

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет права, публічного
управління та національної безпеки
Кафедра правознавства

Кваліфікаційна робота
на правах рукопису

ОСІЧНЮК ЛЮДМИЛА ІВАНІВНА

УДК 347.78 (477)

КВАЛІФІКАЦІЙНА РОБОТА

**Правові та організаційні основи протидії
деструктивному інформаційному впливу в Україні:
шляхи удосконалення**

081 «Право»

Подається на здобуття освітнього ступеня «Магістр»

кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Осічнюк Л.І.

Керівник роботи
Черниш Роман Федорович
кандидат юридичних наук,
доцент

Висновок кафедри правознавства за результатами попереднього захисту:
до захисту допущено

Протокол засідання кафедри правознавства № __ від « __ » грудня 2021 р.

Завідувач кафедри правознавства

к.ю.н., доцент

Р. Д. ЛЯШЕНКО

(підпис)

«__» _____ 2021 р.

Результати захисту випускної кваліфікаційної роботи

Здобувачка вищої освіти Осічнюк Людмила Іванівна
захистила кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою _____

за шкалою ECTS _____

за національною шкалою _____

Секретар ЕК

(підпис)

Т.П. СВЯТОГОР

АНОТАЦІЯ

Осічнюк Л.І. Правові та організаційні основи протидії деструктивному інформаційному впливу в Україні: шляхи удосконалення. Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістра за спеціальністю 081 Право. Поліський національний університет, Житомир, 2021.

У кваліфікаційній роботі досліджено правові та організаційні основи протидії деструктивному інформаційному впливу в Україні. Розглянуто підходи до розуміння поняття «дезінформація». Охарактеризовано критерії оцінки дезінформації. Розглянуто міжнародний досвід протидії деструктивному інформаційному впливу. Проаналізовано нормативно-правові акти, що забороняють поширення інформації шкідливого змісту. Охарактеризовано державну політику з протидії шкідливому інформаційному впливу. Зосереджено увагу на роботі органів державної влади, які створені для протидії поширенню дезінформації і пропаганди. Проаналізовано стратегії держави з протидії шкідливому інформаційному впливу.

Ключові слова: шкідливий інформаційний вплив, дезінформація, мізінформація, пропаганда, національна безпека, національні інтереси.

SUMMARY

Osichnyuk L.I. Legal and organizational bases of counteraction to destructive information influence in Ukraine: ways of improvement. Manuscript qualification work.

Qualifying work for a master's degree in specialty 081 Law. Polissya National University, Zhytomyr, 2021.

In the qualification work the legal and organizational bases of counteraction to destructive information influence in Ukraine are investigated. Approaches to understanding the concept of "disinformation" are considered. Criteria for assessing disinformation are described. The international experience of counteracting destructive information influence is considered. The normative legal acts prohibiting the dissemination of information of harmful content are analyzed. The state policy on counteraction to harmful information influence is characterized. The focus is on the work of public authorities created to counter the spread of disinformation and propaganda. The strategies of the state on counteraction to harmful information influence are analyzed.

Key words: harmful information impact, disinformation, misinformation, propaganda, national security, national interests.

ЗМІСТ

ВСТУП	6
РОЗДІЛ 1. ДЕЗІНФОРМАЦІЯ ЯК ОСНОВНИЙ ЕЛЕМЕНТ ШКІДЛИВОГО ІНФОРМАЦІЙНОГО ВПЛИВУ СУЧАСНОСТІ	9
1.1 Розуміння категорії «дезінформація»	9
1.2. Критерії оцінки дезінформації	12
ВИСНОВКИ ДО РОЗДІЛУ 1	20
РОЗДІЛ 2. МІЖНАРОДНИЙ ДОСВІД БОРОТЬБИ З ДЕСТРУКТИВНИМ ІНФОРМАЦІЙНИМ ВПЛИВОМ	21
2.1. Ініціативи міжнародних організацій у протидії дезінформаційному впливу	21
2.2. Правова та організаційна практики протидії дезінформації в інших країнах	24
ВИСНОВКИ ДО РОЗДІЛУ 2	31
РОЗДІЛ 3. ПРОТИДІЯ ДЕСТРУКТИВНОМУ ІНФОРМАЦІЙНОМУ ВПЛИВУ В УКРАЇНІ	32
3.1. Нормативно-правове регулювання	32
3.2. Державні інституції в боротьбі з дезінформацією	37
3.3. Стратегічний підхід в протидії шкідливому інформаційному впливу	40
ВИСНОВКИ ДО РОЗДІЛУ 3	45
ВИСНОВКИ	46
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	49

