УДК 351.746.1

МЕЛЬНИК Дмитро Сергійович

АКТУАЛЬНІ ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ: ПИТАННЯ ВИЗНАЧЕННЯ ТА ПРОТИДІЇ

Постановка проблеми. В умовах ведення Російською Федерацією гібридної війни проти України забезпечення національної безпеки в інформаційній та інших сферах залежить від організації системної протидії наявним загрозам безпеці. Водночас на сьогодні недостатньо врегульоване питання визначення змісту й характеру загроз, викликів, ризиків та інших негативних чинників у різних сферах життєдіяльності держави, які в сукупності становлять небезпеку для життєво важливих інтересів країни. Потребує зваженого підходу процес визначення переліку реальних і потенційних загроз національній безпеці в інформаційній та інших сферах. Такий стан справ, безумовно, впливає на стан забезпечення національної безпеки в усіх сферах життєдіяльності людини, суспільства та держави.

Аналіз останніх досліджень і публікацій. Науковою розробкою категорій «загрози», «виклики», «ризики» для національної безпеки займалися вітчизняні та зарубіжні фахівці: В. Антонов, В. Горбулін, А. Качинський, М. Кушнір, В. Ліпкан, С. Лисенко, Н. Нижник, Г. Новицький, А. Першин, В. Пилипчук, О. Розвадовський, Г. Ситник, М. Стрельбицький та інші. Досліджували проблематику загроз національній безпеці в інформаційній сфері та/або інформаційній безпеці як складовій національної безпеки В. Бутузов, П. Грищук, Р. Калюжний, А. Марущак, В. Панченко, С. Петров, Д. Прокоф'єва-Янчиленко, Є. Скулиш, І. Сопілко, К. Тітуніна, Т. Ткачук, В. Фурашев, В. Шемчук. Також предметом досліджень таких учених, як В. Бут, В. Домарєв, М. Живко, М. Танцюра, В. Цимбалюк, стала організація протидії загрозам інформаційній безпеці.

Однак, попри велику кількість досліджень, досі немає ані остаточно розробленого понятійного апарату, ані єдиних підходів у науковців до визначення та класифікації загроз в інформаційній сфері. Ураховуючи динамічний характер розвитку загроз національній безпеці в інформаційній сфері у сучасних умовах, така проблематика наукових досліджень не втрачає своєї актуальності.

Метою статті є проведення правового аналізу актуальних загроз національній безпеці України в інформаційній сфері, визначення перспективних заходів протидії для її забезпечення.

Виклад основного матеріалу. У законодавстві, теорії і практиці правозастосування немає єдиного усталеного підходу до розуміння категорій «національна безпека», «інформаційна безпека», «загроза», «виклик», «ризик», хоча вони сьогодні активно використовуються в державному і громадському житті. Така ситуація зумовлює необхідність розгляду та вирішення науковцями цієї проблеми.

Відповідно до усталених у теорії безпекознавства підходів зміст поняття «національна безпека» дослідники розкривають насамперед через взаємозв'язок категорій «загрози», «виклики», «ризики», «національні інтереси», «цінності», «захищеність» тощо, щодо змістового наповнення яких у науці досі тривають дискусії. Тому спершу з'ясуємо значення терміна «загроза».

Словник української мови визначає загрозу як «те, що може заподіювати яке-небудь зло, якусь неприємність», «можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого-, чого-небудь» [1, с. 95]. У словнику С. Ожегова слово «загроза» означає потенційну небезпеку, і передбачається не лише певний процес настання змін, але й можливість їх настання [2, с. 673].

У наукових джерелах і нормативно-правових актах України підходи до визначення змісту поняття «загрози», попри їхні відмінності, збігаються в наявності взаємозв'язку понять «загроза» і «безпека». У цілому загрози безпеці визначаються як сукупність чинників та умов, що у своєму поєднанні створюють небезпеку певному об'єкту.

А. Антонов і В. Балашов визначають загрозу як процес настання змін у стані особи, суспільства й держави, які можуть створити перешкоди або унеможливити реалізацію їхніх інтересів [3, с. 48].

