційно-психологічних впливів; адаптація системи захисту інформації до нових викликів і загроз. Цінність/оригінальність. Оптимізація структури та функцій системи інформаційної безпеки України з урахуванням сучасних викликів і загроз національним інтересам України в інформаційній сфері та вимог до систем творчої безпеки має включати: механізми інформаційно-аналітичного забезпечення інформації. психологічна безпека, яка охоплює мережу аналітичних інститутів (державних і недержавних); механізми співпраці держави з інститутами громадянського суспільства, з міжнародними організаціями та структурами регіональної безпеки; заходи дострокового впливу на причини, що створюють загрози національним інтересам в інформаційній сфері; удосконалення механізму інформаційно-аналітичного забезпечення розробки та впровадження паспортів у практику державного управління загрожують інформаційній та психологічній безпеці.

Ilona Klymenko,
Candidate of Physico-Mathematical Sciences (PhD in Physics and Mathematics), Associate Professor, Associate Professor of the Department of Public Policy of the Educational and Scientific, Institute of Public Administration and Civil Service of the Taras Shevchenko National University of Kyiv, Ukraine

CHALLENGES TO UKRAINE'S INFORMATION SECURITY IN THE CONTEXT OF A FULL-SCALE RUSSIAN INVASION

Abstract. *With the beginning of the full-scale invasion of the Russian Federation on the territory of Ukraine, along with the stagnation of lethal weapons and cyber weapons – the cyber attacks on national information resources, information systems and sites of public authorities, cyber crimes, negative information influence on all spheres of functioning of our state and society became more widespread, causing them considerable losses.* **The purpose** *of the paper is to theoretical substantiation and development of practical recommendations on ensuring information security of Ukraine in conditions of full-scale war with russia. The important tasks are consolidation of society, creation of a unified strategy and tactics of struggle with the aggressor, but today we continue strong encroaching on the information security of our state, connected mainly with attempts of informational subjects, including foreign ones, deliberately cover the contents of events with the participation of Ukraine, to submit in false form information about the development of political, social, economic and other events aimed at discrediting the state in the eyes of the international community and its own people, raising the trust in it as a reliable partner and a significant subject of international law.* **Methodology** *of the research is based on the general scientific and special methods of scientific knowledge of social phenomena and processes, in particular system, historical, logical, structural-functional and other methods of scientific knowledge of public administration, which are intended for obtaining objective and reliable results.* **Results.** *Propaganda and misinformation have been a challenge for decades, but especially dangerous during the war. Misinformation from both state and non-state actors is trying to sow panic, to distort operational information from diplomatic, cultural, economic, military fronts (especially among citizens in the zone of fighting or temporarily occupied territories), to undermine trust in democratic institutions and to present authoritarian regimes as best for ensuring the quality of life of citizens.*

Thus, in the conditions of war, it is important to develop and adopt the National Action Plan on Cybersecurity and Information Security in the conditions of military condition. The key components of which should be: The combination of the cyber capabilities of the coalition states to carry out active preventive cyber operations against the aggressor; the deployment of expert think tanks for modeling and forecasting threats, technologies and algorithms of attacks of the cyber-forces of the aggressor with a view to their pre-emptive and mitigation of risks for the state and society, Strengthening of the complex system of information protection of public authorities and objects of management from local to national levels, public officials and citizens' awareness of possible cyber threats and measures to prevent them, safe work in the environment of information systems, social networks, development of critical attitude to information in the Internet. The priority is also the introduction of a comprehensive system of training of specialists in information and psychological operations, based on European practices and taking into account the Ukrainian experience gained during special operations. This will help to create the appropriate professional personnel reserve. **Practical implications.** *Introduction of the system impact model on information security of the Ukrainian state in the state-management practice of providing information security in the conditions of a full-scale war, which includes: Non-standard system, institutional behavior of information security subjects with the purpose of prevention of negative external informational and psychological influences; adaptation of information security system to new challenges and threats.* **Value/originality.** *Optimization of the structure and functions of the information security system of Ukraine taking into account modern challenges and threats to the national interests of Ukraine in the information sphere and requirements to the systems of creative security, should include: Mechanisms of informational and analytical provision of information and psychological security, which covers the network of analytical institutes (state and non-state); mechanisms of cooperation of the state with civil society institutions, with international organizations and regional security structures; measures of the pre-term influence on reasons that create threats to national interests in the information sphere; improvement of the mechanism of information and analytical support by development and implementation of passports in the state-management practice threaten information and psychological security.*

Вступ. З початком повномасштабного вторгнення російської федерації на територію України, разом із застосовуванням летальної зброї посилилася і кіберзброя – ще більш масованими стали кібератаки на національні інформаційні ресурси, інформаційні системи та сайти органів публічної влади, кіберзлочини, негативні інформаційні впливи на всі сфери функціонування нашої держави і суспільства, завдаючи їм відчутних збитків.

Кібератаки стають більш розповсюдженими, організованими та дорожчими через шкоду, яку вони завдають органам публічної влади, державним та приватним підприємствам/організаціям (особливо критичної інфраструктури), економічній стабільності, транспортним мережам і мережам постачання. Джерелом таких атак можуть бути російські військові та розвідувальні служби держави-агресора, колаборанти, організовані злочинці, терористичні та/або екстремістські групи країн, що підтримують російське вторгнення, тощо. У випадках цілеспрямованого викривлення інформації населення втрачають відчуття реальності й починають жити у створеному для них віртуальному світі. Відбувається посилення негативних інформаційних впливів, розповсюдження дезінформаційних матеріалів, що базується на використанні маніпулятивних технологій із застосуванням підходів соціальної інженерії, нейролінгвістики, психології.

Така ситуація здатна спричинити виникнення як локальних, так і глобальних конфліктів, що в результаті призводить аж до виникнення збройних конфліктів і втрати національного інформаційного суверенітету країни. Діяльність всіх органів влади повинна бути спрямована на консолідацію суспільства, створення єдиної стратегії й тактики боротьби з агресором, але сьогодні продовжуються потужні посягання на інформаційну безпеку нашої держави, пов'язані, здебільшого, із намаганнями інформаційних суб'єктів, у тому числі й закордонних, свідомо викривити зміст подій за участю України, подати у сфальшованому вигляді відомості про розвиток політичних, соціальних, економічних та інших подій із метою дискредитації держави в очах міжнародної спільноти та свого власного народу, підриву довіри до неї як до надійного партнера та вагомого суб'єкта міжнародного права.

4.3.1. Характеристика сучасних маніпулятивних технологій російської федерації

Маніпулятивні технології застосовуються для нагнітання у суспільстві психологічного шоку, страху, відчаю (зокрема, спрямовані на громадян та державних службовців, які перебувають на тимчасово окупованих/прифронтових територіях). До таких технологій відносять: ефект первинності (удар на випередження); ефект присутності (трюки, покликані імітувати реальність у «репортажах з місць боїв»); використання коментарів під публікаціями в ЗМІ, соцмережах для створення контексту, у якому наступні думки людини йдуть в необхідному напрямі, дозують позитивні та негативні елементи. Однією з технологій інформаційної обробки населення є організація виступів свідків подій на підготовленому підґрунті та тиражування в ЗМІ потрібної версії; побудова «фальшивих асоціацій» між певною трагедією та іншими інцидентами за участі військових; «підтасовування фактів», поширення чуток та опитування «очевидців подій», які свідчать про зумисний характер злочинів [1, с. 226].

Загрози психічному здоров'ю населення можуть бути ідентифіковані, як: несанкціоноване використання сучасних інформаційних та психологічних технологій для направленого коригування системи цінностей громадян, їх психофізіологічного стану, інтелектуальних даних, мотиваційної поведінки; агітація та пропаганда, що порушують загальноприйняті норми, провокують ненависть та ворожість; обмеження доступу громадян до достовірних відкритих інформаційних ресурсів органів публічної влади; викривлення соціальнозначущої інформації; відсутність дієвих механізмів попередження використання соціальних мереж для пропаганди насилля, жорстокості, приниження людської гідності тощо.

Напередодні та під час вторгнення в Україну російські ЗМІ, телеведучі, експерти нав'язували Україні і світу 13 основних наративів, виправдовуючи свою агресію [2]:

Майдан 2014 року спровокував громадянську війну та від'єднання Донецька і Луганська від України.

Нацисти та ультранаціоналісти в Україні (нацисти/праві націоналістичні уряди прийшли до влади після державного перевороту у Києві; ЄС підтримує неофашистські сили в Україні; Захід ігнорує проблему нацизму в Україні; Донбас відокремився,

бо націоналісти прийшли до влади у Києві; нацисти організували «одеську різанину»; неофашистські/неонацистські сили брали участь у державному перевороті 2014 року; в Україні поширена нацистська ідеологія; праворадикали та неонацисти залучені до уряду та правоохоронної системи України).

Північний потік-2 (затримка реалізації «Північного потоку-2» веде до кризи в ЄС; США як колоніаліст намагається перешкодити запуску «Північного потоку-2» для збереження власного впливу на Європу; «Північний потік-2» – це не політичний, а виключно комерційний проект; Україна краде транзитний російський газ; український газопровід зношений).

