Черниш Р. Ф.,
кандидат юридичних наук, доцент,
Національна академія Служби безпеки України
ORCID ID: *0000-0003-4176-7569*

DOI: *https://doi.org/10.17721/2413-5372.2021.1-2/156-165*

УДК 329.09.5(477)

ІНСТРУМЕНТИ ДЕСТРУКТИВНОГО ВПЛИВУ НА ДЕРЖАВНУ БЕЗПЕКУ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

«Кожен хоче, аби його інформували чесно, безсторонньо, правдиво – і повністю згідно з його поглядами!»
Гілберт Честертон

Анотація. *У статті констатовано, що новітні інформаційно-комунікаційні технології істотно підвищили залежність кожного індивіда та суспільства в цілому від надійності та достовірності використовуваної інформації. Зазначені технології останнім часом активно застосовуються не лише як реальний соціальний ресурс адаптації людини до життя, а й як засіб маніпулювання свідомістю. Науково обґрунтовуються й набувають поширення інструменти і методи інформаційного управління людьми. У процесі постійного розширення інформаційної складової постійно збільшується відсоток вирішення повсякденних практичних проблем за рахунок спеціалізованої інформації, одержуваної від засобів масової інформації та комунікації. Свідомість людини й суспільства дедалі більше підпорядковується ідеям, які пропагуються засобами масової інформації. А це, в свою чергу, робить людину відкритою і беззахисною перед маніпулятивними технологіями. Зважаючи на викладене,* ***метою статті*** *є дослідження інструменти деструктивного впливу на державну безпеку України в інформаційній сфері.*

Стверджується, що зважаючи на значну консолідацію українського народу, а також істотне зміцнення оборонного потенціалу нашої держави, представники спеціальних служб РФ вдаються до нових форм і методів війни – перехід від відкритого збройного протистояння на сході й півдні до намагань розхитати суспільно-політичну ситуацію зсередини України, в тому числі й шляхом здійснення деструктивного інформаційного впливу.

Зазначається, що наразі більшість науковців не класифікують інструменти деструктивного інформаційного впливу, як окрему інституцію. Вказана проблематика розглядається через призму аналізу інструментів російської інформаційної війни.

У заключній частині констатується, що результати аналізу інструментів деструктивного інформаційного впливу, свідчать, що вони можуть використовуватися індивідуально і комплексно. Визначальними чинниками в процесі їх вибору стають саме індивідуальні особливості об'єкту впливу – людини або соціуму. Залежно від глобальної мети деструктивного інформаційного впливу, його інструменти можуть бути спрямовані на: громадян у зоні конфлікту; громадян держави, щодо якої здійснюється інформаційна агресія, однак на території якої відсутній конфлікт; громадян країни-агресора; міжнародне співтовариство тощо. Для реалізації інструментів деструктивного інформаційного впливу на сьогодні використовуються практично всі канали сучасної комунікації.

Ключові слова: *державна безпека України в інформаційній сфері, деструктивний інформаційний вплив, інструменти деструктивного інформаційного впливу, дестабілізація, фейк.*

Постановка проблеми. Новітні інформаційно-комунікаційні технології істотно підвищили залежність кожного індивіда та суспільства в цілому від надійності та достовірності використовуваної інформації. Зазначені технології останнім часом активно застосовуються не лише як реальний соціальний ресурс адаптації людини до життя, а й як засіб маніпулювання свідомістю. Науково обґрунтовуються й набувають поширення інструменти і методи інформаційного управління людьми. У процесі постійного розширення інформаційної складової постійно збільшується відсоток вирішення повсякденних практичних проблем за рахунок спеціалізованої інформації, одержуваної від засобів масової інформації (далі – ЗМІ) та комунікації. Свідомість людини й суспільства дедалі більше підпорядковується ідеям, які пропагуються ЗМІ. А це, в свою чергу, робить людину відкритою і беззахисною перед маніпулятивними технологіями[1].

Особливої актуальності вказане питання набуло після 2014 року. З моменту, коли російська федерація, нехтуючи загальними принципами міжнародного права та порушуючи основи добросусідства, анексувала частину української території – Автономну Республіку Крим та, зважаючи на намагання подальшого утримання нашої держави в політичній і економічній залежності, стала ініціатором військового конфлікту в Україні.

Аналіз останніх досліджень і публікацій. Проблематика забезпечення державної безпеки в інформаційній сфері досліджувалася такими науковцями і практиками як: В. Горбулін, О. Довгань, І. Доронін, В. Ліпкан, Н. Марута, А. Марущак, В. Пилипчук, М. Погорецький, В. Полевий, Г. Почепцов, Н. Семен, Т. Ткачук, Н. Шуляк та інші. Проте, зважаючи на складність, багатоаспектність та актуальність окресленого питання, потребує подальшого вивчення й узагальнення представниками різних галузей юридичної науки.

