

УДК 329.09.5

Тетяна Присяжнюк

ІНФОРМАЦІЙНО-МАНІПУЛЯТИВНІ ТЕХНОЛОГІЇ У СИСТЕМІ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Стаття присвячена дослідженню інформаційної безпеки держави через з'ясування сутності інформаційно-маніпулятивних технологій. Доведено, що в умовах новітньої гібридної війни інформаційний простір України є недостатньо захищеним від зовнішніх впливів. Загрози інформаційній безпеці аналізуються як складова системи загроз національній безпеці України.

Ключові слова: маніпулятивні технології, національна безпека, інформаційна безпека, інформаційні загрози.

В сучасних умовах глобальних та регіональних протистоянь, поширення інформаційної агресії, зіткнення різновекторних інформаційних інтересів, розповсюдження деструктивних комунікативних впливів пріоритетним стратегічним завданням стає захист національного інформаційного простору.

Загрози національній безпеці України в інформаційній сфері – це сукупність умов та чинників, які становлять небезпеку життєво важливим інтересам держави, суспільства і особи через можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси [11].

Відповідно до фундаментальних положень Доктрини інформаційної безпеки України забезпечення інформаційного суверенітету, запобігання інформаційній агресії, експансії та інформаційній блокаді України з боку іноземних держав, організацій, груп та осіб є пріоритетним завданням для нашої держави. Інформаційна безпека є сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз і являє собою сукупність інформаційно-психологічної та інформаційно-технічної безпеки держави [7].

Слід наголосити, що потреба у засобах накопичення, систематизації, пошуку, передачі інформації, її зберігання та забезпечення безпеки зростає. Актуальністю даної теми є те, що інформація стала чинником, який може призвести до військових конфліктів, істотно дезорганізувати державне управління та фінансову систему. Інформаційна сфера активно впливає на стан політичної, економічної, оборонної та інших складових частин безпеки України.

В основі дослідження концептуальні засади комплексного теоретичного аналізу понять інформаційної безпеки та інформаційно-маніпулятивних технологій, сформульовані в працях українських учених В. Бебика, С. Белая, О. Бойка, Ю. Довгаля, Л. Коваленка, Д. Корнієнка, В. Петрика, Г. Почепцова, Т. Ткачука та ін.

Метою статті є дослідження сутності інформаційно-маніпулятивних технологій, їх місця в системі загроз національній безпеці України, механізму ефективного захисту національного інформаційного простору.

Тому **завданням статті** є аналіз сутності та форм проявів сучасних інформаційних методів прихованого агресивного впливу, вияву дій, що мають маніпулятивний характер і які є реальною загрозою інтересам національної безпеки, шляхи вироблення механізмів протидії їм у всіх напрямках.

Законом України «Про інформацію» забезпечення інформаційної безпеки України віднесено до основних напрямків державної інформаційної політики. Інформація – це будь-які відомості або дані, які можуть бути збережені на матеріальних

носіях або відображені в електронному вигляді, а захист інформації – це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [14, стаття 3].

Вплив інформаційних процесів на деякі сфери життєдіяльності суспільства виявив важливі питання соціального буття, серед них питання інформаційних загроз, що спричинило посилення уваги до інформаційної безпеки.

Інформаційна безпека – 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 [6].

Чинна Стратегія національної безпеки України серед основних загроз національній безпеці, які мають безпосереднє відношення до інформаційної сфери, визначає агресивні дії Росії, що підривають суспільно-політичну стабільність з метою знищення держави Україна і захоплення її території, в тому числі інформаційно-психологічну війну, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу, а також ведення інформаційної війни проти України, вразливість державних інформаційних ресурсів до кібератак, застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [15].

Стратегія національної безпеки України актуальними загрозами національній безпеці України в інформаційній сфері також зазначає ведення інформаційної війни проти України, відсутність цілісної комунікативної політики держави та недостатній рівень медіа-культури суспільства [3, с. 12].