В. Горбулін та А. Качинський розглядають загрозу як родову ознаку безпеки та визначають її як «можливість чи неминучість виникнення соціальних, природних або техногенних явищ із прогнозованими, але неконтрольованими небажаними подіями, що можуть статись у певний момент часу в межах певної території, спричинити смерть людей чи завдати шкоди їхньому здоров'ю, призвести до матеріальних і фінансових збитків тощо» [4, с. 14].

На думку В. Ліпкана, загроза національній безпеці – це, насамперед, «явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію національних інтересів і створюють небезпеку для системи національної безпеки, життєзабезпечення її системостворюючих елементів. Вона носить завжди предметний характер, наповнена конкретним змістом і у випадку чітко вираженого небезпечного стану такого змісту надто часто набуває конкретної правової характеристики» [5, с. 547].

Загрози національній безпеці в інформаційній сфері України виступають детермінуючими факторами, що зумовлюють і породжують негативні явища, які посягають на національні інтереси в цій сфері, організацію та функціонування національ-

ного інформаційного простору загалом. Вони мають або можуть мати масштабне значення, пов'язані з ризиками та небезпеками в інших сферах [6, с. 293].

Відповідно до пункту 6 частини 1 статті 1 Закону України «Про національну безпеку України» загрози національній безпеці – це «явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України» [7]. Національна безпека визначена в цьому законі як «захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз» (п. 9 ч. 1 ст. 1).

Чинний закон, на відміну від попереднього Закону України «Про основи національної безпеки України», не визначає конкретних загроз у відповідних сферах життєдіяльності. Водночас відповідно до низки положень (п. 19 ч. 1 ст. 1, ч. 5 ст. 3, п. 2 ч. 2 ст. 26) цього ж закону актуальні загрози національній безпеці України визначаються Стратегією національної безпеки України.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає кіберзагрози як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів. У цьому законі розкривається зміст проявів таких загроз – кібератак і кіберінцидентів, кіберзлочинності та кіберзлочинів, кібершпигунства і кібертероризму, а також визначення термінів: індикатори кіберзагроз, кіберпростір, кібербезпека, кіберзахист, кібероборона, кіберрозвідка тощо [8].

Конкретні загрози національним інтересам і національній безпеці України в інформаційній сфері попередньо були визначені Стратегією національної безпеки України, затвердженою Указом Президента України від 26.05.2015 № 287/2015, що втратила чинність із прийняттям нової, а також у чинній Доктрині інформаційної безпеки України, затвердженій Указом Президента України від 25.02.2017 № 47/2017.

Зокрема, у п. 4 Доктрини інформаційної безпеки України [9] (далі – Доктрина) визначено такі загрози, що є актуальними в сучасних умовах: здійснення спеціальних інформаційних операцій (далі – СІО) проти України, спрямованих на підрив обороноздатності, деморалізацію особового складу ЗС України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні; інформаційна експансія РФ та контрольованих нею структур на території України та в інших державах; інформаційне домінування РФ на ТОТ України; недостатня розвиненість націо-

нальної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері; неефективність державної інформаційної політики, недосконаліть законодавства щодо регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіакультури суспільства; поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Очевидно, що автори Доктрини при визначенні загроз інформаційній безпеці держави використали той самий підхід, що й до визначення національних інтересів в інформаційній сфері. Однак дослідники констатують наявність у їхньому переліку термінологічної невизначеності, повторень, неповноту переліку загроз і невизначеність їхніх джерел тощо. На їхнє переконання, такі прорахунки знижують ефективність механізму забезпечення інформаційної безпеки [6, с. 289]. Відсутність переліку загроз у чинному профільному законі спричинила також наявність у Доктрині певних недоліків, зокрема щодо визначення загроз інформаційній безпеці.

Перелік загроз інформаційній безпеці України переважно узгоджується з переліком загроз національній безпеці в інформаційній сфері, визначеним новою Стратегією національної безпеки, та ним доповнюється.