Вказане, у повній мірі, стосується й необхідності дослідження інструменти деструктивного впливу на державну безпеку України в інформаційній сфері, що і є **метою цієї статті**.

Виклад основного матеріалу дослідження та його основні результати. Реалії сьогодення свідчать, що поряд із відкритим військовим протистоянням країна-агресор використовує широкий спектр політичних, економічних, інформаційних та інших засобів, які притаманні специфіці ведення так званої «гібридної війни». Зокрема:

– ініціювала висловлення антидержавницьких гасел громадянами України та проведення ними антиконституційних дій (псевдо референдуми на сході та півдні України);

– підтримала утворення на сході нашої держави незаконних збройних (терористичних) формувань;

– систематично матеріально та в інший спосіб підтримує терористів;

– члени НЗФ проходять підготовку на полігонах і в навчальних центрах та лікуються в медичних закладах РФ тощо.

Зважаючи на викладене, наша держава опинилася перед однією з найбільших загроз за всю новітню історію її незалежності – загрозу самого існування.

Особливої актуальності зазначене набуває в контексті систематичних висловлювань вищого керівництва РФ щодо необхідності відділення від України східної та північної частин, яка нібито історично нам не належить.

Поряд з тим, зважаючи на значну консолідацію українського народу, а також істотне зміцнення оборонного потенціалу нашої держави, представники спеціальних служб РФ вдаються до нових форм і методів війни – перехід від відкритого збройного протистояння на сході й півдні до намагань розхитати суспільно-політичну ситуацію зсереди-

[1] Б Калініченко, Інформаційна війна: чинники ескалації і засоби протидії (Київ, 2020) 294.

ни України, в тому числі й шляхом здійснення деструктивного інформаційного впливу.

Зазначеним заходам сприяє:

– перебування України у глибокій системній кризі, яка стала наслідком відсутності реформ і накопичення критичної маси проблем усередині країни;

– домінування протягом тривалого часу російської пропаганди в українському інформаційному просторі, а також відсутність дієвих можливостей щодо блокування відверто сепаратистського контенту;

– неузгодженість дій представників вищих органів державної влади тощо.

Наразі більшість науковців не класифікують інструменти деструктивного інформаційного впливу, як окрему інституцію. Вказана проблематика розглядається через призму аналізу інструментів російської інформаційної війни. Зокрема, Н. Семен виділяє такі: дезінформування та маніпулювання; пропаганда; намагання змінити громадську думку; психологічний та психотропний тиск; поширення чуток[1]. На думку Н. Шуляка до них також можна віднести: блокування теле- та радіоефірів; усунення з ефіру каналів національних меншин, наприклад, татарського каналу в Криму; дезінформація та поширення псевдоновин; поширення фальшивої, так званої фейкової, інформації[2].

За цих обставин, погоджуємося з твердженням І. Мудрої, що зазначені інструменти інформаційної війни є найпопулярнішими в засобах масової інформації, де ведеться постійна боротьба між правдивістю та дезінформацією, між чесністю та підкупністю, між Україною та росією[3].

Реалізація деструктивного інформаційного впливу, на нашу думку, може забезпечуватися за допомогою різних інструментів. Основними з них є:

1. Поширення фейкової інформації.

Поширення фейкової інформації – інструмент деструктивного інформаційного впливу, який полягає у використанні фахових знань, відповідних технічних і психологічних прийомів з метаю підготовки фейкової інформації та її подальшого поширення[4]. Вказане, за певних умов, в короткостроковій перспективі може призвести до негативних наслідків – виникнення осередків соціальної напруги і дестабілізації суспільно-політичної ситуації в окремому регіоні та у державі в цілому, дискредитувати країну на міжнародній арені тощо, а в довгостроковій – викликати поступової зміни світогляду і переконань громадян, підміну спогадів на фейкові[5], формування національної ідеї у вигідному для певної особи (групи осіб) ракурсі.

Констатуємо, що пересічному громадянину в реаліях сьогодення досить складно відрізнити фейкову інформацію від правдивої, а окреслена проблематика є актуальною для усієї міжнародної спільноти[6].

2. Дезінформування.

Дезінформування – інструмент деструктивного інформаційного впливу, який полягає в обмані чи введенні об'єкта спрямувань в оману щодо справжності

[1] Н Семен, Поняття «інформаційна війна» в контексті соціальних комунікацій (2016) 1 (25) *Держава та регіони*: *Серія: Соціальні комунікації* 22–25.

