УДК 342.951:351.85
DOI: 10.31733/2078-3566-2023-6-302-307

Андрій КАЛАШНИК©
аспірант
(Дніпропетровський державний університет внутрішніх справ, м. Дніпро, Україна)

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАХОДИ ЗАПОБІГАННЯ ТА НЕЙТРАЛІЗАЦІЇ ВНУТРІШНІХ І ЗОВНІШНІХ ІНФОРМАЦІЙНИХ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

На підставі аналізу чинного законодавства та наукових здобутків сформовано поняття «інформаційні загрози» та досліджено заходи запобігання та нейтралізації таких загроз для цілісності національної безпеки України.

Розгляд окресленої теми у сьогоднішніх реаліях є досить актуальним, адже вирішення питань національної безпеки становить важливий елемент для потужного розвитку країни.

Висвітлено стан забезпечення національної безпеки в Україні. Доведено, що національна безпека є складною соціально-економічною проблемою, зумовленою різними чинниками, аналіз яких дозволив розглянути безпеку в сучасних умовах як невід'ємну умову діяльності людей, соціальних груп, суспільств, держав і світового співтовариства. Наголошено на доцільності визначення сучасних загроз інформаційній безпеці країни та заходів подолання деструктивних чинників їх поширення, особливо в умовах дії правового режиму воєнного стану.

Найбільшу увагу приділено інформаційним загрозам (інформаційній війні), що мають на меті створення бажаних для організаторів інформаційної пропаганди сукупності точок зору, громадської думки, взаємодоповнюючих логічних процесів мислення та думок із певних питань, що призводить до внутрішнього «розколу» країни.

Ключові слова: *інформаційна загроза, безпека, національна безпека, загрози національній безпеці, національні інтереси, державна політика.*

Постановка проблеми. Захищеність національних інтересів від певного виду загроз та викликів є гарантією збереження конституційного ладу, дотримання законодавства, безпечних умов для усебічного розвитку суспільства та забезпечення національної безпеки української держави в цілому. Цілком очевидним є те, що подальше існування, самозбереження і сталий розвиток України як суверенної, демократичної, соціальної, правової держави залежить від реалізації національно спрямованої внутрішньої та зовнішньої політики щодо захисту інтересів держави, суспільства та особи. Тобто йдеться про створення певної системи, що дає змогу їй гарантувати захищеність життєво важливих інтересів держави, суспільства і особи від внутрішніх та зовнішніх загроз, насамперед в інформаційній сфері.

Сучасна інформаційна війна, поряд з іншими формами інформаційного протиборства та інформаційного конфлікту, є проявом більш широкої категорії, а саме загроз національним інтересам та національній безпеці. Однією з актуальних проблем у сфері інформаційної безпеки є недосконалість правової бази для виявлення та запобігання таким загрозам.

Отже, й досі не вирішено проблему, як протистояти інформаційним загрозам. Навіть після початку війни в України та попри зростання негативних наслідків через інформаційну війну це питання залишається без достатньої уваги.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. Варто зазначити, що проблемні питання, пов'язані з темою дослідження, розкрито у працях таких учених: Л. Сиволап, Ю. Максименко, В. Ліпкана, В. Логінова, О. Олійника, С. Гуцу, Б. Кузьменко, А. Погребняка, І. Трубіна, В. Ткаченка та ін.

Мета статті полягає у визначенні адміністративно-правових заходів запобігання та нейтралізації внутрішніх і зовнішніх інформаційних загроз національній безпеці України.

Виклад основного матеріалу. Початок XXI століття ознаменувався стрімким розвитком інформаційного суспільства і пов'язаною з цим трансформацією різних сфер

ORCID https://orcid.org/0009-0003-2320-7506
k_appad@dduvs.in.ua

суспільних відносин.

Відповідно до Закону України «Про національну безпеку України» від 21.06.2018 національна безпека України визначається як «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних і потенційних загроз» [1].