Так, нова Стратегія національної безпеки України, затверджена Указом Президента України від 14.09.2020 № 392/2020 [10], як сучасні загрози національній безпеці України в інформаційній сфері визначила: стрімкі технологічні зміни та зростання ролі інформаційних технологій у всіх сферах суспільного життя; застосування Росією інформаційної «зброї» у поєднанні з енергетичною для зміцнення позицій у Європі, її намагання впливати на внутрішню ситуацію у європейських державах, підживлення триваючих конфліктів, збільшення військової присутності у Східній Європі; продовження РФ гібридної війни проти України шляхом системного застосування інформаційно-психологічних, кібернетичних, політичних, економічних і воєнних засобів для відновлення свого впливу на неї; внутрішню і зовнішню деструктивну пропаганду, що розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність, використовуючи суспільні суперечності в умовах відсутності цілісної інформаційної політики держави, слабкості системи стратегічних комунікацій; недостатню ефективність державних органів, що ускладнює вироблення і реалізацію державою ефективної політики (зокрема в інформаційній сфері), є джерелом загроз незалежності України, її суверенітету і демократії; посилення загроз для критичної інформаційної інфраструктури, пов'язаних із погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її функціонування, зокрема фізичним і кібернетичним, триваючими бойовими діями, а також тимчасовою окупацією частини території України.

Визначені стратегією загрози можна розподілити на три умовні

групи: загрози інформаційно-психологічній безпеці; загрози кібербезпеці і безпеці інформаційних ресурсів; загрози безпеці критичної інфраструктури. Однак підхід до визначення переліку загроз за вказаними групами дослідники вважають невдалим, оскільки він не враховує структуру механізму забезпечення інформаційної безпеки держави та місце елементів у ньому [6, с. 290–291].

Науковці поділяють загрози інформаційній безпеці на групи за різними критеріями: за характером прояву: на зовнішні та внутрішні; за джерелами походження: природного, техногенного, антропогенного; за характером реалізації: реальні і потенційні, здійснені й уявні; за ступенем гіпотетичної шкоди: загроза і небезпека; за ймовірністю реалізації: вірогідні, можливі, неможливі; за рівнем детермінізму: випадкові й закономірні [6; 11; 12]. Зрозуміло, що такий поділ загроз не є остаточним, адже в сучасних умовах загрози та їхні прояви періодично змінюються внаслідок локалізації й усунення небезпечних факторів або ж появи нових чи актуалізації вже наявних.

Система загроз інформаційній безпеці (як складовій національної безпеки) має комплексний характер і в загальному вигляді включає в себе загрози безпеці інформації та інформаційної інфраструктури; загрози безпеці суб'єктів інформаційної сфери й соціальних зв'язків між ними від інформаційних впливів; загрози належному порядку реалізації прав та інтересів суб'єктів інформаційної сфери [13, с. 183–184].

Разом із тим, перелік указаних загальних загроз національній безпеці України в інформаційній сфері потребує уточнення, конкретизації та доповнення у відповідних профільних стратегіях інформаційної та кібернетичної безпеки України, які розробляються на виконання приписів пункту 66 нової Стратегії національної безпеки України. Одним із пріоритетних завдань у процесі розроблення цих стратегій є об'єктивне оцінювання наявних і потенційних загроз та ступеня їхньої небезпечності для національних інтересів України.

Так, у проєкті Стратегії інформаційної безпеки України, розробленому Міністерством культури та інформаційної політики України [14], у розділі ІІ «Аналіз загроз та викликів інформаційній безпеці» визначено такі глобальні загрози та виклики для інформаційної безпеки: зростання кількості глобальних дезінформаційних кампаній на тлі недостатності спроможностей демократичних держав забезпечувати «інформаційний суверенітет»; РФ як довгострокова загроза не лише для України, але й для більшості демократичних країн внаслідок поширення російських СІО на всі ключові демократичні практики, екстраполяції відпрацьованих в Україні моделей і механізмів інформаційного втручання на інші країни; набуття соціальними мережами статусу суб'єктів міжнародних інформаційних процесів, зміна балансу інформаційних відносин внаслідок сучасних цифрових трансформацій та недостатній захист особистих / приватних прав людини в умовах формування нових підходів до забезпечення

приватності та економічного розвитку; зростання значення цифрових технологій на фоні низького рівня медіаграмотності та цифрової обізнаності населення.