[2] Б Калініченко, Інформаційна війна: чинники ескалації і засоби протидії (Київ, 2020) 294.

[3] І Мудра, Інструменти інформаційної війни проти України в інтернет ЗМІ (2017) 883 *Вісник львівської політехніки «Журналістські науки»* 42–47 <https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/16124/mydrasinkova. pdf> дата звернення 07.05.2021.

[4] Р Черниш, Фейк, як один із інструментів негативного впливу на національну безпеку України в умовах ведення гібридної війни (2019) 2 *Часопис київського університету права* 109–114 <http://kul.kiev.ua/doc/chasopys2019/ CHAS19_2.pdf> дата звернення 07.05.2021.

[5] Fake news can lead to false memories <https://www.eurekalert.org/pub_releases/2019–08/afps-fnc081919.php> accessed 07.05.2021.

[6] Р Черниш, Правовий досвід країн Європейського Союзу у сфері протидії поширенню фейкової інформації (2019) 10 *Підприємництво, господарство і право* 123–128 <http://pgp-journal.kiev.ua/archive/2019/10/22.pdf> дата звернення 07.05.2021.

намірів для спонукання його до вчинення певних дій.

Найчастіше у світовій практиці застосовуються такі форми дезінформування:

– тенденційне викладення фактів – форма дезінформування, яка полягає в упередженому висвітленні фактів або іншої інформації щодо подій за допомогою спеціально підібраних правдивих даних. Як правило, за допомогою цього методу спеціально сформована інформація доводиться до об'єкта спрямувань дозовано, створюючи постійне напруження. Таке напружене становище об'єкта підтримується завдяки безперервному «підкиданню» нових порцій суворо обмежених і дозованих даних у середовище інформаційного дефіциту;

– дезінформування «від зворотного» – відбувається шляхом надання правдивих відомостей у перекрученому вигляді чи в такій ситуації, коли вони сприймаються об'єктом спрямувань як неправдиві. Унаслідок вжиття подібних заходів досягається ефект, коли об'єкт фактично знає правдиву інформацію про наміри чи конкретні дії протилежної сторони, але сприймає її неадекватно, не готовий протистояти негативному впливу;

– термінологічне «мінування» – полягає у викривленні первинної правильної суті принципово важливих, базових термінів і тлумачень загальносвітоглядного та оперативно-прикладного характеру;

– «сіре» дезінформування – передбачає використання синтезу правдивої інформації з дезінформацією;

– «чорне» (бойове) дезінформування – передбачає будь-яке спотворення реальних фактів задля досягнення цілей. Це ефективна зброя, що використовується з єдиною метою – «вибивання мізків» противнику[1].

3. Пропаганда.

Пропаганда – систематична діяльність, що передбачає формування потрібного сприйняття аудиторією наданого їй повідомлення, маніпулювання процесом роздумів, спрямовування поведінки аудиторії в напрямку, вигідному пропагандисту[2]. Тобто, вона спрямована на зміну певних орієнтацій та поведінки людей.

Позитивна (конструктивна) пропаганда прагне довести до об'єкта ті чи інші переконання у зрозумілій формі. Мета позитивної пропаганди – сприяти соціальній гармонії, злагоді, вихованню людей відповідно до загальноприйнятих цінностей. Позитивна пропаганда виконує виховну та інформаційну функції у суспільстві. Вона здійснюється на користь тих, кому адресована, а не обмеженого кола зацікавлених осіб. Позитивна пропаганда, на відміну негативної, не має маніпулятивних цілей. Через те, що «загальноприйняті цінності» вже і без пропаганди є загальноприйнятими, справжні цілі «конструктивної» пропаганди часто розходяться з тими, що декларуються пропагандистами.

Негативна (деструктивна) пропаганда нав'язує людям ті чи інші переконання за принципом «мета виправдовує засоби». Мета негативної пропаганди – розпалювання соціальної ворожнечі, ескалація соціальних конфліктів, загострення протиріч у суспільстві, пробудження низинних інстинктів у людей тощо. Це дозволяє роз'єднати людей, зробити їх слухняними волі пропагандиста.

Для пропаганди потрібна наявність ідеї, цільової аудиторії та коштів, щоб донести ідею до цільової аудиторії.

Ефективність пропаганди визначається співвідношенням фактичної кількості залучених прибічників до запланованої кількості.

[1] М Маркова, А Марков Інформаційно-психологічна війна проти населення України як сучасна реальність: стан проблеми і шляхи подолання наслідків (2016) 2 *Інтегровані комунікації* 73–85 <http://nbuv.gov.ua/UJRN/ integcommu_2016_2_15> дата звернення 07.05.2021.