Обов'язок держави полягає у захисті об'єктів національної безпеки (людини і громадянина та їхніх конституційних прав, свобод; суспільства; інформаційного середовища; навколишнього природного середовища, природних ресурсів; держави, конституційного ладу, суверенітету, територіальної цілісності, недоторканності) шляхом застосування різних заходів запобігання.

Заходи щодо запобігання загрозам національній безпеці включають політичні, економічні, соціальні, екологічні та військові стратегії. Головною метою є стабілізація і захист національних інтересів народу.

Враховуючи, що інформаційна безпека є невід'ємною частиною національної безпеки, її регулювання потребує ефективних механізмів у вигляді політичних рішень та прийнятті нових та актуальних нормативно-правових актів.

У період розвитку інформаційних відносин з'явився термін «інформаційна безпека». Інформаційна безпека має на меті захист і запобігання нанесенню шкоди життєво важливим інтересам особистості, суспільства і держави [2, с. 22].

Багато вчених у своїх працях висловлювали власні міркування щодо визначення поняття «інформаційна безпека». Наприклад, на думку В. Ліпкана, загрози національним інтересам та національній безпеці в інформаційній сфері є синонімом поняття «інформаційна безпека» [3], хоча, на нашу думку, ці два поняття не підлягають ототожненню і мають зовсім різні правові значення.

А. Марущак наводить таке визначення: «Інформаційна безпека – це поглиблене дослідження з питань інформаційної безпеки, пов'язане з пріоритетами розвитку інформаційного законодавства України» [4, с. 23]. Вважаємо, що дослідження є завданням інформаційної безпеки для забезпечення її захисту, але не може бути основною суттю визначення.

Отже, на жаль, сьогодні не існує єдиного поняття інформаційної безпеки, що лише послаблює процес створення дієвих засобів для забезпечення такої безпеки. Тому пропонується доповнити ст. 1 Закону України «Про національну безпеку України» від 21.06.2018 таким визначенням:

«Інформаційна безпека – це захищеність громадянина, суспільства та держави в цілому від посягань на прозорість інформації, що забезпечується різними правовими засобами з метою викорінити витік конфіденційної інформації, розповсюдження неправдивої інформації та посягання на зміну внутрішнього сприйняття світу будь-якої особи».

Інформаційна безпека як складова національної безпеки має певну структуру існування: *національні інтереси → загрози → заходи захисту, протидії та відновлення* [5, с. 8].

Вважаємо за потрібне з'ясувати, які саме існують види загроз, що впливають та порушують інформаційну безпеку, і за яким критерієм їх можна поділити на внутрішні та зовнішні.

У Законі України «Про основи національної безпеки», що наразі втратив чинність, було зазначено види інформаційних загроз, до котрих відносили:

– намагання маніпулювати суспільною свідомістю;
– прояви обмеження свободи слова та доступу громадян до інформації;
– поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм;
– розголошення інформації, що становить державну таємницю, а також конфіденційної інформації.

Після втрати чинності цим законом і прийняття нового Закону України від 21.06.2018 № 2469-VIII вищенаведений перелік видів інформаційних загроз не було включено до нормативно-правового акта, що свідчить про прогалину у новому законодавстві.

Існують інші нормативно-правові акти, що є чинними та містять перелік інформаційних загроз, але наведені у них класифікації є неповними. Наприклад, у п. 16 постанови Кабінету Міністрів України № 373 від 29.03.2006 «Про затвердження Правил

забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» зазначено види загроз для інформаційної безпеки, а саме: витік технічними каналами; несанкціоновані дії з інформацією; спеціальний вплив на засоби обробки інформації [6]. Крім того, Державний стандарт України, затверджений наказом Держстандарту України № 200 від 11.04.1997 («ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення») містить низку термінів, пов'язаних із інформаційною безпекою, що прямо стосуються класифікації загроз [7]. Так, у п. 5 «Загроза для інформації» знаходимо визначення таких понять: витік інформації; порушення цілісності інформації; перехоплення інформації.