ВСТУП

Актуальність теми дослідження. Україна як і все демократичне суспільство нині стикнулася з рядом викликів, які спричинені шкідливим інформаційним впливом, а саме: ускладнення критичного сприйняття інформаційного потоку населенням, зростання недовіри до офіційних новин та медіа, значне зниження довіри до демократичних інститутів. Одночасно такий вплив варто розглядати як частину більш складної проблеми, пов'язаної з операціями впливу на свідомість через маніпуляції громадською думкою. Таке втручання може мати іноземне та внутрішнє походження і має на меті вплинути на громадян в умовах демократії, фактично позбавивши їх свободи вибору [1].

Дана проблема особливо актуалізувалася у 2014 році з анексією Криму та окупаційних процесів на Півдні України. Цілеспрямований дезінформаційний вплив, який супроводжує збройну агресію Російської Федерації в рамках її «гібридної» війни проти України, став першочерговою загрозою для нашої держави. Російські дезінформаційні та пропагандистські операції, які проводяться їх спецслужбами в інформаційному просторі України, мають на меті зміцнити власні позиції серед українців шляхом викривленого уявлення про реальність, тиску на державні інституції, поляризації суспільства тощо. У симбіозі з класичною збройною агресією такий шкідливий інформаційний вплив становить пряму загрозу конституційному устрою, суверенітету та територіальній цілісності України.

Українська влада розпочала адаптацію інформаційного законодавства до вказаних викликів. В цьому процесі важливо розробити і впровадити цілісну концепцію протидії шкідливому інформаційному впливу, взявши за основу позитивний досвід інших країн та враховуючи українські реалії.

Питання, пов'язані з темою дослідження, опрацьовувались в роботах вітчизняних науковців, серед яких, В. Богуш, М. Биченок, В. Горбулін, А. Марущак, М. Ожеван, Д. Олейніков, В. Остроухов, В. Петрик, М. Присяжнюк, І. Руснак, М. Слюсаревський, В. Телелим, Т. Ткачук, В. Толубко, В. Цимбалюк, Р. Черниш, О. Юдін та ін.

Мета та завдання дослідження. Метою дослідження є аналіз правових та організаційних основ протидії деструктивному інформаційному впливу в Україні.

Відповідно до поставленої мети, завданнями кваліфікаційної роботи є:

- визначити поняття та зміст дезінформації;
- охарактеризувати критерії оцінки дезінформації;
- розглянути міжнародний досвід протидії деструктивному інформаційному впливу;
- проаналізувати нормативно-правове регулювання шкідливого інформаційного впливу в Україні;
- з'ясувати роль державних інституцій в боротьбі з дезінформацією;
- оцінити стратегічні підходи до боротьби з деструктивним інформаційним впливом в Україні.

Об'єктом дослідження є деструктивний інформаційний вплив як явище правової дійсності.

Предметом дослідження є правові та організаційні основи протидії деструктивному інформаційному впливу в Україні.

Методи дослідження. Відповідно до мети роботи, в процесі наукового дослідження було використано низку наукових методів сучасної гносеології. Методологічну основу дослідження склала теорія пізнання правових явищ як концептуальних положень, що були розроблені видатними фахівцями у сфері інформаційного права. Крім того, застосовано спеціальні методи наукового дослідження, зокрема: порівняльний - для співставлення положень чинного українського законодавства у сфері забезпечення інформаційної безпеки та нормативно-правових актів країн Європейського Союзу; спеціальний юридичний - для ґрунтовного аналізу нормативно-правових актів, які регламентують процедуру протидії деструктивному інформаційному впливу; системний підхід та логіко-правовий метод - для аналізу впливу негативних чинників на складові елементи досліджуваного явища та формування логічних і конкретних теоретико-прикладних висновків.

Практичне значення одержаних результатів полягає у їх використанні в навчальному процесі під час викладання основ національної безпеки, інформаційного права та ін., а також у правотворчій, інтерпретаційній та правозастосовній діяльності.

