УДК 342.951

НОВИЦЬКИЙ В.Я., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-7386-1221.

СТРАТЕГІЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНИХ УМОВАХ

Анотація. *Розглянуто гібридні інформаційні загрози та виклики, які поширює РФ. Окреслено основні положення сучасної Стратегії інформаційної безпеки України. Розкрито зміст, мета та завдання Стратегії інформаційної безпеки. Деталізовано концептуальні засади державної інформаційної політики в умовах сучасності. Висвітлено типові види загроз зовнішнього інформаційного впливу. Акцентовано увагу на особливостях проведення спеціальних інформаційних операцій проти України. Узагальнено стратегічні засади забезпечення інформаційної безпеки. Підсумовано здобутки вітчизняної спецслужби у сфері забезпечення інформаційної безпеки. Запропоновано уточнення компетенції вітчизняної спецслужби щодо збереження функції забезпечення інформаційної безпеки в умовах її реформування. Визначено шляхи подальшої діяльності Служби безпеки України у рамках реалізації контррозвідувальних та оперативно-розшукових заходів, спрямованих на запобігання та локалізацію деструктивної діяльності РФ на шкоду державним інтересам в інформаційній сфері.*

Ключові слова: *державна інформаційна політика, гібридні загрози, спецслужба, інформаційна безпека, вітчизняний інформаційний простір, спеціальна інформаційна операція, маніпулювання свідомістю.*

Summary. *The hybrid information threats and challenges distributed by the Russian Federation are considered. The main provisions of the modern Information Security Strategy of Ukraine are outlined. The content, purpose and tasks of the Information Security Strategy are revealed. The conceptual principles of the state information policy in modern conditions are detailed. Typical types of threats of external information influence are highlighted. Emphasis is placed on the peculiarities of conducting special information operations against Ukraine. The strategic principles of information security are generalized. The tasks and achievements of the domestic special service in the field of information security are summarized. It is proposed to clarify the competence of the domestic special service to preserve the function of information security in terms of its reform. The directions of the further activity of the Security Service of Ukraine in the framework of the implementation of counterintelligence and operational-investigative measures aimed at preventing and localizing Russian destructive activities to the detriment of state interests in the information sphere have been identified.*

Keywords: *state information policy, hybrid threats, secret service, information security, domestic information space, special information operation, manipulation of consciousness.*

Аннотация. *Рассмотрены гибридные информационные угрозы и вызовы, которые распространяет РФ. Определены основные положения современной Стратегии информационной безопасности Украины. Раскрыты содержание, цель и задачи Стратегии информационной безопасности. Детализированы концептуальные основы государственной информационной политики в условиях современности. Освещены типовые виды угроз внешнего информационного влияния. Акцентировано внимание на особенностях проведения специальных информационных операций против Украины. Обобщены стратегические основы обеспечения информационной безопасности. Подытожены результаты отечественной спецслужбы в сфере обеспечения информационной безопасности. Предложены уточнения компетенции отечественной спецслужбы касаемо сохранения функции в сфере обеспечения информационной*

безопасности в условиях ее реформирования. Определены направления дальнейшей деятельности Службы безопасности Украины в рамках реализации контрразведывательных и оперативно-разыскных мероприятий, направленных на предотвращение и локализацию деструктивной деятельности РФ во вред государственным интересам в информационной сфере.