Також у проєкті Стратегії визначено національні загрози та виклики: зростання інформаційно-психологічного впливу на населення країни з боку іноземних держав, насамперед РФ, що впродовж тривалого часу проводить свої СІО, спрямовані на ліквідацію української державності та ідентичності; неефективне забезпечення інформаційної присутності на ТОТ України, що не дозволяє реалізувати право громадян на доступ до об'єктивної, достовірної й суспільно важливої інформації та безпечний інформаційний простір; обмежені можливості реагувати на маніпуляції, емоційне нагнітання та цілісні дезінформаційні кампанії в умовах відсутності ефективної системи реагування; слабка координація на державному рівні протидії зовнішнім і внутрішнім інформаційним загрозам в умовах триваючого процесу становлення системи стратегічних комунікацій; неможливість ефективного розвитку українського медіаринку, впровадження прозорих правил його функціонування, зменшення залежності ЗМІ від їх власників внаслідок неунормованості медіавідносин, низької професійної підготовки медіафахівців; маніпулювання свідомістю громадян щодо вступу України в ЄС і НАТО за недостатності рівня національної консолідації щодо зовнішньополітичних пріоритетів України; вкрай незадовільне забезпечення інформаційних потреб населення на місцевому рівні; недостатній рівень культури цифрової та медіаграмотності населення для ефективної протидії маніпулятивним і деструктивним інформаційно-психологічним впливам в умовах цифрових трансформацій усіх сфер суспільного життя.

Вказані загрози та виклики стосуються переважно гуманітарних аспектів інформаційної сфери відповідно до вже сформованого розподілу в науці та українському законодавстві сфери інформаційної безпеки на інформаційно-психологічну і технологічну складові (у пункті 13 розділу III Основних засад розвитку інформаційного суспільства в Україні на 2007–2015 роки, затверджених Законом України від 9 січня 2007 року, визначено, що інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації»). Технологічні аспекти реалізації загроз національній безпеці в інформаційній сфері зазначаються в проєкті нової Стратегії кібербезпеки України.

Зокрема, автори проєкту Стратегії кібербезпеки України на 2021–2025 роки «Безпечний кіберпростір – запорука успішного розвитку країни» [15], схваленого робочою групою при НКЦК РНБО України, констатують зростання питомої ваги кіберзагроз у

спектрі загроз національній безпеці країн, а також критично зростаючий технічний рівень інструментарію реалізації цих загроз.

Проєкт визначає низку викликів і загроз інформаційній безпеці в кіберпросторі, зумовлених сучасними трендами розвитку кібербезпекового середовища у світі, викликами для країни, внутрішніми процесами та явищами.

Так, разом із низкою вже відомих і досі актуальних кіберзагроз (зростаюча кіберзлочинність і кібертероризм у національному сегменті кіберпростору; розвідувально-підривна діяльність у кіберпросторі спецслужб іноземних держав, насамперед РФ, проти України, активне використання РФ кіберпростору в гібридній війні проти України та для фінансування терористичних угруповань, недостатній рівень захисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури від кібератак тощо) розробники проєкту визначають як загрози: невпинне нарощення арсеналу кіберзброї наступального, розвідувального та підривного призначення, а також поширення використання кіберпростору для вчинення не лише кібернетичних, але й інших видів злочинів; невідповідність вимогам законодавства рівня захисту інформаційно-комунікаційних систем (ІКС) державних органів та суб'єктів господарювання, в яких обробляється службова інформація та персональні дані громадян; високу технологічну залежність України від іноземних виробників продукції ІКТ та програмного забезпечення, відсутність сучасних національних стандартів щодо безпекових вимог до ланцюга поставок відповідного обладнання, розроблення програмного забезпечення та ІКС, систем сертифікації або оцінки відповідності з безпеки такої продукції; незабезпечення кіберзахисту електронних інформаційних ресурсів значної частини підприємств, установ та організацій усіх форм власності, якими вони розпоряджаються; формування глобального ринку протиправного використання програм-вимагачів, які вимагають кошти за розблокування доступу до інформації у базах даних та інформаційних системах або нерозміщення викраденої інформації в мережі «Інтернет» тощо.

У сучасних умовах забезпечення інформаційної безпеки України безпосередньо залежить від якості організації системи протидії загрозам національній безпеці в інформаційній сфері та ефективного захисту національних інтересів за участі уповноважених суб'єктів [16, с. 71].