Росія повинна себе захищати (НАТО нарощує свою присутність в Україні, що створює небезпеку для росії; НАТО постійно здійснює антиросійські провокації та наближається до російських кордонів; НАТО пообіцяло росії не розширюватися на схід; росія має захищати мешканців «ЛНР/ДНР»; росія просто проводила військові навчання біля кордонів України; Захід провокує війну з росією; Українська влада готує провокації проти росії).

Україна є неліберальною державою, оскільки є жорстка цензура, порушуються права людини, нехтуються права етнічних меншин.

Провал України як держави (економіка та політичні інститути України майже не функціонують; історично Україна є частиною росії).

Контроль і використання України Заходом у власних інтересах (Захід контролює владу в Україні; державний переворот в Україні у 2014 році підтримав/організував Захід; організатором «перевороту» та творцем «української кризи» є Нуланд; Захід хоче знищити українську економіку, щоб позбутися конкурентів та уникнути конкуренції; Україна стала неофіційною військовою базою НАТО; Україна – маріонетка в руках Заходу у глобальній змові; Захід розпалює війну в Україні, використовуючи її у своїх діях проти росії; Захід використовує Україну у своїх діях проти росії; Захід використовує Україну як інструмент проти росії; секретні лабораторії США розміщені по всій Україні; Україна повністю залежить від Заходу).

Захід не зацікавлений в проблемах України, а тим більше – в їх вирішенні (США не вважають Україну важливою; для Заходу Україна є лише буферною зоною; Захід втомився від України; Заходу байдужа Україна).

Росіян дискримінують в Україні (В Україні утискують російську мову).

Проєвропейський вибір України означає антиросійський вибір.

В Україні процвітає антиросійський неонацизм.

Росія не є агресором щодо України (росія не має відношення до війни в Україні; росія не окупувала Крим, це було «возз'єднання»; конфлікт на Сході України є виключно внутрішнім, це громадянська війна).

Україна проводить агресивну політику (Україна загострює конфлікт на Донбасі; Україна проводить чи готує провокації на Донбасі; Україна має намір вирішити конфлікт на Донбасі силовим шляхом; Україна нарощує військову присутність на Донбасі; Українська армія відкриває вогонь по мирних жителів; Україна не дозволяє спостерігачам ОБСЄ фіксувати порушення ЗСУ; Українська армія порушує режим припинення вогню; Україна денонсувала Мінські угоди; Київ ігнорує виконання Мінських угод).

Специфіка дій росії в війні проти України, яка, поєднуючи мілітарні, квазімілітарні, дипломатичні, інформаційні, терористичні, економічні засоби, не гребуючи ядерним шантажем, яскраво демонструє намагання досягти в Україні та в інших країнах світу власних, не завжди зрозумілих міжнародній спільноті політичних цілей.

Гібридний інформаційно-медійний характер російської агресії ще станом на 2014 рік повною мірою виявив неприпустимо слабкі позиції України в забезпеченні власної інформаційної безпеки, зокрема [3]:

– критична кількість медіа, які перебуваючи в інформаційному просторі України, порушують її закони та загрожують її національній безпеці;

– недостатньо захищений від неліцензованих трансляцій вітчизняний телерадіопростір, стабільне технічне покриття якого й досі є значно меншим за територію держави (навіть без урахування окупованих районів);

– неадекватна вимогам часу система нормативно-правового та інституційного забезпечення розвитку інформаційної сфери, зокрема, відсутність концептуальної державної політики інформаційної безпеки;

– недостатньо фахова, слабко організована й надто залежна від власників ЗМІ журналістська спільнота;

– брак дієвих інституцій та механізмів оперативного реагування на інформаційні загрози як технічного, так і психологічного характеру.

Така ситуація призвела до створення умов для масової та безперешкодної трансляції аудіовізуального продукту, зміст якого прямо порушував законодавство України у сфері інформаційної безпеки. Складові інформаційної війни рф проти України, що проводяться шляхом застосування маніпулятивних технологій, формують інформаційне поле та визначають вектор сприйняття населенням країни тих чи інших подій.

Кожний регіон нашої держави перебуває під різним інформаційним впливом, так на Донбасі кількість телеглядачів політичних новин телеканалів «Інтер», «Україна» становить 60 %, російських новин – 78 % глядацької аудиторії. Саме серед глядачів цих телеканалів опинилося більше тих, хто хотів би об'єднатися з Росією, та вважають, що «Україна нездатна подолати існуючі проблеми та труднощі», що свідчить про песимістичні настрої регіону.

Київський міжнародний інститут соціології запропонував вимірювання індексу результативності російської пропаганди (індекс РРП) для оцінки контр-пропагандистської роботи України в тих чи інших регіонах і серед тих чи інших соціальних груп [4]. Під результативністю російської пропаганди на території України розуміється поширеність підтримки головних тез російської пропаганди населенням України в цілому або тієї чи іншої території України. Ідея дослідників полягає в тому, щоб вибрати такі тези офіційної російської пропаганди, в які вірить більше 80% російського населення, тобто тих тез, які показали свою ефективність в Росії і на окупованій території. На думку вчених [4], ядром пропаганди є квазілогічний ланцюжок:

майдан був організований *американцями разом з націоналістами → в результаті майдану до влади прийшли націоналісти, які загрожують російськомовному населенню України → Крим і Схід України були в небезпеці → Крим вдалося захистити, включивши його до складу Росії, а Схід повстав і хоче незалежності і гарантій безпеки → націоналісти, що незаконно прийшли до влади, почали війну зі своїм народом.*

Індекс РРП може бути застосований для оцінки динаміки процесів і для порівняння шкоди, завданої російською пропагандою, різним територіальним та соціально-демографічним групам, зо-

крема ці дані можна використовувати в ситуативних центрах для формування інформаційного контенту для контрвпливу на ризикові групи населення. Середнє значення індексу РРП для населення України в цілому дорівнює 26, значення індексу практично не залежить від віку, статі та рівня освіти респондентів. Дослідження показали суттєві відмінності в нараженості російській пропаганді пов'язані з регіоном проживання респондентів. Найбільш низький рівень нараженості російській пропаганді в Західному регіоні (індекс РРП = 12) та в Центральному регіоні (РРП = 19), набагато вище значення індексу в Південному регіоні (РРП = 32). У Східному регіоні значення індексу в 4 рази вище, ніж у Західному (РРП = 48). Видно, що Східний і Південний регіони являють собою велику проблему та вимагають серйозних зусиль у боротьбі проти російської пропаганди.

Соціологічне дослідження-моніторинг проросійських наративів, джерел їхнього поширення, сприйняття населенням та протидії їм, проведене Київським міжнародним інститутом соціології після повномасштабного вторгнення росії в Україну [5], показало, що не менше 85% респондентів вважають, що в Україні немає утисків російськомовного населення (зокрема, так вважають 85% етнічних росіян і 90% російськомовних жителів України), що Україна має власну довгу історію становлення та державності (а не є «штучним» витвором радянської влади), що західні держави не хотіли і не провокували Україну на війну проти росії, що думки про «нацистів» у владі України є вигадкою, що війна почалася через прагнення росії підкорити Україну (а не через справедливі претензії), що російські війська навмисно атакують цивільну інфраструктуру та цивільних осіб, що російська армія в першу чергу винна у руйнації цивільної інфраструктури і жертвах серед мирного населення. Населення всієї України, зокрема південних і східних регіонів є проукраїнські налаштованими. Крім цього, хоча серед респондентів окупованих територій більш помітні проросійські наративи, але навіть серед них абсолютна більшість має проукраїнську позицію.

Такі показники дуже оптимістичні для України, тим більше, що до лютого 2022 року в Україні було значне засилля проросійських наративів.

Інформаційна складова гібридної війни Росії проти України призвела до необхідності вжиття негайних заходів щодо захисту національного інформаційного простору, та які на сьогодні забезпечили проукраїнську позицію населення:

– запровадження адміністративних обмежень транслювання на українській території програм російських пропагандистських теле- і радіоканалів та поширення іншої мас-медійної продукції (у тому числі книги російського виробництва), яка дестабілізує суспільну ситуацію в Україні і формує загрози національній безпеці;

– заборона в'їзду артистів, що публічно підтримують анексію Криму та воєнну агресію Кремля;

– відновлення українського мовлення на тимчасово окупованих територіях;

– створення незалежного суспільного мовлення, розвиток власного кіновиробництва.

Основними маніпулятивними технологіями, які використовує РФ у гібридній війни проти України, є: нагнітання психологічного шоку, ефект первинності (удар на випередження), ефект присутності (дії, які покликані імітувати реальність у «репортажах з місць боїв») тощо.

Однією з технологій «інформаційної обробки» населення Донбасу став прийом, який застосовує канал «россия» – організація виступів свідків подій на підготовленому підґрунті та тиражування центральним телебаченням потрібної версії.

Крім того, серед прийомів, які застосовуються є такі:

– вибудування «фальшивих асоціацій» між певною трагедією та іншими інцидентами за участі військових;

– «підтасовування фактів» та опитування «очевидців подій», які свідчать про навмисний характер злочинів. За допомогою підтасування фактів, поширення чуток створюється штучна атмосфера, а будь- яка серйозна подія на території обробляється в рамках справжньої «інформаційної блокади» та дозування інформації.