Загалом можемо спостерігати різноманітність класифікацій інформаційних загроз та відсутність єдиного підходу в чинному законодавстві України. Така тенденція наштовхує на висновок, що природа виникнення загроз для інформаційної безпеки є недостатньо вивченою та врегульованою в Україні. У зв'язку з чим можна навести міркування вчених щодо підходів до виокремлення означених видів загроз.

Так, А. Логінов наводить таку класифікацію інформаційних загроз: розкриття інформаційних ресурсів; порушення цілісності інформаційних ресурсів; збій у роботі обладнання [8].

В. Ліпкан визначає більш розширену класифікацію, а саме: 1) за походженням: природні, техногенні або антропогенні; за ступенем передбачуваної шкоди: загрози та небезпеки; за повторюваністю практики: повторюваність та безперервність; 2) за сферою виникнення: зовнішні, внутрішні; 3) за ймовірністю реалізації: можливі, неможливі, умовні; за рівнем детермінованості: закономірні, зумовлені; за цінністю: прийнятні, допустимі; за характером впливу: системні, структурні, фундаментальні; за характером застосування: актуальні, потенційні, реалізовані, уявні; за ставленням до них: об'єктивні, суб'єктивні; за об'єктом впливу: особистість, суспільство, держава [9].

На нашу думку, класифікація, яку надано Б. Кузьменко та О. Чайковським, є більш досконалою, ніж попередні, а саме: 1) загрози конфіденційності інформації. Як наслідок, інформація стає доступною організаціям, котрі не мають права її вивчати; 2) загрози порушення цілісності інформації. Сюди входить зловмисне спотворення інформації, що обробляється за допомогою автоматизованих систем; 3) загроза порушення доступності інформації, що виникає при блокуванні доступу до певних ресурсів автоматизованих систем для легітимних користувачів [9, с. 6–7].

Найбільш науково аргументованою, на нашу думку, є класифікація А. Погребняка. Він вважає, що загрози бувають випадковими без умислу та усвідомлення наслідків, а також навмисні. До випадкових загроз належать: помилки обслуговуючого персоналу і користувачів; втрата інформації внаслідок неправильного її збереження; випадкове знищення або заміна; збій у роботі устаткування, електроживлення, дискових систем, комплектуючих елементів мережі; некоректна робота програмного забезпечення, зокрема внаслідок зараження комп'ютерними вірусами, тощо [10, с. 46–47]. Навмисними загрозами є: несанкціонований доступ до інформації і мережевих ресурсів; розкриття і модифікація даних і програм, їх копіювання; розкриття, модифікація або підміна трафіка обчислювальної мережі; розробка і поширення комп'ютерних вірусів, введення в програмне забезпечення логічних бомб; крадіжка магнітних носіїв і розрахункових документів; руйнування архівної інформації або навмисне її знищення; фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу її прийому; перехоплення та ознайомлення з інформацією, що передана каналами зв'язку [11, с. 50]. Таке бачення, дійсно, заслуговує на увагу з боку держави; завдяки такій класифікації можна виявити умисність дії суб'єкта вчинення та створення загроз, що дозволяє розробити дієву та справедливу міру покарань.

Отже, можна спостерігати відсутність єдиної позиції щодо видів та причин виникнення загроз, котрі впливають на інформаційну складову національної безпеки України.

На нашу думку, до основних видів класифікації загроз варто віднести:

1) загрози за їхніми наслідками: незначні (що не суттєво впливають на ситуації) та серйозні (що спричинили негативні наслідки у суспільстві, наприклад: розкол держави, початок внутрішніх та зовнішніх конфліктів, виникнення особистих проблем у громадян через невірне застосування інформації):

2) внутрішні (суб'єктом створення загрози є громадянин України, який перебуває

на території країни, державні органи, службові органи тощо) та зовнішні (суб'єктом створення загрози є іноземці та влада інших держав) загрози;

3) навмисні та випадкові загрози.