Апробація результатів дослідження. Окремі результати та висновки, отримані в ході проведеного дослідження, були викладені в науковій фаховій статті у виданні, що індексується в Google Scholar, у міжнародних реферативних базах даних «EBSCO Publisher» (США), «WorldCat» (США), «Directory of Open Access Scholarly Resources» (США), «Directory of Open Access Journals» (DOAJ) (Швеція), «Information Matrix for the Analysis of Journals» (Іспанія), «Index Copernicus International» (Польща), «Bielefeld Academic Search Engine» (Німеччина); має повнотекстові мережеві версії в Інтернеті на платформах Національної бібліотеки України імені В.І. Вернадського, «Наукова періодика України», «Central and Eastern European Online Library» (Німеччина), «Worldwide Scientific and Educational Library» (США), Республіканської Міжвузівської Електронної Бібліотеки (Казахстан) та ін. Наразі редколегія провадить роботу щодо входження збірника у Scopus та Web of Science (Черниш Р.Ф., Осічнюк Л.І. Національні інтереси держави та можливість обмеження права на свободу слова: питання співвідношення. *Проблеми законності*. 155. 2021. с. 77-89).

Структура та обсяг роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, семи підрозділів, висновків та списку використаних джерел (79 найменувань).

РОЗДІЛ 1. ДЕЗІНФОРМАЦІЯ ЯК ОСНОВНИЙ ЕЛЕМЕНТ ШКІДЛИВОГО ІНФОРМАЦІЙНОГО ВПЛИВУ СУЧАСНОСТІ

1.1. Розуміння категорії «дезінформація»

Одним з перших кроків у протидії шкідливому інформаційному впливу повинно бути вироблення єдиного підходу в розумінні понятійно-категорійного апарату, який описує вказану діяльність, а в результаті законодавче закріплення відповідних термінів та розробка дієвих механізмів захисту.

Останні п'ять років медійний простір заповнили поняття дезінформація, мізінформація, фейк, постправа та інші. Переважна більшість громадськості, політиків і представників засобів масової інформації використовують ці терміни як синоніми, хоч інтуїтивно відчувається наявність відмінностей, і асоціюють їх з брехнею і неправдою. У 2017 році колишній президент Сполучених Штатів Дональд Трамп популяризував термін «fake news» («фальшиві новини») і упорядники авторитетного словника Collins назвали дане словосполучення «Словом року», так як його використання у світових ЗМІ збільшилось на 365% [2]. Сьогодні нерідко дезінформацію прирівнюють до «fake news», визначаючи її лише як неправдиві новини, проте це значно ширше і складніше поняття, адже не лише фейкові, а і правдиві новини можуть бути використані з шкідливою метою.

Варто зазначити, що термін «дезінформація» не є новим. Американське видання Merriam-Webster датує його появу 30-ми роками ХХ століття і визнає його російське походження, а також визначає дезінформацію як неправдиву інформацію, яка навмисно і часто приховано поширюється (наприклад, шляхом підкидання чуток) з метою впливу на громадську думку або приховування правди [3]. Американський історик Герберт Ромерштейн зазначає, що КДБ почало застосовувати дезінформацію як зброю в 1923 році, коли було створено спеціальне бюро з ведення активної розвідки - дезінформації супротивника. Активно даний термін використовувався КДБ під час Холодної війни. У 1960-ті роки операціями з дезінформування займався відділ «Д» КДБ, який в 1970р. був збільшений і перетворений на «Директорат А» [4].

Розвідник, генерал КДБ Євген Примаков роз'яснював, що на різних етапах розвідувальної роботи операції з дезінформації спецслужб супротивників радянської влади мали кілька суто службових позначень: «акції впливу», «оперативна дезінформація», «активні заходи», «оперативні ігри», «заходи сприяння», тощо. Попри різницю в термінах, всі вони були і є певними цілеспрямованими діями для введення в оману фактичного або потенційного супротивника відносно своїх справжніх намірів або можливостей, а також для отримання вигідної, практично недосяжної відкритими способами реакції «об'єкта впливу» [5, с. 13].

Цілком таємний Контррозвідувальний словник 1972 року визначав дезінформаційні відомості як спеціально підготовлені відомості для створення у супротивника невірного уявлення про дійсність, на основі якої він може ухвалювати рішення, вигідні стороні, що дезінформує (для зручності дезінформація) [6, с. 79].