До загроз національній безпеці України в інформаційній сфері також варто зарахувати: прояви обмеження свободи слова та доступу громадян до інформації; викривлення, спотворення, блокування, замовчування, упереджене та тенденційне висвітлення інформації; несанкціоноване її поширення; відкриту дезінформацію; інформаційну експансію з боку інших держав та руйнівне інформаційне вторгнення у національний інформаційний простір, коли країни з потужнішим інформаційним потенціалом отримали можливість розширити свій вплив через засоби масової інформації на населення і громадськість менш потужної держави; виникнення і функціонування у національному інформаційному просторі держави невідконтрольних інформаційних потоків; поширення засобами масової інформації культури насильства, жорстокості; повільне входження України у світовий інформаційний простір; невиваженість державної інформаційної політики та відсутність необхідної інфраструктури в інформаційній сфері; розміщення дезінформації в інтернеті [8, с. 30].

Відсутність правових засобів регламентації та контролю за змістом інформації, яка циркулює в інтернеті, дозволяє багатьом розгорнути активну інформаційну діяльність. Метою маніпуляції є: внесення в суспільну та індивідуальну свідомість ворожих ідей та поглядів, дезорієнтація та дезінформація мас, послаблення певних переконань, залякування народу образом ворога.

Питання вивчення специфіки формування та використання ресурсів соціальних медіа актуалізується з огляду на те, що в інформаційному суспільстві важливі функції і процеси дедалі більше організовані за принципом мереж.

Входячи в життя суспільства, соціальні мережі дедалі глибше спричиняють у ньому соціокультурні зрушення. Контент та структура соціальних мереж, тематика спілкування відображають актуальні проблеми суспільного життя. Сучасному етапу цивілізаційного розвитку характерним є становлення глобального інформаційного суспільства, основним стратегічним ресурсом якого є інформація.

З огляду на такі властивості, як доступність, анонімність, оперативність, високий рівень довіри, сегментацію за інтересами, соціальні сервіси є гнучким та зручним інструментом прихованого інформаційного впливу – маніпулювання суспільною або масовою свідомістю [10].

Варто зауважити, що негативний вплив соціальних мереж на інформаційну безпеку держави залишається недостатньо усвідомленим у сучасному суспільстві. Інформаційна зброя може стати ефективним силовим засобом, що дозволяє вирішувати багато конфліктів без застосування традиційних засобів збройної боротьби. Аналіз ходу ведення сучасних війн засвідчує, що інформаційне протистояння між сторонами конфлікту є важливою складовою стратегії застосування «м'якої сили», а також ця складова використовується як елемент підготовки до застосування «жорсткої сили».

Слід також зазначити, що удосконалення інформаційних засобів, охоплення інформаційними мережами практично усіх верств населення, миттєве розповсюдження інформації у соціальних мережах формує інформаційний продукт масового споживання, який є об'єктом для маніпулювання масовою свідомістю громадян.

Політична маніпуляція – це система ідеологічного і духовно-психологічного впливу на масову свідомість із метою нав'язати певні ідеї, цінності, вплив на громадську думку і політичну поведінку людей для спрямування її у заданому напрямі [12, с. 91].

«Політичне маніпулювання – за визначенням О. Бойка, – комплекс психологічних, ідеологічних та організаційних дій, спрямованих на приховане корегування масової свідомості з метою стимулювання суспільної активності у потрібному маніпуляторіві напрямі в боротьбі за політичну владу, її захоплення, використання, утримання» [4, с. 9]

Особливість маніпулятивного впливу полягає у тому, що його здійснюють для досягнення тих чи інших політичних цілей і він має політичні наслідки для усього суспільства або певної його частини.

Технології політичного маніпулювання – це комплексна система методів та способів впливу на суб'єктів політики з метою прихованого управління ними. Існують різні класифікації технологій політичного маніпулювання. На думку В. Амеліна, технологічно маніпулювання масами являє собою «вплив на суспільну думку за допомогою управлінських ефектів для досягнення певних цілей комуніканта». Технологія політичної маніпуляції, на його думку, передбачає наступні моменти:

а) впровадження у свідомість під виглядом об'єктивної інформації неявного, але бажаного для певної групи осіб змісту;

б) дія на больові точки суспільної свідомості, які збуджують страх, тривогу, ненависть тощо;

в) реалізацію деяких задумів та цілей, які приховуються і досягнення яких комунікант пов'язує з підтримкою суспільною думкою своєї позиції [1, с.61].