Також використовуються образи надмірного застосування сили; пересування військової техніки як ескалації конфлікту; наслідків військових злочинів та «таємної змови».

Заслуговує на увагу під час російської агресії такий метод інформаційного впливу, як інформаційне вкидання. Під «інформаційним вкиданням» розуміють поширення по завчасно підготовлених каналах спеціального масиву інформації з метою формування в цільової аудиторії певні меседжі.

Разом з тим, інформаційне вкидання не слід ототожнювати з дезінформацією, оскільки, вкидання може нести як достовірну, так і недостовірну інформацію.

Відмінними рисами вкидання від інших методів можуть бути:

а) забезпечення прихованості в процесі досягнення цільової спрямованості із застосуванням певних заходів інформаційного впливу. При цьому інформаційне вкидання маскується під звичайні медійні сюжети;

б) залучення джерел інформації країни-противника в процес поширення інформації. Слід зауважити, що цей ефект ретельно вивчається ще на етапі планування інформаційного вкидання, оскільки він створює «другу хвилю», спрацьовує принцип «доміно». На практиці, майже завжди інформація з російських джерел підхоплювалася українськими або іноземними медіа.

Основними каналами поширення інформаційно-пропагандистських заходів РФ проти України є: російські ЗМІ (радіо, телебачення, друковані та онлайн-видання тощо); підконтрольні ЗМІ на ТОТ Донбасу; зарубіжні російські ЗМІ (зокрема «Sputnik», «RT»); соціальні мережі.

Найпоширенішим об'єктом і одночасно засобом ведення інформаційних заходів у мережі Інтернет є соціальні мережі та сумнівні інтернет-сайти. Вони стали одним з важливих інструментів інформаційно-психологічного впливу, в тому числі впливу з метою маніпулювання особистістю, соціальними групами і суспільством в цілому.

Потужним каналом проросійської пропаганди і сьогодні є Українська православна церква (Московського патріархату), зокрема ті галузі, що підпорядковуються Москві. Керівництво рф її використовує для мобілізації потенційних прибічників його ідеології. Неодноразово траплялися випадки, коли представники цієї церкви різних рівнів виступали з антизахідними меседжами або виправдовували агресивну політику рф.

Також агентами впливу були і є бізнесово-політичні групи, дружні до кремля. Саме вони контролюють діяльність політичних партій та володіють потужним медіа ресурсом в Україні.

Отже, в умовах проведення росії деструктивного інформаційного впливу на цільову аудиторію України та інших держав світу можна визначити такі основні напрями вжиття заходів щодо захисту національного інформаційного простору [6]:

– розроблення нормативно-правової бази стосовно засад державної політики у сфері інформаційної безпеки, яка б визначала взаємодію силових структур України з місцевими органами самоврядування, державними (недержавними) установами, громадсько-політичними організаціями, ЗМІ тощо;

– створення єдиного міжвідомчого органу, який здійснюватиме керівництво, координацію та контроль заходів інформаційної безпеки, зокрема інформаційного протиборства (наприклад, міжвідомча комісія при РНБОУ);

– завершення формування національної системи забезпечення інформаційної безпеки, адекватної масштабам і спрямованості загроз. На державному рівні це означає посилення внутрішніх спроможностей щодо протидії інформаційним загрозам, на міжнародному – формування кооперативного співробітництва;

– створення системи комплексного моніторингу матеріалів популярних аудіовізуальних та друкованих ЗМІ, а також популярних Інтернет-ресурсів;

– створення нової комунікаційної стратегії, здатної швидко й ефективно реагувати на сучасні виклики та загрози, а також визначити та оцінити їх характер і значущість;

– формування державної програми, спрямованої на підвищення в суспільстві рівня медіа грамотності (розуміння небезпеки від негативного інформаційного впливу);

– узаконення діяльності, використання за єдиним замислом ресурсу працівників недержавних установ, звичайних громадян України для виконання завдань захисту інформаційного простору та протидії інформаційним і кібернетичним заходам;

– продовження створення системи національного інформування для формування об'єктивної думки про події в Україні, зокрема за кордоном. У цьому зв'язку необхідно в найкоротший термін відновити мовлення каналу «Ukraine Today»;

– забезпечення специфічними засобами, які б сприяли на сучасному рівні розвитку інформаційних технологій вирішенню завдання захисту об' єктів інформаційної інфраструктури держави та вжиттю превентивних заходів;

– удосконалення системи наукових досліджень у сфері інформаційної безпеки.

Отже, основними стратегічними напрямами негативного інформаційного впливу російських та проросійських ЗМІ і надалі залишаються: дестабілізація суспільно-політичного життя в Україні, дискредитація воєнно-політичного керівництва, Збройних Сил України та престижу військової служби, а також перешкоджання євроінтеграційним, демократичним прагненням України.

4.3.2. Система державного управління забезпеченням інформаційної безпеки України

Гібридна війна, ключовим елементом якої є інформаційний чинник, формує довгострокові виклики для Української держави. У «Стратегії сталого розвитку «Україна – 2020» було заявлено про необхідність реформи системи національної безпеки і оборони, одним з ключових пріоритетів якої має стати інформаційна безпека [7].

Дії противника спрямовані на ініціювання розбрату в українському суспільстві та знищення української громадянської нації, прославляння сепаратизму, штучне посилення реальних і вигаданих внутрішніх протиріч, створення атмосфери громадянської недовіри до дій і намірів влади, провокування актів громадянської непокори, формування у громадян України та міжнародної спільноти викривленого бачення подій в Українській державі, спроби перекручення української історії та маніпулювання історичними фактами [8].

За таких умов, що склалися перед Українською державою постає питання негайного реформування системи національної безпеки і оборони з урахуванням нових викликів та загроз національним інтересам, що пов'язанні із інформаційно-психологічним чинником. Це передбачає перш за все здійснення оцінки відповідності інституційної системи державного управління інформаційною безпекою України завданням адекватного реагування на сучасні виклики та загрози інформаційній безпеці.

Попередньо зауважимо, що інституційна система державного управління інформаційною безпекою представляє собою складну багаторівневу систему, яка, з одного боку, об'єднується особливою загальною функціональною спрямованістю, а з іншого, розділяється специфічними особливостями, пов'язаними з рівнем компетенції і характером відповідних цілей. Суб'єктам забезпечення інформаційної безпеки відповідає окрема специфічна функція – функція розробки або функція реалізації політики інформаційної безпеки. Функція розробки державної політики інформаційної безпеки включає в себе діяльність компетентних органів держави щодо встановлення стратегічних цілей, завдань, основних принципів та напрямів державної діяльності в цій сфері, розробку концепцій та рішень загальнодержавного довгострокового значення. Функція реалізації політики інформаційної безпеки спрямована на досягнення тактичних та оперативних цілей,

забезпечує вирішення конкретних завдань, застосування відповідних засобів, форм та методів державного впливу на суспільні відносини в цій сфері [9, с. 157].

Зрозуміло, що в залежності від характеру завдань, їх виконання входить до компетенції державних органів різного рівня, які відносяться до різних гілок влади, мають різні сфери діяльності та обсяг владних повноважень. Але враховуючи той факт, що політика інформаційної безпеки як суспільне явище носить комплексний характер, включає внутрішньо та зовнішньо політичні, економічні, технологічні, військові та ряд інших елементів і звідси вимагає комплексного підходу, ми повинні розглядати діяльність державних органів, спрямовану на виконання конкретних завдань в цій сфері, в рамках єдиного інституціонального механізму, який об'єднується єдиною метою забезпечення належних умов забезпечення інформаційної безпеки України [9, с. 158].

Так згідно ст. 4 Закону України «Про основи національної безпеки» [10] до складу цієї частини механізму забезпечення інформаційної безпеки входять наступні органи: Президент України; Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; міністерства та інші центральні органи виконавчої влади; Збройні Сили України, Служба безпеки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України.

Розглянемо повноваження деяких державних інституцій у сфері забезпечення інформаційної безпеки України.

Відповідно до Конституції України [11] Верховна Рада України, як єдиний орган законодавчої влади в Україні, здійснює законодавче регулювання і контроль за діяльністю органів державної влади та посадових осіб щодо виконання ними функцій і завдань в інформаційній сфері; ухвалює засади внутрішньої і зовнішньої політики держави в інформаційній сфері; затверджує державний бюджет, в якому передбачаються кошти на забезпечення інформаційної безпеки України.

Тобто до функцій Верховної Ради входить визначення змісту інформаційної безпеки та можливі форми і способи її захисту.

Верховною радою виконуються важливі контрольні функції в сфері інформаційної безпеки. Одним з важливих інструментів парламентського контролю є призначення слідчих комісій Верховної Ради для розслідування тих або інших подій в інформаційній сфері,

проведення парламентських слухань, зокрема з приводу інформаційної безпеки України та ситуації в інформаційній сфері взагалі.

Організаційна структура Верховної Ради передбачає у її складі підрозділи, які повинні більш детально працювати над проблемами інформаційної безпеки. Так при Верховній Раді України створено Консультативну раду з питань інформатизації для сприяння у виробленні політики в сфері інформатизації, при підготовці та затвердженні завдань Національної програми інформатизації з урахуванням найновіших досягнень і технологічних рішень [12].