Сьогодні в Україні не існує універсального підходу до безпеки, що гарантував би стовідсотковий захист. Як наслідок, хакери та злочинці постійно вдосконалюють свої методи злому та проникнення. Тому системи інформаційної безпеки потребують постійного розвитку та посилення.

До адміністративно-правових заходів у цьому контексті варто віднести саме політичні та законотворчі заходи, завдяки яким створюються нові правові поняття та методи захисту.

30 березня 2023 р. Кабінет Міністрів України затвердив новий актуальний план заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року (далі – Стратегія). Сама Стратегія інформаційної безпеки була затверджена рішенням Ради національної безпеки і оборони України від 15 жовтня 2021 р.

Метою Стратегії є посилення спроможності держави гарантувати інформаційну безпеку та інформаційний простір, забезпечувати суспільно-політичну стабільність, обороноздатність держави, захист національного суверенітету, територіальної цілісності України, демократичного конституційного ладу, прав і свобод усіх громадян за допомогою інформаційних засобів та інструментів [12].

Із плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року, затвердженого розпорядженням Кабінету Міністрів України від 30 березня 2023 р. № 272-р., вбачається доречним визначити певний перелік заходів для подолання різних за видами інформаційних загроз. Наприклад, для протидії дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, із-поміж іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини і громадянина, будуть здійснюватися такі заходи:

1) здійснення збору та проведення аналізу інформаційних даних;

2) проведення моніторингу спеціальними методами і способами вітчизняних та іноземних медіа, Інтернету з метою виявлення загроз національній безпеці України в інформаційній сфері;

3) запуск та підтримка механізму системного моніторингу іноземного інформаційного поля з метою виявлення антиукраїнських та дезінформаційних наративів;

4) забезпечення на постійній основі проведення аналізу інформаційного простору з метою гнучкого реагування на потенційні загрози його функціонуванню;

5) здійснення добування, аналітичного опрацювання, оброблення та надання розвідувальної інформації в установленому Законом України «Про розвідку» порядку;

6) підготовка проведення систематичного узагальнюючого моніторингу національного інформаційного простору на предмет виявлення дезінформації, що містить загрози для національної безпеки України;

7) підготовка проведення систематичного узагальнюючого моніторингу іноземного інформаційного простору (стосовно окремих країн) на предмет виявлення дезінформації, що містить загрози для національної безпеки України;

8) проведення офіційного моніторингу телерадіопрограм українських телерадіоорганізацій та іноземних мовників, що ретранслюють свої програми на території України, тощо [13].

У цьому плані сформовано 7 основних стратегічних цілей України до 2025 р. для досягнення стабільної системи захисту інформаційної безпеки України, а також розроблено майже 50 заходів для органів державної влади, спрямованих на запобігання та нейтралізацію внутрішніх і зовнішніх інформаційних загроз.

Наведений документ можна вважати основою для зміцнення інформаційної безпеки в України у період 2023–2025 рр., але вважаємо, що одного документу замало, тим паче стратегія – це певний алгоритм дій та система заходів, що не має підвищеного контролю з боку державної влади за його реалізацією порівняно з наказом, постановою, розпорядженням, законом тощо. Постає тоді питання про те, наскільки дієвою можна вважати наявність лише однієї стратегії у боротьбі з інформаційною війною та

протидією інформаційним загрозам країні.

Висновки. Таким чином, на жаль, чинне законодавство не містить єдиного поняття інформаційної безпеки, а отже, пропонується доповнити ст. 1 Закону України «Про національну безпеку України» від 21 червня 2018 р. таким визначенням: «Інформаційна безпека – це захищеність громадянина, суспільства та держави в цілому від посягань на прозорість інформації, що забезпечується різними правовими засобами з метою викорінити витік конфіденційної інформації, розповсюдження неправдивої інформації та посягання на зміну внутрішнього сприйняття світу будь-якої особи».

Відсутність нормативно закріпленого визначення не дає повного розуміння, які ж саме діяння можна віднести до інформаційних загроз, що, відповідно, зумовлює несвоєчасність їх виявлення та нейтралізації.