На переконання дослідників, усвідомлення загроз та розуміння їхнього змісту, адекватність оцінки і з'ясування ступеня їхньої реальної небезпеки визначають загальну безпекову політику держави і, відповідно, ефективність системи наявних гарантій, тенденції розвитку, зміни її структури тощо [17, с. 21].

Пріоритетні напрями державної політики в інформаційній сфері визначені в пункті 5 Доктрини інформаційної безпеки України [9]. Зокрема, пріоритетами державної політики в інформаційній сфері щодо забезпечення інформаційної безпеки держави мають бути: створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на

них; удосконалення повноважень державних регуляторних органів, які здійснюють діяльність щодо інформаційного простору держави; удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці; законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави суспільно-шкідливої та протиправної інформації визначеного змісту; визначення механізмів регулювання роботи суб'єктів інформаційної діяльності в інформаційному просторі у мирний час та в умовах запровадження правового режиму воєнного стану; створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку, насамперед у ЗС України, з урахуванням практики держав – членів НАТО; розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України; розвиток цифрового мовлення, унеможливлення впливу на його інфраструктуру суб'єктів, пов'язаних з державою-агресором, а також забезпечення повного покриття території України; побудова дієвої та ефективної системи стратегічних комунікацій; розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України; боротьба з дезінформацією та деструктивною пропагандою з боку РФ; посилення спроможностей сектору безпеки і оборони щодо протидії СІО, спрямованим проти держави Україна; виявлення й притягнення до відповідальності суб'єктів українського інформаційного простору, що створені та/або використовуються РФ для ведення інформаційної війни проти України, унеможливлення їхньої підривної діяльності; унеможливлення вільного обігу інформаційної продукції, насамперед походженням з РФ, суспільно-шкідливого та протиправного змісту; проведення розвідувальними органами акцій сприяння реалізації та захисту національних інтересів України в інформаційній сфері, протидії зовнішнім загрозам інформаційній безпеці держави поза її межами; недопущення використання інформаційного простору держави в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні.

Основні напрями діяльності держави для забезпечення її національних інтересів і безпеки, зокрема в інформаційній сфері, визначені в розділі ІІІ нової Стратегії національної безпеки України [10]: активна участь у протидії кіберзагрозам, тероризму, політичному та релігійному екстремізму; запровадження нової моделі відносин з державою-агресором РФ як джерелом довгострокових системних загроз національній безпеці України, що має забезпечити припинення агресії та відновлення територіальної цілісності України; згідно з визначеними пріоритетними завданнями уповноважених державних органів відповідно до їхньої компетенції: активна та ефективна протидія розвідувально-підривній діяльності, СІО та кібератакам, а також підрив ній пропаганді; отримання повної і достовірної упереджувальної інформації про ситуацію в Україні та світі, протидія зовнішнім загрозам

національній безпеці України, сприяння реалізації національних інтересів України в інформаційній та інших сферах для захисту життєво важливих національних інтересів від невоєнних загроз із боку іноземних держав; протидія спробам розпалювання в Україні національної, расової чи релігійної ворожнечі та ненависті, приниження національної честі та гідності, образи почуттів громадян через їхні релігійні переконання, а також обмеженням прав або встановленню привілеїв тощо за мовними або іншими ознаками; рішуче протистояння гуманітарній агресії, розвиток української культури як основи консолідації української нації та зміцнення її ідентичності; запровадження в Україні національної системи стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз, що передбачатиме: оцінку ризиків, своєчасну ідентифікацію загроз і визначення вразливостей; ефективне стратегічне планування і кризовий менеджмент; дієву координацію та чітку взаємодію органів сектору безпеки і оборони, інших державних органів, бізнесу, громадянського суспільства і населення у запобіганні й реагуванні на загрози; розвиток в Україні інклюзивного політичного діалогу через: створення системи стратегічних комунікацій, публічне обговорення актуальних проблем суспільного розвитку, підвищення рівня медіакультури суспільства, гарантування безпеки журналістів під час виконання професійних обов'язків; розвиток конкуренції у сфері надання інформаційних послуг населенню; забезпечення виконання державою лише необхідних функцій, насамперед безпекової, зовнішньополітичної, соціальної, регуляторної; здійснення в Україні цифрової трансформації, забезпечення надання адміністративних послуг через безпечне «єдине вікно» з використанням сучасних інформаційних технологій, поширення цифрової грамотності; гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури в умовах цифрової трансформації як основне завдання розвитку системи кібербезпеки; створення сприятливих умов для розвитку науки, забезпечення розбудови науково-дослідницької інфраструктури, а також ефективної взаємодії вчених із державним і приватним сектором, стимулювання інновацій та запровадження новітніх технологій, зокрема в інформаційній та телекомунікаційній сферах тощо.