Ключевые слова: *государственная информационная политика, гибридные угрозы, спецслужба, информационная безопасность, отечественное информационное пространство, специальная информационная операция, манипулирование сознанием.*

Постановка проблеми. Інформаційна політика в провідних країнах світу являє собою комплекс стратегічних засад діяльності відповідальних органів держави з планування та контролю процесів одержання, зберігання та поширення інформації. Окрім того, розвинені країни наразі активізують діяльність держави у напрямку законодавчого унормування відносин в державному інформаційному просторі. З цією метою такі держави схвалюють спеціальні нормативно-правові акти щодо реалізації пріоритетних засад державної інформаційної політики. В умовах сучасного світового геополітичного протиборства актуальним питанням для України залишається захист вітчизняного інформаційного простору та забезпечення державної безпеки в інформаційній сфері, особливо в умовах поширення трансформаційних гібридних загроз, які переважно поширює держава-агресор. На цьому фоні схвалення на державному рівні 28 грудня 2021 року Стратегії інформаційної безпеки [1] є важливим та відповідальним кроком у напрямку визначення подальших перспектив розбудови вітчизняної інформаційної сфери. Забезпечення інформаційної безпеки включатиме, у першу чергу, чітке розуміння та побудову алгоритмів проведення заходів щодо стримування та протидії реальним та потенційним загрозам, нейтралізації російської інформаційної агресії, у тому числі відсічі можливим спеціальним інформаційним операціям з боку держави-агресора, гарантування інформаційної стійкості суспільства та держави, динамічний розвиток міжнародної співпраці у сфері інформаційної безпеки на паритетних засадах.

Необхідність прискорення визначення в сучасних реаліях декларативних стратегічних засад забезпечення інформаційної безпеки зумовлюється такими викликами, як: складна ситуація в національній інформаційній сфері, що пов’язано як із значним інформаційним впливом, так і втручанням російських медіа; масштабне поширення російськими ЗМІ дезінформації щодо України; виконання РФ спеціального інформаційного завдання з метою дискредитації та створення негативного міжнародного іміджу України у світі; наявні технічні проблеми мовлення українських електронних засобів масової інформації в окремих регіонах нашої держави та у світі.

Невипадково у положеннях оприлюдненої у грудні 2021 року Стратегії інформаційної безпеки України задекларовано тезу про те, що інформаційна політика РФ – це загроза не лише для України, але й для інших провідних демократичних держав світу. За таких умов актуальним та своєчасним є висвітлення базових положень Стратегії інформаційної безпеки України в контексті визначення ролі та завдання вітчизняної спецслужби щодо запобігання загрозам й викликам у вітчизняному інформаційному просторі, забезпечення державної безпеки в інформаційній сфері.

Можна переконливо стверджувати про те, що з метою відновлення свого геополітичного пливу в Україні Російська Федерація, продовжуючи гібридну війну, системно застосовує для цього політичні, соціально-економічні, інформаційно-психологічні важелі та засоби. Деструктивна пропаганда як ззовні, так і всередині України, з використанням суспільних протиріч, розпалює соціальну ворожнечу, провокує конфлікти, підриває суспільну єдність. Відбувається посилення інформаційного впливу з

боку РФ, який межує з відвертим ігноруванням вимог міжнародного та вітчизняного законодавства, зокрема щодо інспірування сепаратистських та автономістських настроїв. Крім того, до проведення своєї пропагандистської деструктивної діяльності російська сторона на фінансовій основі активно залучає українських журналістів-розслідувачів. Водночас, російськими технологами розробляється ціла низка пропагандистських заходів, спрямованих на дестабілізацію внутрішньополітичної ситуації в країні напередодні та під час проведення виборів в органи місцевого самоврядування, насамперед у Східних та Південних областях (Харківська, Донецька, Луганська, Запорізька, Дніпропетровська, Херсонська, Миколаївська, Одеська), а також у Закарпатському регіоні в частині "підігрівання" сепаратистських настроїв. Також головною метою політичного керівництва РФ є нагнітання інформаційної істерії, до якої підсвідомо або цілеспрямовано залучаються й деякі українські ЗМІ, створення передумов, за яких проведення будь-яких якісних реформ стає неможливим. Це змушує усі гілки влади ситуативно реагувати на внутрішні вогнища напруги і спрямовувати зусилля на їх локалізацію, тим самим нівелюючи будь-які стабілізаційні процеси. Тобто масштаби російської пропаганди та дезінформації постійно збільшуються, набираючи обертів, що провокує розробку інституційних та організаційно-правових механізмів запобігання та протидії таким деструктивним проявам, вимагає активізації зусиль Служби безпеки України, посилення її спроможностей щодо подолання російської інформаційної експансії.