Наявність наразі лише одного концептуального документа для запобігання та нейтралізації внутрішніх та зовнішніх інформаційних загроз країні та суспільству у вигляді плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року не дозволяє з упевненістю говорити про належне нормативно-правове забезпечення національної безпеки країни та її інформаційної складової, адже з огляду на положення ст. 17 Конституції України саме забезпечення інформаційної безпеки віднесено до найважливіших функцій держави нарівні із захистом українського суверенітету та територіальної цілісності.

Крім того, пропонується у законодавчій площині визначити повний перелік можливих видів інформаційних загроз національній безпеці України та детермінанти їх поширення; чіткі заходи реагування органів державної влади на виникнення таких загроз; заходи посилення юридичної відповідальності за вчинення таких дій та встановити покроковий алгоритм дій для відновлення стабільної системи захисту інформаційної безпеки. Не менш актуальним вбачається також визначення потенційних каналів проникнення деструктивної інформації в національний інформаційний простір та поступове виявлення нових потенційних загроз для суспільних, державних, інформаційних, організаційних процесів в умовах дії правового режиму воєнного стану.

Список використаних джерел

1. Про національну безпеку України : Закон України від 21 червня 2018 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#doc_info.

2. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. … канд. юрид. наук : 12.00.01. Київ, 2007. 22 с.

3. Ліпкан В. А. Національна безпека України : навч. посібник. Київ : КНТ, 2009. 576 с. URL: http://politics.ellib.org.ua/pages-cat-154.html.

4. Марущак А. І. Пріоритети розвитку інформаційного права України. *Інформація і право*. 2021. № 1. С. 20–24.

5. Олійник О. В. Організаційно-правові засади захисту інформаційних ресурсів України : автореф. … канд. юрид. наук : 12.00.07. Київ, 2016. 20 с.

6. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах : постанова Кабінету Міністрів України від 29.03.2006 № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#doc_info.

7. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Київ : Держстандарт України, 1997. 19 с. URL: https://learn.ztu.edu.ua/pluginfile.php/270982/mod_resource/content/1/dstu_3396.2-97.pdf.

8. Логінов А. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : дис. … канд. юрид. наук : 12.00.07 / Національна академія внутрішніх справ України. Київ, 2005. 200 с.

9. Кузьменко Б. В., Чайковська О. А. Захист інформації : навч. посібник. В 2 ч. Ч. 2. Програмнотехнічні засоби забезпечення інформаційної безпеки. Київ : Видавничий центр КНУКіМ, 2009. 69 с.

10. Погребняк А. В. Технології комп'ютерної безпеки : монографія. Рівне : МЕГУ, 2011. 117 с.

11. Погребняк А. В. Вдосконалення системи захисту інформаційної безпеки. Рівне : МЕГУ, 2015.

12. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

13. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року : розпорядження Кабінету Міністрів України від 30 березня 2023 р. № 272-р. URL: https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#n14.

Надійшла до редакції 05.12.2023

References

1. Pro natsionalnu bezpeku Ukrainy [On the national security of Ukraine] : Zakon Ukrainy vid 21 chervnia 2018 r. URL: https://zakon.rada.gov.ua/laws/show/2469-19#doc_info. [in Ukr.].

2. Maksymenko, Yu. Ye. (2007) Teoretyko-pravovi zasady zabezpechennia informatsiinoi bezpeky Ukrainy [Theoretical and legal principles of ensuring information security of Ukraine] : avtoref. dys. … kand. yuryd. nauk : 12.00.01. Kyiv. 22 p. [in Ukr.].

3. Lipkan, V. A. (2009) Natsionalna bezpeka Ukrainy [National security of Ukraine] : navch. posibnyk. Kyiv : KNT. 576 p. URL: http://politics.ellib.org.ua/pages-cat-154.html. [in Ukr.].

4. Marushchak, A. I. (2021) Priorytety rozvytku informatsiinoho prava Ukrainy [Priorities of development of information law of Ukraine]. *Informatsiia i pravo.* № 1, pp. 20–24. [in Ukr.].