Також до складу Верховної Ради входять профільні парламентські комітети: Комітет з питань культури і духовності; Комітет з питань національної безпеки і оборони; Комітет з питань свободи слова та інформації, які виконують завдання щодо підготовки законопроектів з питань розвитку інформаційної безпеки [13].

Інтегруючим елементом системи державних органів управління інформаційною безпеки є Президент України. В межах своїх повноважень він здійснює керівництво інформаційною безпекою України: створює, реорганізує та ліквідує органи виконавчої влади, визначає їх функції та основні завдання; видає укази і розпорядження, що стосуються функціонування та розвитку державного управління в сфері інформаційної безпеки тощо.

Президент має цілий ряд інших засобів впливу в інформаційній сфері. Згідно ч. 3. ст. 106 Конституції Президент видає укази і розпорядження, які є обов'язковими до виконання на території України. Це право Президента широко ним використовується для регулювання питань, пов'язаних з функціонуванням інформаційної сфери [14].

В руках Президента зосереджені ключові функції щодо організаційного забезпечення інформаційної безпеки. Так, Президент очолює Раду національної безпеки і оборони, утворює, реорганізує та ліквідовує за поданням Кабінету Міністрів міністерства та інші центральні органи виконавчої влади, що здійснюють державне управління інформаційною безпекою.

Відповідно до ст. 2 Закон України «Про основи національної безпеки» [14] Президентом розробляються і затверджуються Стратегія національної безпеки України і Воєнна доктрина України, доктрини, концепції, стратегії і програми, якими визначаються цільові настанови та керівні принципи воєнного будівництва, а також напрями діяльності органів державної влади в конкретній обста-

новці з метою своєчасного виявлення, відвернення і нейтралізації реальних і потенційних загроз національним інтересам України.

Президентом для забезпечення здійснення його конституційних повноважень створюється Адміністрація Президента України, що є постійно діючим органом [15].

В структурі Адміністрації Президента України існує цілий ряд профільних підрозділів з питань інформаційної політики та інформаційної безпеки [16]. Серед них можна виокремити Головний департамент з питань національної безпеки та оборони, Головний департамент інформаційної політики та Головний департамент з питань гуманітарної політики, які забезпечують окремі напрямки діяльності Президента України в сфері інформаційної безпеки.

В безпосередньому підпорядкуванні Адміністрації Президента України знаходиться Національний інститут стратегічних досліджень, який є базовою науково-дослідною установою аналітико-прогнозного супроводження діяльності Президента України. Згідно п. 9 Статуту цього Інституту його основним завданням є здійснення науково-аналітичні та прогнозні дослідження з питань суспільно-політичної, соціально-економічної, зовнішньополітичної, воєнно-політичної, етнополітичної, гуманітарної, інформаційної та екологічної стратегії розвитку України та її регіонів, а також з проблем національної безпеки держави [17].

Координаційні функції з питань інформаційної безпеки виконуються згідно ст. 107 Конституції України Радою національної безпеки і оборони України (РНБОУ), яка визначена як «координаційний орган з питань національної безпеки і оборони при Президентові України» [11]. Її головним завданням є координація і контроль діяльності органів виконавчої влади у відповідній сфері.

Згідно норм ст. 3 Закону «Про Раду національної безпеки і оборони України» [18] функціями цього органу є: внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки і оборони; координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони у мирний час; координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України.

Також відповідно до своєї компетенції РНБОУ розглядає на своїх засіданнях питання, які належать до сфери національної безпеки та оборони та подає пропозиції Президентові України щодо: визначення стратегічних національних інтересів України, концептуальних підходів та напрямів забезпечення національної безпеки і оборони у політичній, економічній, соціальній, воєнній, науково-технологічній, екологічній, інформаційній та інших сферах; удосконалення системи забезпечення національної безпеки та організації оборони, утворення, реорганізації та ліквідації органів виконавчої влади у цій сфері та ін.

Разом з тим зазначимо наступне, що система інституцій, які допомагають Президенту здійснювати конституційні повноважень була сформована ще в ті часи коли в країні актуальними були проблеми, які зовсім не відповідають сьогоденню. Саме в зв'язку з тим, що сьогодні на перший план виходять абсолютно нові виклики та загрози для національної безпеки України, було створено Комітет з питань розвідки при Президентові України.

Основним завданням Комітету є підготовка Президентові України пропозицій щодо здійснення керівництва, координації і контролю за діяльністю розвідувальних органів України [19].

Функції Президента у сфері інформаційної безпеки доповнюються відповідними функціями Кабінету Міністрів України. Його завдання щодо застосування засобів впливу на суспільні відносини в інформаційній сфері підкріплюються широкими конституційними повноваженнями. Зокрема, можна назвати визначені нормами ст. 116 Конституції України: забезпечення проведення державної інформаційної політики, здійснення заходів щодо забезпечення обороноздатності і національної безпеки України, вжиття заходів щодо захисту інформаційних прав і свобод громадян, розробку і здійснення загальнодержавних програм щодо розвитку інформаційної сфери, передбачення при формуванні державного бюджету коштів на різного роду заходи щодо забезпечення інформаційної безпеки, загальна координація діяльності органів виконавчої влади щодо захисту інформаційної безпеки тощо [11].

Забезпечення діяльності Кабінету Міністрів здійснюється в межах покладених на них функцій структурними підрозділами Секретаріату Кабінету Міністрів [20]. В Секретаріаті Кабміну діє цілий ряд підрозділів, які покликані виконувати функції Кабінету Міністрів в інформаційній сфері. Так, безпосередньо питання

інформаційної політики входять до компетенції Управління розвитку інформаційного суспільства та інформаційної безпеки та Департаменту інформації та комунікацій з громадськістю.

Необхідно відмітити, що Кабінетом Міністрів, було внесено відповідні зміни до Регламенту Кабінету Міністрів України, поновив інститут «Урядових комітетів» [21]. Урядовий комітет є робочим колегіальним органом Кабінету Міністрів, який утворюється для забезпечення ефективної реалізації повноважень Кабінету Міністрів, координації дій органів виконавчої влади, попереднього розгляду проектів нормативно-правових актів, основних напрямів реалізації державної політики, інших документів, що подаються на розгляд Кабінету Міністрів [22].

Так, постановою від 19 березня 2014 року було утворено чотири урядових комітети [23], зокрема Урядовий комітет з питань оборони, оборонно-промислового комплексу та правоохоронної діяльності на який покладено завдання розгляду проектів нормативно-правових актів з питань інформаційної безпеки та національної безпеки в цілому.

Таким чином, ми окреслили функції і повноваження законодавчої влади і вищих органів виконавчої влади України щодо забезпечення інформаційної безпеки. Але залишається ціла низка міністерств та відомств, які також відіграють важливу роль у реалізації державного управління в сфері інформаційної безпеки. Тому обов'язково необхідно виділити ряд суб'єктів, які здійснюють цілеспрямований державно-управлінський вплив на сферу інформаційних відносин.

Також в Україні створено Міністерство культури та інформаційної політики України, яке є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сферах культури, державної мовної політики, популяризації України у світі, державного іномовлення, інформаційного суверенітету України та інформаційної безпеки [24]. При Міністерстві в 2021 році був створений Центр стратегічних комунікацій та інформаційної безпеки, діяльність якого сфокусована на протидії зовнішнім загрозам, об'єднанні зусиль держави та громадських організацій у боротьбі з дезінформацією, оперативному реагуванні на фейки, а також на промоцію українських наративів. Ключовими завданнями Центру стратегічних комунікацій та інформаційної безпеки є [25]:

– розбудова стратегічних комунікацій (розробка контрнаративів РФ, проведення інформкампаній, включення українських наративів у щоденну комунікацію Уряду);

– протидія дезінформації та формування стійкості до неї. Постійне сповіщення про інформаційні атаки проти України на ресурсах Центру;

– підвищення обізнаності про гібридні загрози (розробка та проведення тренінгів для державних службовців, зокрема для представників комунікаційних підрозділів);

– регулярне інформування про гібридну агресію з боку Росії на міжнародному рівні, напрацювання механізмів протидії дезінформації спільно з міжнародними партнерами.

Ще одним з ключових органів державного управління інформаційною сферою, безперечно, є Державний комітет телебачення і радіомовлення України (далі – Держкомтелерадіо України).

Держкомтелерадіо України є головним у системі центральних органів виконавчої влади з формування та реалізації державної політики у сфері телебачення і радіомовлення, в інформаційній та видавничій сферах [26].

До повноважень Держкомтелерадіо України в сфері інформаційної безпеки віднесено зокрема: розробка заходів щодо запобігання внутрішньому і зовнішньому інформаційному впливу, який загрожує інформаційній безпеці держави, суспільства, особи; участь у формуванні єдиного інформаційного простору, сприяння розвитку інформаційного суспільства; реалізація разом з іншими державними органами завдання щодо забезпечення інформаційної безпеки; підготовка пропозицій щодо вдосконалення системи державного управління у сфері телебачення і радіомовлення, інформаційній та видавничій сферах тощо.

Окремо в системі державного управління інформаційною безпекою слід виділити такий орган як Національна рада з питань телебачення і радіомовлення. Згідно Закону «Про Національну раду з питань телебачення і радіомовлення», Національна рада є конституційним, постійно діючим позавідомчим державним органом, підзвітним Верховній Раді України та Президентові України [27].