Крім того, для системного захисту від загроз національній безпеці в інформаційній та інших сферах необхідним є розвиток сектору безпеки і оборони. Для цього зокрема потрібно переглянути й забезпечити реалізацію норм законодавства у сфері національної безпеки і оборони; створити систему ефективного управління та координації діяльності органів сектору безпеки і оборони, удосконалити її архітектуру; завершити створення національної системи кібербезпеки, формування сучасних спроможностей суб'єктів забезпечення кібербезпеки і кібероборони та зміцнити систему координації їхньої діяльності.

Саме за цими напрямами мають визначатися та реалізовуватися конкретні шляхи й інструменти (механізми) захисту національних інтересів і безпеки України в інформаційній сфері. Регламентують цю роботу Стратегія інформаційної безпеки та Стратегія кібербезпеки як головні документи щодо організації діяльності уповноважених суб'єктів у цій сфері національної безпеки.

Національна безпека в інформаційній сфері має забезпечуватися злагодженою системою дій компетентних суб'єктів, ефективне функціонування якої залежить від їхньої спроможності своєчасно і точно ідентифікувати загрози, здатні завдати шкоди безпеці, розпізнати та виокремити джерела загроз, впливати на них із метою недопущення настання шкідливих наслідків.

Тому при доопрацюванні проєктів указаних стратегічних документів щодо забезпечення національної безпеки в інформаційній сфері доцільно застосовувати вже усталені в західних школах безпекознавства ризикорієнтовані підходи до організації роботи систем забезпечення національної безпеки, засновані на принципі роботи «від загроз». Застосування таких передових практик у поєднанні з вітчизняним досвідом протидії гібридній агресії РФ сприятиме покращанню забезпечення національної безпеки України в інформаційній та інших сферах.

Висновки. Поняття «загроза» є одним із ключових у безпекознавстві та складовою категорії «національна безпека». Визначення змісту та конкретних проявів загроз необхідне для створення ефективної системи моніторингу й управління загрозами національній безпеці в інформаційній сфері. Пріоритетне завдання держави полягає у створенні та налагодженні стабільно функціонуючого механізму протидії таким загрозам із метою забезпечення її інформаційної безпеки. Ефективність протидії залежить від спроможності компетентних суб'єктів своєчасно і точно ідентифікувати загрози, що можуть завдати шкоди національній безпеці в інформаційній сфері, розпізнати та виокремити їхні джерела, впливати на них із метою недопущення настання шкідливих наслідків.

Список використаних джерел

1. Словник української мови : в 11 т. / АН УРСР, Ін-т мовознавства ім. О. О. Потебні ; редкол.: К. Білодід (голова) та ін. Київ : Наукова думка, 1972. Т. 3. 744 с.

2. Ожегов С. И. Словарь русского языка. Москва, 1988. 748 с.

3. Антонов А., Балашов В. Основы обеспечения безопасности личности, общества и государства : [учебное пособие]. Москва : Институт защиты предпринимателя, 1996. 170 с.

4. Горбулін В., Качинський А. Засади національної безпеки України. Київ : Інтертехнологія, 2009. 272 с.

5. Ліпкан В. А. Теоретичні основи та елементи національної безпеки України : монографія. Київ : Текст, 2003. 600 с.

6. Шемчук В. В. Загрози інформаційній безпеці: проблеми визначення та подолання. URL: http://maup.com.ua/assets/files/expert/7/23.pdf (дата звернення: 12.04.2021).

7. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2469-19 (дата звернення: 12.04.2021).

8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19/print1514243147129624 (дата звернення: 13.04.2021).

9. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25.02.2017 № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 12.04.2021).

10. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 14.04.2021).

11. Політологія : підручник. URL: https://pidruchniki.com/15341220/politologiya/ponyattya_vidi_zagroz_natsionalnim_interesam_natsionalniy_bezpetsi_informatsiyniy_sferi (дата звернення: 12.04.2021).

12. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека : термінологічний навчальний довідник / за ред. Кривуци В. Г. Київ, 2004. 508 с.

13. Ткачук Т. Ю. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право*. 2017. № 10. С. 182–186.

14. Лист Міністерства культури та інформаційної політики України щодо проекту Стратегії інформаційної безпеки України від 02.03.2021 № 2233/5.11.1.

15. Робоча група при НКЦК РНБО України схвалила проєкт Стратегії кібербезпеки України на 2021–2025 роки. URL: https://www.rnbo.gov.ua/ua/Diialnist/4838.html (дата звернення: 12.04.2021).

16. Мельник Д. С. Щодо актуальних загроз національній безпеці України в інформаційній сфері. *Актуальні проблеми управління інформаційною безпекою держави* : зб. матер. відомч. наук-практ. сем., (Київ, 26 берез. 2021 р.). Київ : НА СБУ, 2021, С. 68–71.

17. Антонов В. О. Конституційно-правові засади державної політики в галузі державної безпеки. *Державна безпека України*. Київ. 2006. № 3(6). С. 19–25.

Рецензенти:
кандидат юридичних наук
О. Шамсутдінов,
доктор юридичних наук,
старший дослідник В. Гребенюк

Аннотация. В статье исследуются актуальные угрозы национальной безопасности Украины в информационной сфере на основе анализа доктринальной и нормативно-правовой базы. По результатам анализа положений законодательства Украины и научных исследований сделан вывод об отсутствии единого подхода к определению и пониманию категории «угрозы национальной безопасности Украины в информационной сфере», которые иногда трактуются как угрозы информационной безопасности, киберугрозы и т. д.

Abstract. The article analyzes current threats to the national security of Ukraine in the field of information on the basis of the analysis of the present doctrine and normative-legal documents. Considering the results of the Ukrainian legislation analysis and a number of scientific researches the author concludes about the absence of a unified approach to determine and comprehend the category of a «threat to the national security of Ukraine in the field of information», that is sometimes interpreted as a threat to information security, cyber threat, etc.

Угрозы национальной безопасности в информационной сфере Украины являются детерминирующими факторами, порождающими ряд отрицательных явлений, которые посягают на национальную безопасность и интересы в этой области, организацию и функционирование национального информационного пространства. Такие угрозы национальной безопасности Украины могут иметь национальное или мировое значение, могут быть связаны с рисками и вызовами в других сферах жизнедеятельности. Поэтому особенно важно понимание их содержания и форм проявления для организации и эффективного противодействия, а также их локализации.

В современных условиях обеспечение информационной безопасности Украины непосредственно зависит от качества организации системы противодействия угрозам национальной безопасности в информационной сфере и эффективной защиты национальных интересов при участии уполномоченных субъектов.

Эффективность такого противодействия зависит от возможности уполномоченных субъектов своевременно и точно выявлять угрозы национальной безопасности в информационной сфере, распознавать и выделять их источники, воздействовать на них для недопущения наступления пагубных последствий.

Одной из приоритетных задач государства сегодня является создание и налаживание стабильно функционирующего механизма обеспечения национальной безопасности Украины в информационной сфере для противодействия существующим и предотвращения потенциальных угроз.

Ключевые слова: национальная безопасность, информационная сфера, обеспечение, угрозы, противодействие, функции государства.

The threats to the national security in the field of information of Ukraine are viewed as determining factors, generating a number of negative phenomena that can affect the country's national security and interests in the related sphere, organization and functioning of the national information space on the whole. Such threats to Ukraine's national security can be both of the national or international significance, related to the risks and challenges in other vitally important spheres. Therefore, their content and forms of manifestation should be borne on mind to effectively counteract their emergence and localization.

The efficiency of such a counteraction depends on the authorized bodies' capabilities to timely and accurately detect the threats to the national security in the field of information, recognize and point out their sources, influence them in order to prevent offensive and harmful consequences.

One of the state's primary tasks for today is the creation and development of a stably functioning mechanism to ensure the national security of Ukraine in the field of information for the counteraction to existing threats and prevention of potential ones.

Key words: national security, field of information, ensuring, threats, counteraction, state functions.