В. Бебик серед арсеналу методів впливу виділяє такі:

– брехня — відверте підтасування фактів і поширення неправдивої інформації;

– замовчування — блокування правдивої інформації щодо діяльності того чи іншого суб'єкта політики, події тощо;

- напівправа - коли з метою забезпечити довіру аудиторії об'єктивно і докладно висвітлюються конкретні, малозначущі факти і одночасно замовчуються більш важливі або ж подається загальна хибна інтерпретація подій;
- навішування ярликів - для компрометації і відторгнення слухачами осіб чи ідей їм без доказів навішується ярлик фашиста, імперіаліста чи «червоного»;
- упровадження іміджів і кліше — укорінення в суспільну свідомість бажаних для правлячої еліти стереотипів щодо тих чи інших суб'єктів політики, окремих подій чи фактів [2, с.268-269].

У сучасних умовах українське суспільство перебуває під постійною загрозою отримання недостовірної, інколи шкідливої інформації, її несвоечасного надходження, шпигунства, кібератак. Ці фактори є елементами гібридної війни, які сприяють вторгненню агресора в національну свідомість громадян, підриву національної та інформаційної безпеки.

Значущість інформаційної безпеки як складової національної безпеки України пояснюється залежністю реалізації найбільш важливих інтересів України у воєнній сфері від інформаційних загроз. З аналізу найбільш небезпечних загроз національним інтересам України у воєнній сфері випливає, що реалізаційною основою більшості цих загроз є інформаційна. З-поміж інших загроз стабілізації воєнно-політичної обстановки та недопущення збройних конфліктів в Центральній Європі розглядаються такі: висунення територіальних претензій до України; втручання у внутрішні справи України; нестабільність воєнно-політичної обстановки навколо України; активізація сепаратистських сил і підтримання їх ззовні; заяви та акції, що дискредитують внутрішню і зовнішню політику України; войовничість політичного керівництва сусідніх країн; загострення міжетнічних і міжконфесійних суперечностей; нестабільність соціально-політичної обстановки в суміжних з Україною країн. Не виникає сумніву в тому, що всі ці загрози тією чи іншою мірою реалізуються на інформаційному рівні, причому їх інформаційна складова досить вагома [14].

Крім того, за оцінками вітчизняних експертів з проблем інформаційної безпеки, що сформовані на основі аналізу іноземного впливу на інформаційний медіа і кіберпростір України, існують ознаки реальних загроз для нашої держави. Про це свідчать такі основні тенденції: цілеспрямоване формування окремими іноземними державами негативного міжнародного іміджу України; здійснення рядом зарубіжних країн потужного інформаційного тиску на Україну з метою спонукання українського керівництва до прийняття вигідних для цих країн рішень у внутрішньо- та зовнішньополітичній сферах; посилення інформаційних заходів з перешкоджання реалізації Україною її зовнішньополітичного курсу та спонукання її до участі в проектах, які в сучасних умовах не вигідні нашій державі; дискредитація нашої держави як конкурента у сфері міжнародного військово-технічного співробітництва; зростання для України загроз кібернетичних атак, що обумовлено появою нових, більш досконалих зразків кібернетичної зброї [9, с.61].

Запорукою успішної протидії широкомасштабній зовнішній агресії та сталого розвитку інформаційного суспільства в Україні є сьогодні не лише нарощування технологічних можливостей здійснення інформаційного обміну, а й глибоке усвідомлення усіма суб'єктами інформаційних відносин необхідності здійснення усіх заходів захисту інформаційних ресурсів та забезпечення інформаційної безпеки держави [16, с. 45-46].

В умовах сучасних інформаційних протистоянь національний інформаційний простір України є недостатньо захищеним від зовнішніх негативних пропагандистських інформаційно-психологічних впливів та загроз.

Більшість проблем розвитку медіа-сфери України наразі викликані інформаційною війною у медіапросторі. У якості протидії інформаційній агресії рішення органів влади, перш за все, були і продовжують бути зведені до обмеження доступу до небезпечного або небажаного контенту.