Повноваження Ради дозволяють їй фактично контролювати перелік телерадіоорганізацій, які здійснюють трансляції на території України і певною мірою контролювати зміст цих трансляцій.

Тому діяльність ради має виняткове значення для забезпечення інформаційної безпеки держави.

Невід'ємним елементом системи забезпечення інформаційної безпеки є так звані «силові відомства», основним профільним «силовим» відомством з питань інформаційної безпеки, безперечно є Служба Безпеки України (далі – СБУ) та Служба зовнішньої розвідки України (далі – СЗР).

Законом України визначається, що на СБУ покладається у межах визначеної законодавством компетенції захист інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, а також до її завдань входить попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, тероризму, які безпосередньо створюють загрозу життєво важливим інтересам України [28].

В структурі Центрального управління СБУ безпосередньо питаннями інформаційної безпеки займаються наступні функціональні підрозділи: контррозвідки, військової контррозвідки, контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, інформаційно-аналітичний.

В свою чергу в структурі СЗР особливе місце займає Департамент протидії зовнішнім загрозам національній безпеці держави.

На СЗР з метою забезпечення інформаційної безпеки держави покладаються такі основні завдання: здійснення спеціальних заходів впливу, спрямованих на підтримку національних інтересів і державної політики України в економічній, політичній, військово-технічній, екологічній та інформаційній сферах, зміцнення обороноздатності, економічного і науково- технічного розвитку; вжиття заходів протидії зовнішнім загрозам національній безпеці України, життю, здоров'ю її громадян та об'єктам державної власності за межами України [29].

Попередньо підсумуємо: в Україні інституційна системи державного управління інформаційною безпекою станом на сьогодні не готова діяти як єдина функціональна структура. На разі існують лише окремі відомства (Збройні сили України, Служба безпеки України, Служба зовнішньої розвідки та ін.) на які покладено завдання забезпечення окремих видів інформаційної безпеки. Також залишаються відкритими питання щодо нормативного визначення суб'єктів забезпечення інформаційно-психологічної безпеки, які були б наділені відповідними повноваженнями.

Таким чином, аналіз нормативно-правової бази забезпечення інформаційної безпеки України показав, що система державного управління забезпеченням інформаційної безпеки органічно поєднує у своєму складі:

а) суб'єкти управління забезпеченням інформаційною безпекою: Адміністрацію Президента України (Головний департамент з питань національної безпеки і оборони, Головний департамент з питань інформаційної політики, Головний департамент з питань гуманітарної політики); Раду національної безпеки і оборони України; Комітет з розвідки при Президентові України; Національний інститут стратегічних досліджень при Президентові України;

Верховну Раду України (Комітет з питань національної безпеки і оборони, Комітет з питань культури і духовності, Комітет з питань свободи слова та інформації, Консультативну раду з питань інформатизації та сприяння у виробленні політики у сфері інформатизації);

Секретаріат Кабінету Міністрів України (Управління розвитку інформаційного суспільства та інформаційної безпеки, Департамент інформації та комунікацій з громадськістю), Урядовий комітет з питань оборони, оборонно-промислового комплексу та правоохоронної діяльності;

а) спеціальні органи державної влади, що безпосередньо та опосередковано опікуються питаннями забезпечення інформаційної безпеки: Міністерство інформаційної політики та культури України, Міністерство оборони України, Міністерство внутрішніх справ України, Міністерство освіти та науки України, Міністерство фінансів України;

б) об'єкти управління забезпеченням інформаційної безпеки:

об'єкти інформаційної безпеки; інституційне середовище, система та механізми забезпечення інформаційної безпеки; сили та засоби державного реагування на загрози інформаційній безпеці.

Аналіз сучасного стану системи державного управління забезпеченням інформаційної безпеки України дозволяє констатувати, що ця система залишається остаточно не сформованою й не готовою діяти як єдина функціональна структура.

В Україні створено в цілому достатню нормативно-правову базу діяльності держави із забезпечення національної безпеки загалом та інформаційної безпеки зокрема. Основою цієї бази є Конституція України, прийнята на п'ятій сесії Верховної Ради

України 28 червня 1996 р. [11]. Відносини у цій сфері регулюються низкою спеціальних законів та підзаконних нормативно-правових актів, до яких, зокрема, належать закони України «Про державну таємницю» [30], «Про інформацію» [31], «Про доступ до публічної інформації» [32], «Про основи національної безпеки України» [33], затверджені указами Президента України, Стратегія національної безпеки України [34], Стратегія кібербезпеки України [35], Воєнна доктрина України [8], Доктрина інформаційної безпеки України [36], затверджений наказом Служби безпеки України Звід відомостей, що становлять державну таємницю [37], та інші нормативно-правові акти.

Конституція України поряд із захистом суверенітету і територіальної цілісності України, забезпечення її економічної безпеки визначає захист інформаційної безпеки як одну з найважливіших функцій держави, справу всього Українського народу (ст. 17) [11].

Під національними інтересами Закон України «Про основи національної безпеки України» розуміє життєво важливі матеріальні, інтелектуальні та духовні цінності Українського народу як носія суверенітету і єдиного джерела влади в Україні, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток (абз. 3 ст. 1) [33].

Основні напрями державної політики з питань національної безпеки України в інформаційній сфері, що визначені Законом № 964-ГУ, знайшли подальший, більш деталізований розвиток у Стратегії національної безпеки України, схваленій рішенням Ради національної безпеки і оборони України від 6 травня 2015 р. та затвердженій Указом Президента України від 26 травня 2015 р. № 287/2015 (Стратегія НБУ) [34].

До актуальних загроз інформаційній безпеці Стратегія НБУ відносить ведення інформаційної війни проти України, відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства (п. 3.6) [34].

Серед основних напрямів державної політики національної безпеки України Стратегія НБУ двома групами заходів формулює завдання держави щодо протидії загрозам в інформаційній сфері: заходи щодо забезпечення інформаційної безпеки та заходи щодо забезпечення кібербезпеки і безпеки інформаційних ресурсів.

Згідно зі Стратегією НБУ пріоритетами забезпечення інформаційної безпеки є:

– забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії;

– створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

– протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства;

– розробка і реалізація скоординованої інформаційної політики органів державної влади;

– виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;

– створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики держав-членів НАТО;

– удосконалення професійної підготовки у сфері інформаційної безпеки, упровадження загальнонаціональних освітніх програм з медіакультури із залученням громадянського суспільства та бізнесу (п. 4.11) [34].

Пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів відповідно до Стратегії НБУ є:

– розвиток інформаційної інфраструктури держави;

– створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT);

– моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації;

– розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів;

– забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого в Російській Федерації;

– реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав-членів НАТО та ЄС;

– створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони;

– розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки (п. 4.12) [34].

Важливим кроком у захисті національних інтересів України в інформаційній сфері стало затвердження Указом Президента України від 25 лютого 2017 р. № 47/2017 Доктрини інформаційної безпеки України (Доктрина-2017) [36].

Логічно припустити, що зміст Доктрини – 2017, як і будь-якого іншого акта, повинен базуватися на розумінні змісту поняття, що є предметом його регулювання. Однак Доктрина – 2017 не подає значення терміна «інформаційна безпека» і не містить посилання на інші акти, які визначають його сутність.

У Доктрині – 2017 визначено ‘її мету та принципи, національні інтереси та актуальні загрози національним інтересам і національній безпеці України та пріоритети державної політики в інформаційній сфері, а також механізм реалізації Доктрини.

Як особливий інструментарій досягнення мети Доктрина – 2017 визначає систему комунікацій – стратегічних, урядових та кризових – як спеціалізованих (різнорівневих, різнопредметних та різносуб’єктних) комплексів заходів з реалізації державної політики в забезпеченні інформаційної безпеки України (абз. 7, 8, 9 розд. 1) [36]. Значення Доктрини – 2017 як у площині протидії загрозам інформаційній та національній безпеці України, осучаснення векторності діяльності держави у захисті інформаційного простору країни від зовнішньої інформаційної агресії, так і з точки зору вдосконалення нормативно-правового регулювання інформаційної сфери є безперечним. Зміст Доктрини-2017 переконливо доводить, що інформаційна безпека є невід’ємною органічною складовою системи національної безпеки України. Хоча, звичайно, ефективність викладених у Доктрині – 2017 положень залежатиме від ретельності, послідовності, вчасності, якості їх виконання, а також інших чинників, що впливатимуть на реалізацію в цілому державної політики в інформаційній сфері на всіх рівнях всіма суб’єктами інформаційних відносин.

Сучасний стан системи забезпечення інформаційної безпеки потребує вирішення наступних завдань:

– реформування системи забезпечення інформаційної безпеки України з урахуванням особливостей національного інформаційного простору України;

– розроблення та практичного освоєння системи спільної морально-психологічної підготовки особового складу Збройних Сил України, інших військових формувань і правоохоронних органів до застосування в умовах гібридної війни;

– розроблення та практичного освоєння системи спільної підготовки організаційних структур Збройних Сил України, інших військових формувань і правоохоронних органів до ведення інформаційно-психологічного протиборства;

– відновлення повного контролю та забезпечення надійного захисту національного інформаційного простору;

– підвищення ефективності протидії інформаційному тероризму;

– запровадження ефективного контррозвідувального режиму на всій території України;

– визначення системи асиметричних дії, спрямованих на ліквідацію можливої переваги над нашою державою у інформаційній сфері;

– підготовки і проведення спеціальної інформаційної операції, спрямованої на подолання наслідків окупації у східних та південних регіонах України.