[2] А Баровська, Інформаційні виклики гібридної війни: контент, канали, механізми протидії: аналіт. доп. (Київ, НІСД, 2016) 109.

Виділяють три основні критерії змісту ефективної пропаганди:

– наявність центральної тези;

– легкість розуміння цільової аудиторією;

– складність для критики (обґрунтованість тез, їх несуперечність одна одній тощо).

Таким чином, просуватиметься деяка ідея «1», доступна розумінню аудиторією «2» та стійка до критики з боку «3». І має бути дотриманий баланс між «2» та «3». Якщо баланс не дотримується, ідеї будуть просто незрозумілі значній частини цільової аудиторії або занадто вразливі для контрпропаганди.

Що стосується форми, можна виділити такі критерії:

– чіткість центральної тези – вона не повинна зливатися з фоном;

– привабливість фону[1].

4. Диверсифікація громадської думки.

Диверсифікація громадської думки – створення та надання хибної важливості дрібним питанням, акцентування на них особливої та підвищеної уваги, відволікання від реальних проблем, які потребують термінового, невідкладного вирішення.

5. Маніпуляція.

Маніпуляція – здійснення прихованого інформаційно-психологічного впливу на аудиторію з метою зміни її ставлення до певних проблем та програмування поведінки на підтримку чи на сприйняття ідей, вигідних ініціатору інформаційного впливу.

Як окрему технологію маніпулювання можна виділити так зване маніпулювання на форумах.

Даний вид технології полягає в коментуванні, в т.ч. анонімному, тієї чи іншої проблематики та ситуації різними користувачами Інтернет-ресурсу, що є ознакою демократизму і плюралізму Інтернету. Водночас, зацікавлені особи можуть активно втручатися у форуми, коментуючи, начебто й неупереджено, ті чи ті події. Насправді ж «голос народу» виявляється звичайним пропагандистським засобом, іноді провокативним, але завжди дієвим, бо здається об'єктивним. Маніпулювання на Інтернет-форумах соціально шкідливе, оскільки розповсюдження неправдивої інформації дискредитує сам інститут громадської думки, робить його вразливим і недієздатним[2].

6. Психологічний тиск.

Психологічний тиск – інструмент деструктивного інформаційного впливу, який полягає у впливі на психіку людини та спрямований на підрив громадського духу, деморалізацію збройних сил і дезорієнтацію вищих органів державної влади.

7. Поширення чуток.

Поширення чуток – діяльність щодо поширення різної інформації (переважно неправдивої) серед широких верств населення здебільшого неофіційними каналами для дезорганізації суспільства і держави чи окремих державних інституцій.

Чутки, як форма міжособистісної комунікації, спрямовані на формування почуття страху, апатії, тривоги перед потенційною загрозою. Залякана людина більш схильна піддаватися маніпулюванню та користується не так раціональним, скільки емоційним сприйняттям. Це робить людину вразливою, схильною до необдуманих вчинків, адже деформується сприйняття справжньої реальності[3].

Американські фахівці з психологічної війни виокремлюють такі характеристики чуток: а) вони повинні бути логічними і достовірними; б) вони мають формуватися довкола ситуації чи персони, які добре відомі; в) ефект чуток зростає за умови їх важливості для безпеки слухача, його теперішнього стану

[1] Информационная и гибридная война <https://intellect.icu/informatsionnaya-i-gibridnaya-vojna-8758> дата звернення 07.05.2021.

[2] І Сологуб, Кому ми довіряємо? <https://voxukraine.org/komu-my-doviryayemo/> дата звернення 07.05.2021.

[3] О Саєнко, Механізм інформаційно-психологічного впливу в умовах гібридної війни (2015) 1 *Вісник Національної академії Державної прикордонної служби України Серія: Психологія* <http://nbuv.gov.ua/UJRN/Vnadpn_2015_1_11> дата звернення 07.05.2021.

і поглядів на майбутнє; г) вони повинні сприяти особистому рішенню зробити що-небудь чи підготуватися до майбутньої дії; ґ) поклик має бути емоційним і прагматичним; д) вони повинні бути простими, аби їх можна було легко перекладати та звести до ключової фрази, яку було б легко розповсюджувати.

Класифікація чуток здійснюється за трьома параметрами: експресивним (емоційні стани, виражені в змісті чутки, і відповідні типи емоційних реакцій), інформаційним (ступінь вірогідності сюжету чутки) і за ступенем впливу на психіку. За експресивною характеристикою виокремлюють чутки-бажання, чутки-залякування й агресивні чутки.