Результати аналізу наукових публікацій. Проблемні питання забезпечення інформаційної безпеки та пошук оптимальних шляхів удосконалення пріоритетних засад у цій площині висвітлювали своїх наукових працях: В. Довгань [2], Т. Ткачук [3], О. Золотар [4], Т. Перун [5], О. Солодка [6]. Ґрунтовий аналіз положень Доктрини інформаційної безпеки, яка діяла у 2017 – 2021 роках, проводили такі вчені, як: Н. Тарасенко [7], С. Гордієнко [8], Ю. Самохвалов [9], А. Турчак [10]. Проте висвітлення останніх новел законодавства, присвячених розвитку органічних стратегічних основ забезпечення інформаційної безпеки в контексті масштабного поширення гібридних загроз, ці вчені не розглядали, що зумовлює актуальність цієї статті.

Метою статті є узагальнення на підставі аналізу положень оприлюдненої Стратегії інформаційної безпеки України сучасних завдань та функцій вітчизняної спецслужби з реагування на гібридні загрози, які активно продукує РФ у вітчизняному медіа просторі.

Виклад основного матеріалу. На даний час зберігається високий рівень зовнішніх загроз у вітчизняному інформаційному просторі, викликаних активною інформаційно-пропагандистською експансією з боку РФ. Зокрема, здійснюються спроби впливати через інформаційну сферу на політичні та соціально-економічні процеси в нашій державі, підривати авторитет легітимної української влади з метою деморалізації суспільства та посилення невдоволень та протестних настроїв. Також російською стороною активно впроваджуються технології розміщення в мережі Інтернет та ЗМІ тенденційної інформації, поширення якої спрямоване на місцеве населення на окупованих територіях, громадян РФ та міжнародної спільноти. Антиукраїнська інформаційна кампанія функціонально реалізується російською стороною за низкою напрямів, якими передбачається: популяризація ідей федеративного державного устрою України як альтернативи розпаду держави; забезпечення безперервного потоку маніпулятивної дезінформації щодо подій в Україні, та на її окупованих територіях; внесення розколу в середовище українських правлячих кіл, у т.ч. шляхом публікації провокаційних та деструктивних матеріалів, критики центральних органів влади, які "ігнорують інтереси регіонів", компрометації громадсько-політичних діячів, інспірування масових протестів;

створення в Україні під прикриттям представництв європейських організацій підконтрольних російській стороні громадських структур для проведення активної роботи в інформаційно-аналітичній і гуманітарній сферах в геополітичних інтересах РФ тощо.

За таких умов, при розгляді проблеми організації забезпечення інформаційної безпеки набуває особливого значення її структурна класифікація, яка відносно умовна і будується відповідно до певних цілей і завдань. У зазначеному аспекті доцільно розділити інформаційну безпеку залежно від джерел загрози на два типи – безпеку технічного характеру, що зумовлено технологією інформаційних і комунікаційних процесів, та безпеку, яку зумовлюють соціальні чинники. Таким чином, на даний час загрози інформаційній безпеці носять соціальний характер і зосереджені у внутрішньополітичній, економічній, соціальній, екологічній, інформаційній та духовній сферах життєдіяльності нашого суспільства [5, с. 51-52].

З метою адекватного реагування на поширення гібридних загроз в Україні наприкінці 2021 року на державному рівні була схвалена Стратегія інформаційної безпеки як фундаментальний документ, який визначає завдання та шляхи діяльності держави з метою недопущення кризових явищ у вітчизняному інформаційному просторі, посилення інформаційної безпеки та її складових. Очікується, що практичне впровадження цієї Стратегії має посилити можливості держави щодо забезпечення власної інформаційної безпеки, захисту інформаційного простору. Основною загрозою безпеці України в цьому документі визначена Росія і проведена цією країною інформаційна політика. Стратегію планується реалізувати до 2025 року.