Виконання вказаних завдань передбачає вдосконалення державної політики забезпеченням інформаційної безпеки України в умовах гібридної війни на сучасному етапі за напрямами:

– розробка перспективної моделі системи забезпечення інформаційної безпеки Української держави в умовах гібридної війни;

– розробити та упровадити в державно-управлінську практику модель організації системи державного управління забезпеченням інформаційної безпеки в умовах інформаційно-психологічного протиборства, що дозволить системно впливають на інформаційну безпеку Української держави та забезпечити нестандартність системно-інституційної поведінки суб'єктів інформаційної безпеки для попередження негативних зовнішніх інформаційно-психологічних впливів;

– для адаптації системи забезпечення інформаційної безпеки до нових викликів і загроз здійснювати систематизацію нормативно-законодавчої бази за доктринально-стратегічним, тактичним, функціонально-спеціальним рівнями.

Під систематизацією законодавства розуміють – діяльність суб'єктів права з втілення комплексу заходів, що спрямовані на приведення нормативної бази в єдину внутрішньо узгоджену систему шляхом удосконалення, звільнення від застарілих і суперечливих норм та усунення прогалин у праві та чинному законодавстві [38, с. 11]. До доктринально-стратегічного, в першу чергу, необхідно відносити нормативно-правові акти, які в сукупності закріплюють систему цінностей, цілей, принципи функціонування системи забезпечення інформаційної безпеки, визначають систему офіційних поглядів на місце і роль держави в сфері забезпечення інформаційної безпеки, визначають наявні і потенційні загрози у інформаційній сфері [39]. До тактичного рівня належать акти, що визначають суб'єктів забезпечення інформаційної безпеки та основні напрями їх діяльності і взаємодії, що у сукупності утворює систему, забезпечення інформаційної безпеки та вихідні принципи, які визначають стратегію діяльності суб'єктів забезпечення інформаційної безпеки. Основну частину предмета правового регулювання вказаної частини складатимуть цілі, завдання окремих суб'єктів забезпечення інформаційної безпеки, предмет їх діяльності, форми та засоби досягнення поставленої мети, організація і порядок їх взаємодії.

Функціонально-спеціальний рівень містить документи, що деталізують діяльності суб'єктів забезпечення інформаційної безпеки за певних обставин. Планування на вказаному рівні здійснюється в межах діяльності окремо взятого суб'єкта. Відповідно, плани суб'єктів забезпечення інформаційної безпеки повинні містити конкретні практичні заходи з реалізації тактичного рівня.

На нашу думку, це надасть можливість привести нормативну базу у сфері забезпечення інформаційної безпеки в єдину узгоджену систему шляхом удосконалення, звільнення від застарілих і суперечливих норм та усунення дублювання і прогалин у праві та чинному законодавстві; присвоїть інформаційно-психологічній безпеці статусу пріоритетного напряму в роботі органів законодавчої та виконавчої влади; розширить перелік викликів і загроз інформаційно-психологічного характеру та конкретизувати положення законів України «Про основи національної безпеки України», «Про засади внутрішньої і зовнішньої політики», Стратегії національної безпеки, Доктрини інформаційної безпеки України, Воєнної доктрини України щодо протидії інформаційно-психоло-

гічним впливам; оптимізує структуру та функції системи забезпечення інформаційної безпеки України з урахуванням сучасних викликів і загроз національним інтересам України в інформаційній сфері та вимог до систем забезпечення безпеки креативного типу; удосконалити механізм інформаційно-аналітичного забезпечення шляхом розробки та впровадження в державно-управлінську практику паспортів загроз інформаційно-психологічній безпеці; удосконалити механізм державного реагування шляхом розробки та впровадження в державно-управлінську практику технологій державного реагування на загрози інформаційно-психологічній безпеці; удосконалити механізм кадрового забезпечення шляхом упровадження інноваційних підходів до формування практико орієнтованого навчання фахівців-управлінців у сфері інформаційної безпеки України; удосконалити класифікацію загроз інформаційній безпеці в умовах інформаційно-психологічного протиборства шляхом доповнення таких критеріїв класифікації як критерію форми реалізації деструктивного інформаційно-психологічного впливу, що дозволяє визначити ступінь маскування ворожих та недоброзичливих намірів суб'єктів протиборства (явні та сугестивні загрози), критерію напрямів деструктивного інформаційно-психологічного впливу на масову свідомість.

Напередодні війни при РНБО України в 2021 році був створений Центр протидії дезінформації, мета діяльності якого полягала в розробці та реалізації заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою [40].

На наш погляд, актуальними завданнями Центру протидії дезінформації у воєнний час повинні бути: паралельна розробка та реалізація стратегічного та ситуаційного плану комплексного захисту інформації, що циркулює в системі державного управління; оперативна розробка моделі загроз проведення моделювання та оцінювання шкоди безпеки держави від реалізації можливих загроз.

Пріоритетними напрямами роботи Центру протидії дезінформації при РНБО України під час російської агресії виступають: оперативне інформування населення; виявлення

загрозливих інформаційних матеріалів маніпулятивного та дезінформаційного характеру; розкриття дезінформації та маніпуляцій; забезпечення інформаційної безпеки; налагодження взаємодії держави та інституцій громадянського суспільства щодо протидії дезінформації та деструктивним інформаційним впливам і кампаніям, організація інформаційно-просвітницьких заходів з питань підвищення медіа-грамотності суспільства; боротьба з інформаційним тероризмом.

В рамках просвітницької діяльності до державних службовців, громадян повинен бути доведений практичний алгоритм виявлення дезінформації та припинення її поширення, запропонований альянсом НАТО [41], що має такі етапи:

– перевірка джерела інформації: автор та розповсюджувач інформації, редакційна відповідальність, підтвердження облікового запису та ім'я користувача в соціальних мережах, складність та розмір дескриптора (використовуються безкоштовні детектори ботів та онлайн-інструменти, що позначають та оцінюють сайти дезінформації);

– перевірка емоційного навантаження тексту: викликає сильну емоційну реакцію, особливо відчуття страху та гніву;

– перевірка історії публікації: використовують сайти перевірки фактів, такі як BBC Reality Check і AFP Fact Check , що дозволяють перевірити точність історій;

– перевірка документальності, правдивості зображень: використовують платформи Google, TinEye і Bing, що дозволяють запускати зворотний пошук зображень, щоб побачити, де зображення з'являється в Інтернеті, і знайти схожі зображення. Інструменти SurfSafe та Serelay визначають підроблені зображення;

– включення критичного мислення до інформації, яка містить власні уподобання або переконання громадян.

Дезінформація, пропаганда та дезінформація були викликом протягом десятиліть, але особливо небезпечними стали під час війни. Дезінформація як державних, так і недержавних суб'єктів намагається посіяти паніку, спотворити оперативну інформацію з дипломатичних, культурних, економічних, військових фронтів (особливо стосується громадян, що перебувають в зоні бойових дій або на тимчасово окупованих територіях), підірвати довіру до демократичних інституцій і представити авторитарні режими як кращі для забезпечення якості життя громадян.

Висновки. Загрози національній безпеці України в інформаційній сфері накопичувалися роками, особливо в період з 2014 року. Поміж них найнебезпечнішими є: ініціювання розбрату в українському суспільстві та знищення української громадянської нації; прославляння сепаратизму; штучне посилення реальних і вигаданих внутрішніх протиріч; створення атмосфери громадянської недовіри до дій і намірів влади; провокування актів громадянської непокори; формування у громадян України викривленого бачення української історії; агресивна і надмірна комерціалізація частотного ресурсу та медійного ринку, непрозорість політики власників провідних телерадіоканалів та газетно-журнальних холдингів з великою часткою іноземного капіталу, брутальна примітивізація змістовного складника інформаційного продукту, який нерідко має антиукраїнську спрямованість.

Особливу небезпеку створює засилля медійного простору України російськими пропагандистськими інформаційними продуктами та наративами, які звеличують і виправдовують сталінізм, ідеалізують російські спецслужби й силові структури, культивують неповагу до Української держави, її символів, принижують українську націю та інші народи, паплюжать українську мову та традиції, поширюють україножобські міфи, розпалюють міжетнічну ворожнечу на расовому ґрунті, пропагують насильство і жорстокість.

Отже, в умовах війни важливим є розробка та прийняття Національного плану дій щодо кіберзахисту та інформаційної безпеки в умовах воєнного стану. Ключовими складовими якого повинні бути: поєднання кіберспроможностей коаліційних держав для проведення активних превентивних кібероперацій проти агресора; розгортання експертно-аналітичних центрів для моделювання та прогнозування загроз, технологій та алгоритмів атак кібервійськ агресора з метою їх упередження та нівелювання ризиків для держави і суспільства, посилення комплексної системи захисту інформації органів публічної влади та об'єктів управління від місцевого до загальнодержавного рівнів, просвіта державних службовців та громадян щодо можливих кіберзагроз та заходів по їх запобіганню, безпечної роботи в середовищі інформаційних систем, соцмереж, вироблення критичного ставлення до інформації в мережі Інтернет.