Розглянемо їх більш детально. Чутки-бажання – поширювана інформація має на меті викликати розчарування з приводу нездійснених очікувань і деморалізацію об'єкта впливу. Чутки-залякування – після поширенні в особистості ініціюється стан тривоги, невпевненості. Це можуть бути чутки про смертельну суперзброю, якою володіє супротивник (тобто сторона, що поширює чутки), чутки про недостачу продовольства, зараження місцевості, питної води тощо. Роз'єднувальні агресивні чутки – розповсюджувана інформація має на меті внести розлад у суспільство, порушити соціальні зв'язки.

За інформаційною характеристикою чутки поділяються на: абсолютно недостовірні, недостовірні, недостовірні з елементами правдоподібності, правдоподібні чутки. Чутки за своєю характеристикою є самопоширюваними. Їх природа базується на інформації, яку важко втримати. Особа обов'язково має розповісти про почуте комусь іншому. Достатньо створити відповідну чутку і запустити її в обіг у потрібному місці у слушний час – «людський гомін» зробить решту і цьому практично немає ефективних засобів протидії. На офіційному рівні зупинити чутки нереально – ці заходи викликають прямо протилежний ефект. Для людей, яких безпосередньо цікавлять чутки, це є підтвердженням правдивості останніх. Чим численніші намагання їх спростувати, тим більшою стає впевненість в їх достовірності. Єдиний можливий спосіб подолання ефективності чуток – їх цілковите ігнорування. Як правило, через деякий час напруження спадає, зайва активність в обговоренні вже неактуальних новин згасає, інтерес до порушеної в чутках проблеми зникає. Поява нових проблем повністю нейтралізує можливі небезпечні наслідки дезорганізації суспільства та держави[1].

В умовах російсько-української війни досить поширеними є чутки про ніби завдання ЗС України ударів по мирному населенню на тимчасово окупованих територіях. Мета – підтримувати населення у стані «фортеці в осаді», перемикання уваги з соціальних проблем на безпекові, які мають вищий пріоритет за пірамідою потреб Абрагама Маслоу.

8. Дестабілізація.

Дестабілізація – інструмент деструктивного інформаційного впливу спрямований на створення неналежного стану суспільно-політичної чи економічної ситуації в державі-жертві, загострення міжнаціональних, міжетнічних, міжконфесійних конфліктів тощо.

В умовах сьогодення вказаний інструмент реалізується, переважно, шляхом несанкціонованого втручання в сталу роботу офіційних веб-ресурсів органів державної влади та органів місцевого самоврядування[2], об'єктів критичної інфраструктури[3], правоохоронних органів[4]

[1] М Маркова, А Марков, Інформаційно-психологічна війна проти населення України як сучасна реальність: стан проблеми і шляхи подолання наслідків (2016) 2 *Інтегровані комунікації* 73–85 <http://nbuv.gov.ua/UJRN/ integcommu_2016_2_15> дата звернення 07.05.2021.

[2] Експерт розповів, як уникнути повторення кібератак на сайти держустанов <https://www.unian.ua/science/kiberataki-v-ukrajini-hakerski-ataki-na-derzhavni-sayti-novini-11158679.html> дата звернення 07.05.2021.

[3] Кібератака <https://www.ukrinform.ua/tag-kiberataka> дата звернення 07.05.2021.

[4] Масштабні хакерські атаки: невідомі зламали сайти нацполіції в кількох областях <https://www.5.ua/suspilstvo/masshtabni-khakerski-ataky-nevidomi-zlamaly-saity-natspolitsii-v-kilkokh-oblastiakh-224726.html> дата звернення 07.05.2021.

тощо, що призводить до спотворення процесу обробки інформації, її несанкціонованої маршрутизації та, можливо, використання в протиправних цілях (кіберзлочини1 та інші протиправні діяння спрямовані на шкоду державній безпеці України в інформаційній сфері).

На нашу думку, вказане вище обумовлено об'єктивними (відсутність належного фінансування, застарілість обладнання та програмного забезпечення тощо) і суб'єктивними чинниками (призначення на посади осіб, відповідальних за технічну безпеку, без досвіду роботи та належного фахового рівня, нехтування положеннями чинних нормативно-правових актів в інформаційній сфері тощо).

Одним із перших широковідомих прикладів сучасної реалізації інструментів деструктивних інформаційних впливів став так званий план «Шатун», який було спрямовано на дестабілізацію ситуації в Україні у період з 15 листопада 2016 до березня 2017 року. Його, за твердженнями хакерського угрупування «CyberHunta», виявлено у зламаній поштовій скрині В. Суркова, екс-помічника російського президента В. Путіна. Головна мета – дискредитація органів державної влади та проведення дострокових парламентських і президентських виборів.