Метою цієї Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина. Досягнення мети здійснюватиметься шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки.

Цим декларативним документом (Стратегія інформаційної безпеки) визначено 7 важливих перспективних цілей. *Перша* передбачає протидію дезінформації та інформаційним операціям, насамперед з боку держави-агресора, спрямованої проти України. *Друга* – забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності. *Третя* – підвищення рівня медіакультури та медіаграмотності суспільства. *Четверта* – забезпечення дотримання прав особи на збір, зберігання, використання і поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації, а також забезпечення захисту прав журналістів. *П'ята* – інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, всеукраїнського інформаційного простору. *Шоста* – розвиток інформаційного суспільства та підвищення рівня культури діалогу. *Сьома* ціль – створення ефективної системи стратегічних комунікацій. Тобто вказані цілі формують сфери, які потребують посилення контролю з боку держави, та є визначальними в контексті забезпечення інформаційної безпеки.

Таким чином, до переліку загроз та викликів, які стоять перед нашою державою, належать: повноформатна експансійна інформаційна політика РФ; досить низький рівень медіаграмотності громадян; динамічне збільшення кількості глобальних дезінформаційних кампаній; інформаційне домінування РФ на тимчасово окупованих територіях; використання технологій маніпулювання свідомістю пересічних громадян щодо наслідків вступу України в НАТО та ЄС тощо. Зокрема планується, що успішна реалізація Стратегії інформаційної безпеки матиме такі позитивні наслідки, як: побудований захищений інформаційний простір, гарантування інформаційної безпеки держави та її складових; ефективне функціонування системи стратегічних комунікацій; запровадження механізмів ефективної протидії поширенню незаконного контенту тощо.

З цього приводу слушно вказує М. Гаврильців, що в умовах гібридної війни наша держава, що стала об'єктом агресії, неминуче наражається на широкий спектр інформаційних загроз, нейтралізація яких, з одного боку, вимагає вжиття надзвичайних правових і адміністративних заходів, а з іншого – може супроводжуватися істотним згортанням демократичних прав і свобод. Пошук балансу між інтересами національної безпеки й ідеями верховенства права – це стратегічно важливе завдання держави [11, с. 202]. Отож, нині інформаційна безпека в контексті глобалізаційних процесів та міжнародної інтеграції стає особливо важливою. Держави, що мають потужний потенціал в інформаційному середовищі, можуть впливати на країни, в яких інформаційний простір є незахищеним. Упродовж останніх трьох років Україна провела в межах інформаційного простору більшу кількість заходів по забезпеченню інформаційної безпеки, ніж за весь попередній період незалежності [10, с. 126].

Загалом існує з десяток різних видів інформаційного впливу. Тому потрібно розрізняти пропаганду, спеціальні інформаційні операції, психологічні операції, дезінформацію та інші впливи, оскільки кожен з них має свій алгоритм, форми й методи реалізації. Досвід протидії інформаційним операціям переконливо демонструє, що переважно вони плануються й організовуються із-за кордону, але з опорою на наявні оперативні позиції й можливості в країні, де проводиться така операція. Зазвичай російські інформаційні операції вирізняються тим, що вони плануються й реалізуються у рамках єдиного оперативного задуму та спільного стратегічного наративу, відрізняючись лише формами й методами реалізації, а також вибором цільової аудиторії. Але безпосередні виконавці часто мешкають в Україні, що і надає змогу вітчизняній спецслужбі викривати конкретних осіб, мережі ботоферм чи тролеферм, застосовувати до них відповідні заходи, передбачені чинним законодавством.