Оптимізація структури та функцій системи забезпечення інформаційної безпеки України з урахуванням сучасних викликів

і загроз національним інтересам України в інформаційній сфері та вимог до систем забезпечення безпеки креативного типу, повинна включати: механізми інформаційно-аналітичного забезпечення інформаційно-психологічної безпеки, що охоплює мережу аналітичних інститутів (державних і недержавних); механізми взаємодії держави з інститутами громадянського суспільства, з міжнародними організаціями та структурами регіональної безпеки; заходи випереджального впливу на причини, що породжують загрози національним інтересам в інформаційній сфері; удосконалення механізму інформаційно-аналітичного забезпечення шляхом розробки та впровадження в державно-управлінську практику паспортів загроз інформаційно-психологічній безпеці.

Впровадження в державно-управлінську практику забезпечення інформаційної безпеки в умовах повномасштабної війни моделі системного впливу на інформаційну безпеку Української держави, яка включає: нестандартність системи, інституційну поведінка суб'єктів інформаційної безпеки з метою запобігання негативним зовнішнім інформаційно-психологічним впливам; адаптацію системи інформаційної безпеки до нових викликів і загроз.

Пріоритетним також є запровадження комплексної системи підготовки фахівців з інформаційно-психологічних операцій, що ґрунтуватиметься на європейських практиках та з урахуванням українського досвіду, набутого під час проведених спеціальних операцій. Це уможливить формування відповідного професійного кадрового резерву.

Список використаних джерел

1. Кочубей Лариса. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційнокомунікаційних технологій у сучасному донбасі). URL: https://ipiend.gov.ua/wp-content/uploads/2018/07/kochubei_informatsina.pdf

2. Propaganda diary URL: https://rusdisinfo.voxukraine.org

3. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. 496 с.

4. Індекс результативності російської пропаганди. URL: http://www.kiis.com.ua/?lang=ukr&cat=reports&id=510&page=1

5. Прес-релізи та звіти – Індекс сприйняття російсько-української війни: результати телефонного опитування, проведеного 19-24 травня 2022 року. URL: https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1113&page=2

6. Сірик А. О., Озеров С. В. Напрями протидії інформаційним заходам під час російської агресії на території України : зб. наук. пр. Харк. ун-у Повітряних Сил. Харків : ХУПС, 2015. Вип. 4 (45) С. 43–46.

7. Стратегія сталого розвитку «Україна–2020». URL: https://zakon.rada.gov.ua/laws/show/5/2015#Text

8. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України» : Указ Президента України від 24.09.2015 № 555/2015. URL: https://zakon.rada.gov.ua/laws/show/555/2015#Text

9. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : дис. ... д-ра юрид. наук: спец. 12.00.07. Одеса, 2004. 427 с.

10. Про інформацію : Закон України від 13.01.2011 № 2938-1. URL: https://zakon.rada.gov.ua/laws/show/2938-17#Text

11. Конституція України : Прийнята Верховною Радою України 28 чкрвня 1996 року. *Відом. Верховної Ради України.* 1996. № 30. Ст. 141.

12. Про Консультативну раду з питань інформатизації при Верховній Раді України : Постанова Верховної Ради України від 02.02.1998 № 77/98-ВР. *Відом. Верховної Ради України.* 1998. № 27. Ст. 184.

13. Про комітети Верховної Ради України сьомого скликання : Постанова Верховної Ради України від 25.12.2012 № 11-VII. *Відом. Верховної Ради України.* 2013. № 38. Ст. 506.

14. Про основи національної безпеки України : Закон України від 19.06.2003 № 964–IV. *Офіц. вісн. України.* 2003. № 29. Ст. 1433.

15. Про Положення про Державний комітет телебачення і радіомовлення України : Указ Президента України від 07.05.2011 № 559/2011. *Офіц. вісн. Президента України.* 2011. № 16. Ст. 734.

16. Питання Адміністрації Президента України : Указ Президента України від 14.07.2014 № 592/2014. *Офіц. вісн. Президента України.* 2014. № 3. С. 30.

17. Питання Національного інституту стратегічних досліджень : Указ Президента України від 16.12.2002 № 1158. *Офіц. вісн. України.* 2002. № 51. С. 15.

18. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 № 183/98-ВР. *Відом. Верховної Ради України.* 1998. № 35. Ст. 237.

19. Про Комітет з питань розвідки при Президентові України : Указ Президента України від 07.10.2014 № 760. *Офіц. вісн. України.* 2014. № 82. Ст. 2320.

20. Деякі питання Секретаріату Кабінету Міністрів України : Постанова Каб. Міністрів України від 27.05.2014 № 157. *Офіц. вісн. України.* 2014. № 46. Ст. 1210.

21. Про внесення змін до Регламенту Кабінету Міністрів України : Постанова Каб. Міністрів України від 12.03.2014 № 68. *Офіц. вісн. України.* 2014. № 2 (24). Ст. 735.

22. Про затвердження Регламенту Кабінету Міністрів України : Постанова Каб. Міністрів України від 18.07.2007 № 950. URL: http://zakon4.rada.gov.Ua/laws/show/950-2007-%D0%BF/paran1210#n1210

23. Про утворення урядових комітетів та затвердження їх посадового складу : Постанова Каб. Міністрів України від 19.03.2014 № 75. *Офіц. вісн. України.* 2014. № 27. Ст. 775.

24. Положення про Міністерство культури та інформаційної політики України. URL: https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text

25. Презентовано Центр стратегічних комунікацій та інформаційної безпеки. URL: https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki

26. Положення про Державний комітет телебачення і радіомовлення України : затверджене Постановою Каб. Міністрів України від 13.08.2014 № 341. URL: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=170429&cat_id=32820

27. Про Національну раду України з питань телебачення і радіомовлення : Закон України від 23.09.1997 № 538/97-ВР. *Відом. Верховної Ради України.* 1997. № 48. Ст. 296.

28. Про Службу зовнішньої розвідки України : Закон України від 01.12.2005 № 3160-IV. *Відом. Верховної Ради України.* 2006. № 8. Ст. 94.

29. Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави : Закон України від 19.06.2003 № 975-IV. URL: http://zakon3.rada.gov.ua/laws/show/975-15

30. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. URL : https://goo.gl/bSOKaF

31. Про інформацію : Закон України від 13.01.2011 № 2938-1. URL : https://goo.gl/7i2j7G

32. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL : https://goo.gl/S1gzpe

33. Про основи національної безпеки України : Закон України 09.06.2003 № 964-ГV. URL : https://goo.gl/lRoMzZ

34. Про рішення Ради національної безпеки і оборони України від 06.05.2015 «Про Стратегію національної безпеки України» : Указ Президента України від 26.05.2015 № 287. URL : https://goo.gl/OvFRER

35. Про рішення Ради національної безпеки і оборони України від 27.01.2016 «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96. URL : https://goo.gl/LqyZg7

36. Про затвердження Зводу відомостей, що становлять державну таємницю : наказ Служби безпеки України від 12.08.2005 № 440, зареєстр. в Міністерстві юстиції України 17.08.2005 р. за № 902/11182. URL: https://goo.gl/gX7y9w

37. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 № 537-V. URL : https://goo.gl/oPp05P

38. Новицький Г. В. Теоретико-правові основи забезпечення національної безпеки України : монографія. Київ : Інтертехнологія, 2008. 495 с

39. Смолянюк В. Ф. Військова могутність України: теоретико-методологічні засади формування і розвитку (політологічний аналіз досвіду 1990-х років) : монографія. Київ ; Ірпінь : ВТОР «Перун», 2000. 448 с.

40. Про рішення Ради національної безпеки і оборони України від 11.03.2021 року «Про створення Центру протидії дезінформації» : Указ Президента України від 19.03.2021 № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text

41. NATO's approach to countering disinformation: a focus on COVID-19 URL: https://www.nato.int/cps/en/natohq/177273.htm#top-tips (Last accessed: 07.06.2022).

Reference

1. Kochubei Larysa. Informatsiina bezpeka derzhavy: instrumenty zakhystu ukrainskoho informatsiinoho polia (na prykladi osoblyvostei informatsiinokomunikatsiinykh tekhnolohii u suchasnomu donbasi), Retrieved from: https://ipiend.gov.ua/wp-content/uploads/2018/07/kochubei_informatsina.pdf

2. Propaganda diary, Retrieved from: https://rusdisinfo.voxukraine.org

3. Svitova hibrydna viina: ukrainskyi front: monohrafiia / za zah. red. V. P. Horbulina, Kyiv, NISD, 2017. 496 s.

4. Indeks rezultatyvnosti rosiiskoi propahandy, Retrieved from: http://www.kiis.com.ua/?lang=ukr&cat=reports&id=510&pa ge=1

5. Pres-relizy ta zvity – Indeks spryiniattia rosiisko-ukrainskoi viiny: rezultaty telefonnoho opytuvannia, provedenoho 19-24 travnia 2022 roku, Retrieved from: https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1113&page=2

6. Siryk, A. O., Ozerov, S. V. (2015), Napriamy protydii informatsiinym zakhodam pid chas rosiiskoi ahresii na terytorii Ukrainy, Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl. Kharkiv, KhUPS, Is. 4 (45) pp. 43–46.