Основні посили плану:

– залучення до масових акцій активістів окремих українських політичні партії («Опоблок», Всеукраїнське об'єднання «Батьківщина», Радикальна партія Олега Ляшка);

– «використання втемну» народних депутатів Мустафу Найєма, Сергія Лещенка, Світлану Заліщук та Ольгу Червакову для формування відповідної громадської думки;

– проникнення російських агентів в середовище волонтерів з метою інспірування панічних настроїв серед громадян;

– організація «Тарифного майдану» (Майдану-3);

– підготовка фінансової бази протестів в усіх обласних центрах України;

– активна критика соціально-економічної політики центральної та місцевої влади;

– проведення хресних ходів;

– активізація діяльності сепаратистських рухів у регіонах тощо[2].

Одразу після оприлюднення 24 жовтня 2016 року в мережі Інтернет сканів тексту плану серед населення розгорілася дискусія – це фейк чи реальність?

Одночасно необхідно зазначити, що зі слів керівництва Служби безпеки України та органів Національної поліції України – автентичність плану підтверджена в результаті проведення відповідних експертиз.

При цьому, відповідно до інформації, оприлюдненої 11 листопада 2016 року в ході спільного брифінгу представників СБ України та служби зовнішньої розвідки України,– «… масивна інформація, вилучена із поштової скриньки радника президента РФ Владислава Суркова, свідчить про початок здійснення так званого плану з дестабілізації суспільно-політичної ситуації в Україні під умовною назвою «Шатун». Безпосереднє керівництво і реалізацію цього плану здійснює відомий Службі безпеки України і Службі зовнішньої розвідки перший заступник Суркова – Ардзінба, а контакт із політичними рухами в нашій державі та окремими громадськими організаціями, задіяними в акціях протесту, як правило всліпу, або за фінансову винагороду, громадянин Вірменії – Мартиросян…»[3,4].

---

[1] М Погорецький, В Шеломенцев, Поняття кіберпростору як середовища вчинення злочинів (2009) 2 *Інформаційна безпека людини, суспільства, держави* 77–81; М А Погорецький, В П Шеломенцев, Кіберзлочини: до визначення поняття (2012) 8 *Вісник прокуратури* 89–96.

[2] Вікіпедія: План «Шатун» <https://uk.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D0%BD_%C2%AB%D0%A8%D0%B0%D1%82%D1%83%D0%BD%C2%BB> дата звернення 09.05.2021.

[3] Р Черниш, Дестабілізація суспільно-політичної ситуації в Україні спецслужбами Російської Федерації (на прикладі реалізації плану «Шатун») 12: Збірник тез за матеріалами IV Всеукраїнської науково-практичної конференції «Права людини: історичний вимір і сучасні тенденції» (м. Житомир, Літописець, 24–25 листопада 2016 року) (Житомир, ФОП Левковець, 2017) 22–24.

[4] Хто реалізує російський план по розвалу України «Шатун» <https://www.5.ua/suspilstvo/u-sbu-povidomyly-

Поряд з іншим, про автентичність плану (його проекту) може свідчити й достатньо професійний аналіз розвитку суспільно-політичних процесів в Україні та список запропонованих конкретних кроків спрямованих на їх подальшу дестабілізацію, а також те, що частина передбачених заходів (зокрема організація проплаченого «тарифного майдану») була реалізована в 20-х числах листопада 2016 року.

Вбачається, що в умовах сьогодення не доцільно дискутувати чи конкретний план «Шатун» був автентичним. Необхідно розуміти, що керівництво країни-агресора не полишає намірів із загарбання території України, і тому не важливо, як такі плани будуть називатися, а необхідно подбати про дієву систему протидії їм.

Висновки. Результати аналізу інструментів деструктивного інформаційного впливу, свідчать, що вони можуть використовуватися індивідуально і комплексно. Визначальними чинниками в процесі їх вибору стають саме індивідуальні особливості об'єкту впливу – людини або соціуму.

Залежно від глобальної мети деструктивного інформаційного впливу, його інструменти можуть бути спрямовані на: громадян у зоні конфлікту; громадян держави, щодо якої здійснюється інформаційна агресія, однак на території якої відсутній конфлікт; громадян країни-агресора; міжнародне співтовариство тощо.

На нашу думку, для реалізації зазначених інструментів деструктивного інформаційного впливу на сьогодні використовуються практично всі канали сучасної комунікації. Зважаючи на об'єм, предмет та мету даного дослідження значна кількість проблематичних питань щодо забезпечення державної безпеки України в інформаційній сфері залишилися поза увагою та будуть висвітлені в наступних публікаціях.