5. Oliinyk, O. V. (2016) Orhanizatsiino-pravovi zasady zakhystu informatsiinykh resursiv Ukrainy [Organizational and legal principles of protection of information resources of Ukraine] : avtoref. … kand. yuryd. nauk : 12.00.07. Kyiv. 20 p. [in Ukr.].

6. Pro zatverdzhennia Pravyl zabezpechennia zakhystu informatsii v informatsiinykh, elektronnykh komunikatsiinykh ta informatsiino-komunikatsiinykh systemakh [On the approval of the Rules for ensuring the protection of information in information, electronic communication and information and communication systems] : postanova Kabinetu Ministriv Ukrainy vid 29.03.2006 № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#doc_info. [in Ukr.].

7. DSTU 3396.2-97. Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Terminy ta vyznachennia [DSTU 3396.2-97. Protection of information. Technical protection of information. Terms and definitions]. Kyiv : Derzhstandart Ukrainy, 1997. 19 p. URL: https://learn.ztu.edu.ua/pluginfile.php/270982/mod_resource/content/1/dstu_3396.2-97.pdf. [in Ukr.].

8. Lohinov, A. V. (2005) Administratyvno-pravove zabezpechennia informatsiinoi bezpeky orhaniv vykonavchoi vlady [Administrative and legal provision of information security of executive authorities] : dys. … kand. yuryd. nauk : 12.00.07 / Natsionalna akademiia vnutrishnikh sprav Ukrainy. Kyiv. 200 p. [in Ukr.].

9. Kuzmenko, B. V., Chaikovska, O. A. (2009) Zakhyst informatsii [Protection of information] : navch. posibnyk. V 2 ch. Ch. 2. Prohramnotekhnichni zasoby zabezpechennia informatsiinoi bezpeky. Kyiv : Vydavnychyi tsentr KNUKiM. 69 p. [in Ukr.].

10. Pohrebniak, A. V. (2011) Tekhnolohii kompiuternoi bezpeky [Computer security technologies] : monohrafiia. Rivne : MEHU. 117 p. [in Ukr.].

11. Pohrebniak, A. V. (2015) Vdoskonalennia systemy zakhystu informatsiinoi bezpeky [Improvement of the information security protection system]. Rivne : MEHU. [in Ukr.].

12. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky» [On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 «On Information Security Strategy»] : Ukaz Prezydenta Ukrainy vid 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text. [in Ukr.].

13. Pro zatverdzhennia planu zakhodiv z realizatsii Stratehii informatsiinoi bezpeky na period do 2025 roku [On the approval of the plan of measures for the implementation of the Information Security Strategy for the period until 2025] : rozporiadzhennia Kabinetu Ministriv Ukrainy vid 30 bereznia 2023 r. № 272-r. URL: https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#n14. [in Ukr.].

ABSTRACT

Andrii Kalashnyk. Administrative and legal measures for prevention and neutralization of internal and external information threat to national security of Ukraine. Based on the analysis of current legislation and scientific achievements, the author formed the concept of «informational threats» and researched measures to prevent and neutralize such threats to the integrity of the national security of Ukraine.

Consideration of this topic in today's realities is quite relevant, because solving national security issues is an important element for the strong development of the country.

The main measures to prevent and neutralize threats that affect national security include control over certain types of social relations, reforming state institutions, eradicating corruption, ensuring and complying with Ukraine's national security strategy, controlling and eradicating cybercrime, as well as ending the so-called «information war» .

The author paid the most attention to the informational threats of the «information war», which are aimed at creating a set of points of view, public opinion, complementary logical processes of thinking and opinions on certain issues, which is desirable for the organizers of information propaganda, which leads to the internal «split» of the country.

Since the full-scale invasion of Russia on the territory of Ukraine, the identification of informational threats to the national security of Ukraine has been a constant phenomenon, which requires the constant application of prevention and neutralization measures.

Keywords: *information threat, security, national security, threats to national security, national interests, state policy.*