7. Stratehiia staloho rozvytku «Ukraina –2020», Retrieved from: https://zakon.rada.gov.ua/laws/show/5/2015#Text

8. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 2 veresnia 2015 roku «Pro novu redaktsiiu Voiennoi doktryny Ukrainy»: Ukaz Prezydenta Ukrainy vid 24.09.2015 r. № 555, Retrieved from: https://zakon.rada.gov.ua/laws/show/555/2015#Text

9. Kormych, B. A. (2004), Orhanizatsiino-pravovi osnovy polityky informatsiinoi bezpeky Ukrainy : dys. ... doktora yur. nauk: spets. 12.00.07. Odesa, 427 p.

10.Pro informatsiiu : Zakon Ukrainy vid 13.01.2011 r. № 2938-1, Retrieved from: https://zakon.rada.gov.ua/laws/show/2938-17#Text

11. Konstytutsiia Ukrainy. Pryiniata Verkhovnoiu Radoiu Ukrainy 28 chervnia 1996 roku, Vidomosti Verkhovnoi Rady Ukrainy. 1996. Is. 30. St. 141

12. Postanova Verkhovnoi Rady Ukrainy «Pro Konsultatyvnu radu z pytan informatyzatsii pry Verkhovnii Radi Ukrainy» vid 02.02.1998 № 77/98-VR, 1998, № 27, St. 184.

13. Postanova Verkhovnoi Rady Ukrainy «Pro komitety Verkhovnoi Rady Ukrainy somoho sklykannia» vid 25.12.2012 № 11-VII, Vidomosti Verkhovnoi Rady Ukrainy. 2013. № 2 38. St. 506.

14. Zakon Ukrainy «Pro osnovy natsionalnoi bezpeky Ukrainy» vid 19 chervnia 2003 r. № 964 – IV, Ofitsiinyi visnyk Ukrainy. 2003. № 29. s. 38. St. 1433.

15. Ukaz Prezydenta Ukrainy «Pro Polozhennia pro Derzhavnyi komitet telebachennia i radiomovlennia Ukrainy» vid 07 travnia 2011 r. № 559/2011. Ofitsiinyi visnyk Prezydenta Ukrainy. 2011. № 16. s. 5. St. 734.

16. Ukaz Prezydenta Ukrainy «Pytannia Administratsii Prezydenta Ukrainy» vid 14 lypnia 2014 r. № 592/2014. Ofitsiinyi visnyk Prezydenta Ukrainy. 2014. № 3. s. 30.

17. Ukaz Prezydenta Ukrainy «Pytannia Natsionalnoho instytutu stratehichnykh doslidzhen» vid 16 hrudnia 2002 roku № 1158/2002 Ofitsiinyi visnyk Ukrainy. 2002. № 51. s. 15.

18. Zakon Ukrainy «Pro Radu natsionalnoi bezpeky i oborony Ukrainy» vid 5 bereznia 1998 roku № 183/98-VR. Vidomosti Verkhovnoi Rady Ukrainy. 1998. № 35. St. 237.

19. Ukaz Prezydenta Ukrainy «Pro Komitet z pytan rozvidky pry Prezydentovi Ukrainy» vid 07 zhovtnia 2014 roku № 760/2014. Ofitsiinyi visnyk Ukrainy. 2014. № 82. s. 25. St. 2320.

20. Postanova Kabinetu Ministriv Ukrainy «Deiaki pytannia Sekretariatu Kabinetu Ministriv Ukrainy» vid 27 travnia 2014 roku № 157 Ofitsiinyi visnyk Ukrainy. 2014. № 46. s. 9. St. 1210.

21. Postanova Kabinetu Ministriv Ukrainy «Pro vnesennia zmin do Rehlamentu Kabinetu Ministriv Ukrainy» vid 12 bereznia 2014 roku № 68. Ofitsiinyi visnyk Ukrainy. 2014. №2 (24). s. 37. St. 735.

22. Postanova Kabinetu Ministriv Ukrainy «Pro zatverdzhennia Rehlamentu Kabinetu Ministriv Ukrainy» vid 18 lypnia 2007 roku № 950. Retrieved from: http://zakon4.rada.gov.Ua/laws/show/950-2007-%D0%BF/paran1210#n1210.

23. Postanova Kabinetu Ministriv Ukrainy «Pro utvorennia uriadovykh komitetiv ta zatverdzhennia yikh posadovoho skladu» vid 19.03.2014 № 75 Ofitsiinyi visnyk Ukrainy. 2014. № 27. s. 5. St. 775

24. Polozhennia pro Ministerstvo kultury ta informatsiinoi polityky Ukrainy, Retrieved from: https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text

25. Prezentovano Tsentr stratehichnykh komunikatsii ta informatsiinoi bezpeky, Retrieved from: https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki

26. Polozhennia pro Derzhavnyi komitet telebachennia i radiomovlennia Ukrainy, zatverdzhene postanovoiu KMU vid 13.08.2014 № 341, Retrieved from: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=170429&cat_id=32820

27. Zakon Ukrainy «Pro Natsionalnu radu Ukrainy z pytan telebachennia i radiomovlennia» vid 23.09.1997 r № 538/97-VR, Vidomosti Verkhovnoi Rady Ukrainy. 1997. № 48. St. 296.

28. Zakon Ukrainy «Pro Sluzhbu zovnishnoi rozvidky Ukrainy» vid 01 hrudnia 2005 roku № 3160-IV. Vidomosti Verkhovnoi Rady Ukrainy. 2006. № 8. s. 231. St. 94.

29. Zakonu Ukrainy «Pro demokratychnyi tsyvilnyi kontrol nad Voiennoiu orhanizatsiieiu i pravookhoronnymy orhanamy derzhavy» vid 19 chervnia 2003 roku № 975-IV, Retrieved from: http://zakon3.rada.gov.ua/laws/show/975-15

30. Pro derzhavnu taiemnytsiu: Zakon Ukrainy vid 21.01.1994 r. № 3855-KhII. Verkhovna Rada Ukrainy. Zakonodavstvo Ukrainy, Retrieved from: https://goo.gl/bSOKaF

31. Pro informatsiiu : Zakon Ukrainy vid 13.01.2011 r. № 2938^1. Verkhovna Rada Ukrainy. Zakonodavstvo Ukrainy, Retrieved from: https://goo.gl/7i2j7G

32. Pro dostup do publichnoi informatsii : Zakon Ukrainy vid 13.01.2011 r. № 2939-VI. Verkhovna Rada Ukrainy. Zakonodavstvo Ukrainy, Retrieved from: https://goo.gl/S1gzpe

33. Pro osnovy natsionalnoi bezpeky Ukrainy : Zakon Ukrainy 09.06.2003 № 964-HV / Verkhovna Rada Ukrainy. Zakonodavstvo Ukrainy, Retrieved from: https://goo.gl/lRoMzZ

34. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 roku «Pro Stratehiiu natsionalnoi bezpeky Ukrainy» : Ukaz Prezydenta Ukrainy vid 26.05.2015 r. № 287/2015 / Verkhovna Rada Ukrainy. Zakonodavstvo Ukrainy, Retrieved from: https://goo.gl/OvFRER

35. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku «Pro Stratehiiu kiberbezpeky Ukrainy» : Ukaz Prezydenta Ukrainy vid 15.03.2016 r. № 96/2016 / Verkhovna Rada Ukrainy. Zakonodavstvo Ukrainy, Retrieved from: https://goo.gl/LqyZg7.

36. Pro zatverdzhennia Zvodu vidomostei, shcho stanovliat derzhavnu taiemnytsiu : nakaz Sluzhby bezpeky Ukrainy vid 12.08.2005 № 440, zareiestr. v Ministerstvi yustytsii Ukrainy 17.08.2005 r. za № 902/11182 /

Verkhovna Rada Ukrainy. Zakonodavstvo Ukrainy, Retrieved from: https://goo.gl/gX7y9w

37. Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007-2015 roky : Zakon Ukrainy vid 09.01.2007 r. № 537-V / Verkhovna Rada Ukrainy. Zakonodavstvo Ukrainy, Retrieved from: https://goo.gl/oPp05P.

38. Novytskyi, H. V. (2008), Teoretyko-pravovi osnovy zabezpechennia natsionalnoi bezpeky Ukrainy : monohrafiia, Kyiv, Intertekhnolohiia, 495 p.

39. Smolianiuk, V. F. (2000), Viiskova mohutnist Ukrainy: teoretyko-metodolohichni zasady formuvannia i rozvytku (politolohichnyi analiz dosvidu 1990-kh rokiv) : monohrafiia, Kyiv; Irpin : VTOR «Perun», 448 p.

40. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 11 bereznia 2021 roku «Pro stvorennia Tsentru protydii dezinformatsii» UKAZ PREZYDENTA UKRAINY vid 19 bereznia 2021 roku № 106/2021, Retrieved from: https://zakon.rada.gov.ua/laws/show/106/2021#Text

41. NATOs approach to countering disinformation: a focus on COVID-19 URL: https://www.nato.int/cps/en/ natohq/177273.htm#top-tips (Last accessed: 07.06.2022)