REFERENCES

BIBLIOGRAPHY

AUTHORED BOOKS

1. Kalinichenko B M, *Informatsiina viina: chynnyky eskalatsii i zasoby protydii* [Information War: Escalation Factors and Countermeasures] (Kyiv, 2020) 294 [in Ukrainian].

EDITED BOOKS

2. Barovska A (za zah. red.), *Informatsiini vyklyky hibrydnoi viiny: kontent, kanaly, mekhanizmy protydii: analit. Dop* [Informational challenges of hybrid warfare: content, channels, countermeasures: analyst. add.] (Kyiv, NISD, 2016) 109 [in Ukrainian].

ARTICLES

3. Chernysh R, Feik, yak odyn iz instrumentiv nehatyvnoho vplyvu na natsionalnu bezpeku Ukrainy v umovakh vedennia hibrydnoi viiny [Fake, as one of the tools of negative influence on the national security of Ukraine in the conditions of conducting a hybrid war] (2019) 2 *Chasopys kyivskoho universytetu prava* 109–114 <http://kul.kiev.ua/doc/chasopys2019/CHAS19_2.pdf> data zvernennia 07.05.2021 [in Ukrainian].

4. Chernysh R, Pravovyi dosvid krain Yevropeiskoho Soiuzu u sferi protydii poshyrenniu feikovoi informatsii [Legal experience of the countries of the European Union in the field of combating the spread of fake information] (2019) 10 *Pidpryiemnytstvo, hospodarstvo i pravo* 123–128 <http://pgp-journal.kiev.ua/archive/2019/10/22.pdf> data zvernennia 07.05.2021 [in Ukrainian].

5. Markova M, Markov A, Informatsiino-psykholohichna viina proty naselennia Ukrainy yak suchasna realnist: stan problemy i shliakhy podolannia naslidkiv [Information and psychological warfare against the population of Ukraine as a modern reality: the state of the problem and ways to overcome the consequences] (2016) 2 *Intehrovani komunikatsii* 73–85 <http://nbuv.gov.ua/UJRN/ integcommu_2016_2_15> data zvernennia 07.05.2021 [in Ukrainian].

khto-realizovuie-rosiiskyi-plan-po-razvalu-ukrayny-shatun-130830.html> дата звернення 10.05.2021.

6. Mudra I, Instrumenty informatsiinoi viiny proty Ukrainy v internet-ZMI [Tools of information warfare against Ukraine in the Internet media] (2017) 883 *Visnyk lvivskoi politekhniky «Zhurnalistski nauky»* 42–47 <https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/16124/mydrasinkova.pdf> data zvernennia 07.05.2021 [in Ukrainian].

7. Pohoretskyi M, Shelomentsev V, Poniattia kiberprostoru yak seredovyshcha vchynennia zlochyniv [Concept of cyberspace as an environment for committing crimes] (2009) 2 *Informatsiina bezpeka liudyny, suspilstva, derzhavy* 77–81 [in Ukrainian].

8. Pohoretskyi M A, Shelomentsev V P, Kiberzlochyny: do vyznachennia poniattia [Cybercrime: to the definition of the concept] (2012) 8 *Visnyk prokuratury* 89–96 [in Ukrainian].

9. Saienko O, Mekhanizm informatsiino-psykholohichnoho vplyvu v umovakh hibrydnoi viiny [Mechanism of informational and psychological influence in conditions of hybrid warfare] (2015) 1 Visnyk Natsionalnoi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy Seriia: Psykholohiia <http://nbuv.gov.ua/UJRN/Vnadpn_2015_1_11> data zvernennia 07.05.2021[in Ukrainian].

10. Semen N, Poniattia «informatsiina viina» v konteksti sotsialnykh komunikatsii [The Concept of «Information War» in the Context of Social Communications] (2016) 1 (25) Derzhava ta rehiony: Seriia: Sotsialni komunikatsii 22–25 [in Ukrainian].

CONFERENCE PAPERS

11. Chernysh R, Destabilizatsiia suspilno-politychnoi sytuatsii v Ukraini spetssluzhbamy Rosiiskoi Federatsii (na prykladi realizatsii planu «Shatun») [Destabilization of the socio-political situation in Ukraine by the special services of the Russian Federation (on the example of the implementation of the «Shatun» plan)] *Litopysets Vypusk* 12: Zbirnyk tez za materialamy IV Vseukrainskoi naukovo-praktychnoi konferentsii *«Prava liudyny: istorychnyi vymir i suchasni tendentsii»* (m. Zhytomyr. 24–25 lystopada 2016 roku) (Zhytomyr. FOP Levkovets, 2017) 22–24 [in Ukrainian].