Що стосується протидії масовому психологічному впливу через ЗМІ, то важливим фактором зміцнення національної безпеки держави та позитивного розвитку громадянського суспільства є розробка чіткої та послідовної програми побудови та розвитку засобів масової інформації, створення відповідного інформаційного простору на теренах держави та за її межами.

В Україні на конституційному рівні кожному гарантовані права на свободу думки і слова, на вільне вираження своїх поглядів і переконань, на вільне збирання, зберігання, використання і поширення інформації усно, письмово або в інший спосіб – на свій вибір. Здійснення цих прав може бути обмежене законом, зокрема, в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для захисту репутації або прав інших людей, для підтримання авторитету і неупередженості правосуддя (стаття 34 Основного Закону України) [18].

Чинний Кримінальний кодекс України передбачає кримінальну відповідальність за насильницьку зміну чи повалення конституційного ладу (ст. 109), посягання на територіальну цілісність і недоторканість України (ст. 110), порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками (ст. 161), заклики до вчинення дій, що загрожують громадському порядку (ст. 295). Проте, як наголошує український правознавець Н. Савінова, у ньому не криміналізовані інформаційно-психологічні впливи на свідомість людей із цією метою. Вона вважає, що саме шляхом здійснення впливу на свідомість можливе втягнення населення у вчинення подібних злочинів, зокрема – втягнення в сепаратистські рухи, екстремістські організації та релігійні секти [19, с.192].

Але реалізація зазначеного питання на практиці відразу стикається з необхідністю дотримання гарантованих міжнародними нормативно-правовими актами і Конституцією України прав та основоположних свобод людини, насамперед у сфері доступу до інформації. Право на доступ до інформації є конституційним правом людини, яке передбачене і гарантоване ст. 34 Конституції України, а саме: право кожного на свободу думки і слова, на вільне вираження своїх поглядів і переконань; право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб на свій вибір. Здійснення цих прав може бути обмежене лише у визначених законом випадках, проте, положення ч. 2 ст. 15 Конституції України містить імперативну норму, що цензура в державі заборонена.

У контексті дослідження, варто зазначити про можливість прийняття нового закону «Про медіа», який викликав великий резонанс в українському суспільстві. Ініціатори та розробники законопроекту «Про медіа» акцентують увагу на необхідності законодавчих змін, оскільки наявна законодавча база не відповідає сучасним реаліям і не допомагає Україні захищати свої інтереси в інформаційному просторі.

До того ж є потреба імплементації до законодавства України Директиви Європейського парламенту та Ради ЄС про аудіовізуальні медіапослуги 2010 року зі змінами, внесеними Директивою (ЄС) від 2018 року.

1 липня 2020 року Комітет Верховної Ради з питань гуманітарної та інформаційної політики рекомендував парламенту прийняти в першому читанні за основу доопрацьований законопроект «Про медіа» № 2693-д.

Доопрацьований варіант законопроекту спрямований на приведення українського законодавства в сфері медіа до відповідності поточному рівню розвитку технологій та актуальним викликам : зокрема, він пропонує покращити прозорість власності, захищати дітей, визначити правила роботи медіа під час війни, віднести до кола медіа не тільки звичні телеканали, радіостанції та провайдерів, але й пресу, інтернет-ЗМІ та соціальні мережі.

Проте медіаексперти та громадськість висловлюють свої критичні зауваження щодо блокування свободи слова. Багато запропонованих положень цього закону є дискусійними. Зокрема, це стосується розширення повноважень Національної ради з питань телебачення та радіомовлення, акцентуючи увагу на тому, що великі повноваження завжди створюють ризики вибіркового підходу – як правило, жертвами такого вибіркового підходу стають медіа, які критикують владу.

Складна воєнно-політична ситуація, яка склалася внаслідок збройної агресії Росії проти України, анексії та окупації частини території України зумовлює загрози в інформаційному просторі.

Погодимось із міркуваннями С. Дерев'янка про те, що «інформаційна війна, яка інтенсивно ведеться проти України Російською Федерацією стала істотним компонентом гібридної війни. Втягнутими в неї виявились фактично, усвідомлено чи ні, більшість громадян держави». Потужна пропагандистська машина країни-агресора зуміла створити негативний образ українців у свідомості знаної частини росіян і цим забезпечити, якщо не підтримку, то відсутність масових акцій протесту проти війни. Нестійкою є підтримка й частини громадян окремих європейських країн попри позицію глав держав ЄС та санкції [5, с. 66–67].