Наприклад, тролеферми – більш складна структура, яка має свою ієрархію, де працюють "живі" люди. Найвища ланка – це ті, хто пише пости, виступає з "експертною" думкою, ініціює дискусії й задає напрями обговорення. Як правило, вони особисто пишуть тексти на задану замовником тему, згідно із затвердженими методичними рекомендаціями. Але в них складно знайди спільні фрази і вислови. Можна побачити лише емоційно забарвлені маркери, такі як "тарифний геноцид", "київська влада", "каратєлі" тощо. Знов-таки, демаскуючою ознакою таких тролів є співпадіння меседжів і часу порушення того чи іншого питання. Нижче в ієрархії є виконавці, які поширюють дописи перших, долучаючи свої слова й активно відповідаючи на коментарі користувачів, щоб підтримували публікацію у стрічці новин. Найнижчою ланкою є особи, які здійснюють позиційне коментування. Як правило, вони поширюють заздалегідь прописані для них (10 – 20 варіантів) коментарі і неохоче дискутують. На більш-менш серйозне питання щодо теми, яка коментується, вони неспроможні відповісти. Головне завдання тролів – ініціювати в мережі інформаційну хвилю на задану тематику (або

хвилю “флуду” чи “флейму”), до якої масово приєднаються реальні користувачі, яких на професійному жаргоні росіяни називають “гарматним м’ясом”. Але бото- чи тролеферми не є небезпечними самі по собі. Їхню вражаючу ефективність забезпечує те, що майже всі сегменти бото- й тролеферм (якщо ми говоримо про російські) є функціональною складовою російських автоматизованих комплексів моніторингу мережі Інтернет із прихованими функціями впливу на процеси у середовищі соціальних мереж. Так, у РФ діють системи моніторингу компаній “Крібрум”, “Медіалогія”, “Квант”, “Бастіон”, “Brand Analytics” тощо. Кількість автоматизованих бот-акаунтів, які діють у всьому світу, складає понад 100 млн. акаунтів (тільки в системі “Крібрум”). Таке поєднання дає змогу реалізувати небезпечну технологію впливу на користувачів соціальних мереж, так званий “астротурфінг” – імітацію широкої громадської підтримки певних ідей, думок, меседжів, а також осіб чи політичних сил. Астротурфінг дає змогу створити фейкову громадську думку або інтерпретацію події, яку користувачі мережі Інтернет сприйматимуть як справжню. Наявність таких систем дозволяє РФ на основі моніторингу контенту в Інтернеті й аналітичного опрацювання “Великих даних” виявляти вразливості противника, планувати, здійснювати й коригувати власні інформаційні атаки, а також відстежувати їхню ефективність і результативність.

За таких умов не можна недооцінювати роль та місце Служби безпеки України у питаннях забезпечення інформаційної безпеки в Україні. Логічно, що у положеннях Стратегії інформаційної безпеки значна роль відводиться діяльності вітчизняної спецслужби, яка у межах своєї компетенції проводить моніторинг завдяки спеціальним методам і способам вітчизняних та іноземних засобів масової інформації та Інтернету з метою виявлення реальних та потенційних загроз державній безпеці в інформаційній сфері; організовує та забезпечує протидію проведенню проти України спеціальних інформаційних операцій, особливо з боку РФ, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України.

Так, наприклад, за результатами своєї успішної діяльності із запобігання та протидії інформаційним загрозам, вітчизняна спецслужба за підсумками першого півріччя 2021 року прозвітувала про такі здобутки: розпочато 21 кримінальне провадження за ст. 109 та ст. 110 Кримінального кодексу України; оголошено підозру 19 особами за здійснення діяльності, відповідальність за яку передбачена ст. 109 та ст. 110 Кримінального кодексу України; заборонено в’їзд в Україну понад 50 іноземним громадянам; заблоковано 8 ботоферм загальною чисельністю понад 35 тисяч акаунтів; припинено діяльність 16 Інтернет-агітаторів; проведено понад 180 профілактичних заходів; заблоковано 58 вебресурсів, на яких поширювався фейковий та деструктивний контент [12]. У першому півріччі 2021 року кіберфахівці Служби безпеки України локалізували майже 350 потенційних загроз інформаційній безпеці нашої держави. До кримінальної відповідальності притягнуто 35 хакерів і ворожих пропагандистів, 14 зловмисників засуджено.