WEBSITES

12. Ekspert rozpoviv, yak unyknuty povtorennia kiberatak na saity derzhustanov [The expert told how to avoid repeating cyberattacks on the websites of state institutions] <https://www.unian.ua/science/kiberataki-v-ukrajini-hakerski-ataki-na-derzhavni-sayti-novini-11158679.html> data zvernennia 07.05.2021 [in Ukrainian].

13. Fake news can lead to false memories <https://www.eurekalert.org/pub_releases/2019–08/afps-fnc081919.php> accessed 07.05.2021.

14. Khto realizuie rosiiskyi plan po rozvalu Ukrainy «Shatun» [Who implements the Russian plan for the collapse of Ukraine «Shatun»] <https://www.5.ua/suspilstvo/u-sbu-povidomyly-khto-realizovuie-rosiiskyi-plan-po-razvalu-ukrayny-shatun-130830.html> data zvernennia 10.05.2021 [in Ukrainian].

15. Kiberataka [Cyber attack] <https://www.ukrinform.ua/tag-kiberataka> data zvernennia 07.05.2021 [in Ukrainian].

16. Masshtabni khakerski ataky: nevidomi zlamaly saity natspolitsii v kilkokh oblastiakh <https://www.5.ua/suspilstvo/masshtabni-khakerski-ataky-nevidomi-zlamaly-saity-natspolitsii-v-kilkokh-oblastiakh-224726.html> data zvernennia 07.05.2021 [in Ukrainian].

17. Solohub I, Komu my doviriaiemo? [Who do we trust?] <https://voxukraine.org/komu-my-doviryayemo/> data zvernennia 07.05.2021 [in Ukrainian].

18. Ynformatsyonnaia y hybrydnaia voina [Information and hybrid warfare] <https://intellect.icu/informatsionnaya-i-gibridnaya-vojna-8758> data zvernennia 07.05.2021 [in Ukrainian].

19. Vikipediia: Plan «Shatun» [Wikipedia: «Shatun» Plan] <https://uk.wikipedia.org/wiki/% D0%9F%D0%BB%D0%B0%D0%BD_%C2%AB%D0%A8%D0%B0%D1%82%D1%83%D0%BD%C2%BB> data zvernennia 09.05.2021[in Ukrainian].

Chernysh R.,
Candidate of Law, Associate Professor,
National Academy of Security Service
of Ukraine
ORCID ID: *0000-0003-4176-7569*

DOI: *https://doi.org/10.17721/2413-5372.2021.1-2/156-165*

INSTRUMENTS OF DESTRUCTIVE INFLUENCE ON THE STATE SECURITY OF UKRAINE IN THE INFORMATION SPHERE

«Everyone wants to be informed honestly, impartially, truthfully -
and entirely in accordance with his views!»
Gilbert Chesterton

Annotation. *The article states that the latest information and communication technologies have significantly increased the dependence of each individual and society as a whole on the reliability and validity of the information used. These technologies have recently been actively used not only as a real social resource for human adaptation to life, but also as a means of manipulating consciousness. The tools and methods of information management of people are being scientifically substantiated and are becoming widespread. In the process of constant expansion of the information component, the percentage of solving everyday practical problems due to specialized information obtained from mass media and communication is constantly increasing. The consciousness of man and society is increasingly subordinated to the ideas promoted by mass media. And this, in turn, makes a person open and defenseless against manipulative technologies.*

Taking into account the above, ***the purpose of the article*** *is to study the instruments of destructive influence on the state security of Ukraine in the information sphere.*

It is claimed that, taking into account the significant consolidation of the Ukrainian people, as well as the significant strengthening of the defense potential of our state, representatives of the special services of the russian federation are resorting to new forms and methods of war – the transition from open armed confrontation in the east and south to efforts to shake the socio-political situation from within Ukraine, including through destructive information influence.

It is noted that currently most scientists do not classify the tools of destructive information influence as a separate institution. The indicated problems are considered through the prism of the analysis of the tools of the Russian information war.

In the final part, it is stated that the results of the analysis of the tools of destructive information influence show that they can be used individually and comprehensively. The determining factors in the process of their selection are precisely the individual characteristics of the object of influence – a person or society. Depending on the global goal of destructive information influence, its tools can be aimed at: citizens in the conflict zone; citizens of the state against which informational aggression is being carried out, but on whose territory, there is no conflict; citizens of the aggressor country; the international community, etc. Today, almost all channels of modern communication are used to implement tools of destructive informational influence.

Key words: *state security of Ukraine in the information sphere, destructive information influence, tools of destructive information influence, destabilization, fake.*