Тому інформаційна безпека України є невід'ємною складовою частиною системи забезпечення національної безпеки в цілому.

Отже, ефективне забезпечення національної безпеки України потребує розробки науково обґрунтованої державної політики та стратегії в інформаційній сфері, виявлення та систематичного моніторингу актуальних загроз інформаційній безпеці держави, пошуку ефективних заходів для забезпечення інформаційної безпеки, захисту від інформаційних загроз і реалізації права на отримання достовірної інформації. При цьому забезпечення інформаційної безпеки повинно бути пріоритетним напрямом державної політики, від якого залежатиме існування суверенної України, її національна безпека, соціально-економічний розвиток та її місце у світовому співтоваристві.

1. Амелин В. Н. Социология политики: Спецкурс / В. Н. Амелин. – М. : Изд-во МГУ, 1992. – 184 с.

2. Бебик В. Менеджмент виборчої кампанії: ресурси, технологія, маркетинг: Навч.-метод. Посіб.—К.:МАУП, 2001. – 389с., С.268-269

3. Белай С. В., Корнієнко Д. М. Інформаційна безпека сьогодення - невід'ємна складова воєнної безпеки. *Актуальні проблеми управління інформаційною безпекою держави*. Київ: Національна академія Служби безпеки України, 2018. 408 с.

4. Бойко О. Д. Політичне маніпулювання. Навч. посібник. Київ: Академвидав, 2010. 432 с.

5. Дерев'янка С. Гібридна війна: інформаційний вимір. Національна і регіональна безпека в умовах інформаційної війни. зб. матеріалів Міжрегіон. наук.-практ. конф. (м. Івано-Франківськ, 30 листопада 2018 року). Івано-Франківськ, 2018. С. 62–67.

6. Довгаль Ю.С. Інформаційна безпека як складова інформаційної безпеки України. *Актуальні проблеми управління інформаційною безпекою держави X*

Всеукраїнська науково-практична конференція. збірник тез наукових доповідей Київ, 4 квіт. 2019 р. СБУ, 2019. – 384 с.

7. Доктрина інформаційної безпеки України: Затверджена Указом Президента України ввід 25 лютого 2017 року №47/2017. URL :<http://zakon.rada.gov.ua/laws/show/47/2017?lang=ru>.

8. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам / У. Ільницька // Humanitarian vision. - 2016. - Vol. 2, Num. 1. - С. 27-32. - Режим доступу: http://nbuv.gov.ua/UJRN/hv_2016_2_1_7.

9. Інформаційне право : підручник / В. Я. Настюк (кер. авт.кол.), Л. П. Коваленко та ін.; за заг. ред. В. Я. Настюка, Л. П. Коваленко – Харків : Право, 2016. – 280 с.

10. Панченко В.М., Полевий В.І. Методика виявлення ознак інформаційного впливу в засобах масової інформації // Інформаційна безпека людини, суспільства, держави. – 2011. - №3 (7). – С. 67-73

11. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи (Електронний ресурс) В. Петрик. – режим доступу: <http://www.justinian.com.ua/article.php?id=3222>

12. Політична наука. Словник: категорії, поняття і терміни./ За ред. Б.Кухти.— Л.: Кальварія, 2003. – 473с., С. 91

13. Проект Закону про медіа : внесений народними депутатами України О. Ткаченком, М. Потураєвим, Є. Кравчук та ін. 27.12.2019 № 2693 URL : https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67812

14. Про інформацію : Закон України від 02.10.1992 р. № 2657-ХІІ. Поточна редакція від 21.12.2019 р. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.

15. Про рішення Ради національної безпеки і оборони України від 06.05.2015 р. «Про національну безпеку України»: Указ Президента України від 26.05.2015 р. №287-2015 [Електронний ресурс]. – Режим доступу: www.president.gov.ua/documents-2872015-190

16. Присяжнюк М. М. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки.* 2013. Вип. 30. С. 42-46

17. Коваленко Л. П. Сучасний стан розвитку інформаційної безпеки в сфері оборони. *Актуальні проблеми управління інформаційною безпекою держави X Всеукраїнська науково-практична конференція: збірник тез наукових доповідей Київ, 4 квіт. 2019 р. СБУ, 2019. – 384 с.*

18. Конституція України : Закон України від 28 червня 1996 р. № 254к/96–ВР / [Електронний ресурс]. – Режим доступу : <http://zakon1.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>.)

19. Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні : теоретичні та практичні аспекти : монографія / Н. А. Савінова. – К. : ДКС, 2011. – 342 с.

References

1. Amelyn V. N. Sotsyolohyya polytyky: Spetskurs / V. N. Amelyn. – М. : Yzdvo MNU, 1992. – 184 s. [in Russian].
2. Bebyk V. Menedzhment vyborchoyi kampaniyi: resursy, tekhnolohiya, marketynh: Navch.-metod. Posib.—К.:МАUP, 2001. – 389s., S.268-269 [in Ukrainian].
3. Belay S. V., Korniyenko D. M. Informatsiyna bezpeka s'ohodennya - nevid'yemna skladova voyennoyi bezpeky. Aktual'ni problemy upravlinnya informatsiynoyu

bezpekoyu derzhavy. Kyiv: Natsional'na akademiya Sluzhby bezpeky Ukrainy, 2018. 408 s. [in Ukrainian].

4. Boyko O. D. Politychne manipulyuvannya. Navch. posibnyk. Kyiv: Akademydav, 2010. 432 s. [in Ukrainian].

5. Derevyanko S. Hibrydna viyna: informatsiynyy vymir. Natsional'na i rehional'na bezpeka v umovakh informatsiynoyi viyny. zb. materialiv Mizhrehion. nauk.-prakt. konf. (m. Ivano-Frankivs'k, 30 lystopada 2018 roku). Ivano-Frankivs'k, 2018. S. 62–67. [in Ukrainian].

6. Dovhal' YU.S. Informatsiyna bezpeka yak skladova informatsiynoyi bezpeky Ukrainy. Aktual'ni problemy upravlinnya informatsiynoyu bezpekoyu derzhavy KH Vseukrayins'ka naukovopraktychna konferentsiya. zbirnyk tez naukovykh dopovidey Kyiv, 4 kvit. 2019 r. SBU, 2019. – 384 s. [in Ukrainian].

7. Doktryna informatsiynoyi bezpeky Ukrainy: Zatverdzhena Ukazom Prezydenta Ukrainy vvid 25 lyutoho 2017 roku №47/2017. URL :<http://zakon.rada.gov.ua/laws/show/47/2017?lang=ru>. [in Ukrainian].

5. Derevyanko S. Hybrid warfare: information dimension. National and regional security in the conditions of information war. zb. materials Interregion. scientific-practical conf. (Ivano-Frankivsk, November 30, 2018). Ivano-Frankivsk, 2018. P. 62–67. [in Ukrainian].

6. Dovgal Yu.S. Information security as a component of information security of Ukraine. Actual problems of information security management of the state X All-Ukrainian scientific-practical conference. collection of abstracts of scientific reports Kyiv, April 4. 2019 SBU, 2019. - 384 p. [in Ukrainian].

7. Doctrine of information security of Ukraine: Approved by the Decree of the President of Ukraine on February 25, 2017 №47 / 2017. URL: <http://zakon.rada.gov.ua/laws/show/47/2017?> [in Ukrainian].

8. Il'nyts'ka U. Informatsiyna bezpeka Ukrainy: suchasni vyklyky, zahrozy ta mekhanizmy protydyi nehatyvnyim informatsiyno-psykholohichnym vplyvam / U. Il'nyts'ka // Humanitarian vision. - 2016. - Vol. 2, Num. 1. - S. 27-32. - Rezhym dostupu: http://nbuv.gov.ua/UJRN/hv_2016_2_1_7. [in Ukrainian].

9. Informatsiyne pravo : pidruchnyk / V. YA. Nastyuk (ker. avt.kol.), L. P. Kovalenko ta in.; za zah. red. V. YA. Nastyuka, L. P. Kovalenko – Kharkiv : Pravo, 2016. – 280 s. [in Ukrainian].