На цьому фоні СБУ стала дієвим інструментом у роботі РНБО. Також слід вказати, що у липні 2021 року при РНБО України створено групу з питань захисту вітчизняного інформаційного простору. Очікується, що напрацювання та результати робочої групи можуть бути використані для ініціювання внесення відповідних нормативних змін з урахуванням досвіду демократичних країн світу щодо забезпечення високого рівня захисту від трансформаційних гібридних загроз.

Висновки.

Цілеспрямоване маніпулювання громадською думкою із застосуванням технологій інформаційно-психологічного впливу – один із найбільш небезпечних проявів гібридної війни, яку держава-агресор реалізує проти України. Інформаційна безпека є

характеристикою стабільного, стійкого стану загальної системи державного управління, яка під час впливу внутрішніх та зовнішніх загроз зберігає свої важливі компоненти. Іншими словами, інформаційна безпека відповідає за захищеність інтересів громадянина та держави в інформаційній сфері від різного роду загроз, як реальних, так і віртуальних. Концепт інформаційної безпеки для України розкривається через стратегію її існування як суверенної та стабільної держави, а також через розробку та впровадження цілеспрямованої системної та виваженої політики захисту національних інтересів від зовнішніх та внутрішніх інформаційних загроз.

Важливим та актуальним правовим актом, який узагальнює нагальні та декларує актуальні питання забезпечення безпеки у вітчизняному інформаційному просторі, є Стратегія інформаційної безпеки держави, яка розрахована на наступні п'ять років (2022 – 2025 рр.). У положеннях вказаної Стратегії концептуально розкриваються такі важливі для нашої держави аспекти, як: глобальні та національні загрози й виклики для вітчизняної інформаційної безпеки; завдання та напрями реалізації базових положень Стратегії; засади стратегічного планування у цій сфері; методологія досягнення результативності виконання її базових положень; механізми успішної реалізації її положень у практичну площину в контексті розбудови засад державної інформаційної політики.

При цьому важливим завданням держави визначено прискорення затвердження плану заходів з реалізації Стратегії інформаційної безпеки та забезпечення контролю за його виконанням. Актуальним завданням державного стратегічного планування залишається раціональний розподіл державою потенційних можливостей і наявних ресурсів (людських, інформаційних, фінансових, телекомунікаційних, технічних, технологічних), завдяки яким держава гарантує забезпечення національної безпеки та стабільний соціально-економічний і цифровий розвиток громадянського суспільства в цілому. Для досягнення цієї мети необхідні достатньо високий рівень управлінської культури державного апарату та застосування методів системного аналізу й прогнозування, спеціальних методів забезпечення інформаційної безпеки тощо. Саме стратегічне планування у сфері забезпечення інформаційної безпеки дає змогу значно підвищити ефективність та якість державного управління у цій сфері. Стратегічне планування повинно розглядатися усіма органами державної влади та управління як універсальний інструмент, завдяки якому можливо забезпечити реалізацію актуальних державних завдань у сфері забезпечення інформаційної безпеки, у тому числі й з використанням механізму державно-приватного партнерства. В сучасних умовах суспільство в цілому та державний та громадський сектор ІТ-сфери зокрема, добре відчувають наслідки триваючої агресії РФ, яка має гібридний характер, проникаючи в інформаційний простір, завдаючи при цьому значної шкоди державним інтересам та приватному бізнесу. РФ намагається маніпулювати свідомістю пересічних громадян, інспірувати соціальну напругу, а також поширювати заборонену законом інформацію завдяки використанню новітніх технологій, зокрема соціальних мереж та системи мікроблогів тощо.

У найближчий перспективі прогнозується збільшення кількості проведення РФ подальших спеціальних інформаційних операцій проти України з метою створення передумов для соціальної напруги, формування загальної недовіри до чинної влади, шляхом поширення фейкової або викривленої інформації щодо діяльності центральних органів влади, військового командування, правоохоронних органів, а також стимулювання населення для участі в акціях непокори, насамперед, використовуючи соціально-економічну та суспільно-політичну проблематику. Кінцевою метою вказаної діяльності є формування суспільно-політичної платформи проросійського напрямку та

приведення до влади проросійськи-орієнтованих політиків для кардинальної зміни зовнішньополітичного курсу України.

В сучасних реаліях гібридна війна стає інтенсивнішою і набуває нових форм. Тому реформа Служби безпеки України повинна враховувати інноваційні гібридні загрози з боку Російської Федерації та надати спецслужбі додаткові механізми для протидії таким загрозам. Запобігання та недопущення реалізації з боку РФ такого сценарію "керованого хаосу" вимагає від вітчизняної спецслужби посилення спроможностей щодо реалізації контррозвідувальних та оперативно-розшукових заходів, орієнтованих, у першу чергу, на запобігання та локалізацію такої деструктивної діяльності на шкоду державним інтересам в інформаційній сфері.

Важливими завданнями, які мають зберігатися за компетенцією Служби безпеки України, є: реалізація заходів, спрямованих на виявлення, попередження та припинення використання іноземними організаціями та їх функціонерами, радикально налаштованими представниками вітчизняних мас-медійних кіл на шкоду безпеці України; вжиття на системній основі додаткових заходів, спрямованих на блокування поширення в ЗМІ та Інтернет-просторі матеріалів, що містять заклики до посягання на державний суверенітет, територіальну цілісність України, розпалювання міжнаціональних, міжконфесійних конфліктів, пропаганду війни тощо.

Використана література

1. Стратегія інформаційної безпеки: Указ Президента України від 28.12.21 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069

2. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право*. № 1(24)/2018. С. 89-103.

3. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монографія. Київ: ТОВ "Видавничий дім "АртЕк", 2018. 411 с.

4. Золотар О.О. Правові основи інформаційної безпеки людини: автореф. дис. …д-ра юрид. наук: спеціальність 12.00.07. Харків. 2018. 37 с.

5. Перун Т.С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: автореф. дис. …канд. юрид. наук: спеціальність 12.00.07. Львів. 2019. 23 с.

6. Солодка О.М. Пріоритети удосконалення інформаційної безпеки України. *Інформація і право*. № 3(15)/2015. С. 36-42.

7. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. *Резонанс.* 2017. № 18. С. 3-14. URL: http://nbuviap.gov.ua/images/rezonans/2017/rez18.pdf

8. Гордієнко С. Доктринальні положення інформаційної безпеки України в умовах сучасності. *Юридичний вісник*. 2019. № 3. URL: https://lexinform.com.ua/dumka-eksperta/doktrynalni-polozhennya-informatsijnoyi-bezpeky-ukrayiny-v-umovah-suchasnosti

9. Самохвалов Ю.Я., Браіловський М.М. Оцінка інформаційної безпеки організації за критерієм впевненості. *Захист інформації*. 2019. Т. 21. № 1. С. 13-24.

10. Турчак А.В. Основні засади державної політики забезпечення інформаційної безпеки в Україні. *Інвестиції: практика та досвід*. 2019. № 11. С. 123-127.

11. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий журнал*. 2020. № 2. С. 200-203.

12. "Україна – на вістрі гібридної атаки РФ у світі" – на міжнародній конференції в Академії СБУ обговорили досвід протидії інформаційним операціям РФ. URL: https://academy.ssu.gov.ua/ua/news-1-8-136-ukraina-–-na-vistri-gibridnoi-ataki-rf-u-sviti-–-na-mizhnarodniy-konferencii-v-akademii-sbu-obgovorili-d

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~