10. Panchenko V.M., Polevyy V.I. Metodyka vyyavlennya oznak informatsiynoho vplyvu v zasobakh masovoyi informatsiyi // Informatsiyna bezpeka lyudyny, suspil'stva, derzhavy. – 2011. - №3 (7). – S. 67-73[in Ukrainian].

11. Petryk V. Sutnist' informatsiynoyi bezpeky derzhavy, suspil'stva ta osoby (Elektronnyy resurs) V. Petryk. – rezhym dostupu: <http://www.justinian.com.ua/article.php?id=3222>[in Ukrainian].

12. Politychna nauka. Slovyk: katehoriyi, ponyattya i terminy./ Za red. B.Kukhty.—L.: Kal'variya, 2003. – 473s., S. 91[in Ukrainian].

13. Proekt Zakonu pro media : vnesenyy narodnymy deputatamy Ukrainy O. Tkachenkom, M. Poturayevym, YE. Kravchuk ta in. 27.12.2019 № 2693 URL : https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67812[in Ukrainian].

14. Pro informatsiyu : Zakon Ukrainy vid 02.10.1992 r. № 2657-XII. Potochna redaktsiya vid 21.12.2019 r. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>. [in Ukrainian].

15. Pro rishennya Rady natsional'noyi bezpeky i oborony Ukrainy vid 06.05.2015 r. «Pro natsional'nu bezpeku Ukrainy»: Ukaz Prezydenta Ukrainy vid 26.05.2015 r. №287-

2015 [Elektronnyy resurs]. – Rezhym dostupu: www.president.gov.ua-documents-2872015-190[in Ukrainian].

16. Prysyzhnyuk M. M. Informatsiyna bezpeka Ukrainy v suchasnykh umovakh. Visnyk Kyyivs'koho natsional'noho universytetu imeni Tarasa Shevchenka. Viys'kovo-spetsial'ni nauky. 2013. Vyp. 30. S. 42-46[in Ukrainian].

17. Kovalenko L. P. Suchasnyy stan rozvytku informatsiynoyi bezpeky v sferi oborony. Aktual'ni problemy upravlinnya informatsiynoyu bezpekoyu derzhavy KH Vseukrayins'ka naukovo-praktychna konferentsiya: zbirnyk tez naukovykh dopovidey Kyyiv, 4 kvit. 2019 r. SBU, 2019. – 384 s. [in Ukrainian].

18. Konstytutsiya Ukrainy : Zakon Ukrainy vid 28 chervnya 1996 r. № 254k/96–VR / [Elektronnyy resurs]. – Rezhym dostupu : [http://zakon1.rada.gov.ua/laws/show/254 %D0 % BA/96-%D0 %B2 %D1 %80.](http://zakon1.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80)) [in Ukrainian].

19. Savinova N. A. Kryminal'no-pravove zabezpechennya rozvytku informatsiynoho suspil'stva v Ukraini : teoretychni ta praktychni aspekty : monohrafiya / N. A. Savinova. – K. : DKS, 2011. – 342 s. [in Ukrainian].

Prisyazhnyuk Tetyana Information and manipulative technologies in the system of threats to the national security of Ukraine

The article is devoted to the exploration of information security of the state by clarifying the essence of information and manipulative technologies. It is proved that in the conditions of the latest hybrid war the information space of Ukraine is insufficiently protected from external influences. Threats to information security are analyzed as part of the system of threats to national security of Ukraine.

In the current conditions of global and regional confrontations, the spread of information aggression, the clash of multi-vector information interests, the spread of destructive communicative influences, the priority strategic task is to protect the national information space. The difficult military-political situation that has developed as a result of Russia's armed aggression against Ukraine, annexation and occupation of part of the territory of Ukraine causes threats in the information space.

Effective national security of Ukraine requires the development of scientifically sound state policy and strategy in the information sphere, identification and systematic monitoring of current threats to information security, search for effective measures to ensure information security, protection from information threats and the right to reliable information. At the same time, ensuring information security should be a priority of state policy. Because the existence of a sovereign Ukraine, its national security, socio-economic development and its place in the world community will depend on it.

Key words: *manipulative technologies, national security, information security, information threats.*