Колишній румунський генерал розвідки Іон Міхай Пачепа зазначав, що Йосип Сталін винайшов таємну «науку» дезінформації, давши їй ім'я, яке звучить на французький манер, і зробив вигляд, що це відноситься до брудної практики Заходу [7]. На підтримку такої парадигми працювала і наукова спільнота. Так, наприклад, професор Ясен Засурський у своїй праці «Техніка дезінформації і обману» створює образ маніпулятивної буржуазної преси, яка нехтує об'єктивністю з метою захисту капіталізму [8]. Разом з тим, науковець детально описує методи та способи дезінформації, які актуальні навіть у ХХІ столітті. Отримавши у спадок досвід декількох десятиліть активного застосування дезінформаційних операцій, Російська Федерація тримає світове лідерство у цій діяльності, а тому змушує міжнародне співтовариство вивчати «науку» Сталіна. Виходячи з того, що Росія, як один з найбільших поширювачів дезінформації, використовує її проти інших країн в контексті спланованої діяльності спецслужб з чітко визначеною метою, то вбачається помилковим синонімізувати дану категорію виключно з неправдивою інформацією.

Кембриджський словник дезінформацію визначає як неправдиву інформацією, яка поширюється з метою введення в оману людей [9]. В даному трактуванні акцент зроблено на меті поширення інформації. Подібний підхід простежується в декількох міжнародних джерелах. Кодекс практики ЄС щодо протидії дезінформації не дає чіткого визначення, але вказує, що дезінформація має на меті економічні вигоди для того, хто її поширює [10]. Представники ООН, ОБСЄ та інших організацій у спільній декларації про свободу вираження думки, “фейкові новини”, дезінформацію і пропаганду вказали, що найчастіше дезінформація спрямована на обман людей і перешкоджання знати, отримувати, шукати, поширювати інформацію [11]. Спеціальний доповідач із заохочення і захисту права на свободу думок і їхнє вільне вираження (ООН) у доповіді від 13 квітня 2021 року, наголосивши на існуванні плутанини в термінах, узагальнив поняття дезінформації назвав як брехливої інформації, яка навмисно поширюється з метою заподіяння серйозної соціальної шкоди [12].

Варто чітко розуміти різницю між дезінформацією та неправдивою інформацією. Неправильні дані можуть поширюватися через необізнаність автора, через неуважність, тобто поширювач такої інформації переконаний в її достовірності. Для її позначення останнім часом часто використовують термін «мізінформація» - некоректна або оманлива інформація, що розповсюджується без мети когось обманути [13]. В той час як поширення дезінформації – це цілеспрямована діяльність з конкретно визначеною метою. Отже, принциповою ознакою дезінформації, яка відрізняє дану категорію від звичайної недостовірної інформації, є умисел на її створення та поширення.

Заслуговує на увагу, на нашу думку, позиція науковиці Мар'яни Кіци, котра визначає дезінформацію як спосіб психологічного впливу, що полягає в намірі подання об'єктові такої інформації, яка вводить його в оману стосовно справжнього стану справ та створює викривлену реальність [14]. Такий підхід зосереджує увагу на когнітивній здатності індивіда, а тому доречний в контексті протидії дезінформації на рівні особистісному рівні (підвищення

медіаграмотності та інше), проте є недоречним в процесі нормативно-правового регулювання.

В Україні відсутнє нормативне закріплення поняття дезінформації. Варто звернути увагу, що вітчизняні законотворці робили спробу ввести дану категорію в правове поле. У 2020 році Міністерство культури, молоді та спорту України презентувало законопроект «Про протидію дезінформації». У вказаному документі дезінформація визначалася як недостовірна інформація з питань, що становлять суспільний інтерес, зокрема стосовно національної безпеки, територіальної цілісності, суверенітету, обороноздатності України, права українського народу на самовизначення, життя та здоров'я громадян, стану довкілля [15]. Таке визначення дезінформації, на нашу думку, є абсолютно недопустимим, оскільки не описує природу цього явища, а зводиться лише до факту достовірності і тематики. Разом з тим факт достовірності не є критерієм ідентифікації дезінформації, оскільки нею може бути правдива інформація, поміщена в спеціальний контекст.

1.2. Критерії оцінки дезінформації

Одним з дискусійних питань в протидії шкідливому інформаційному впливу є криміналізація дезінформації. Генеральний секретар Європейської федерації журналістів Рікардо Гутьєррес зазначив, що цей спосіб боротися з дезінформацією є хибним і суперечить європейським стандартам свободи слова [16]. Не дивно, що жодна країна Європи не вдалася до такого методу боротьби з дезінформацією. На сьогодні лише у декількох країнах існує кримінальна відповідальність за поширення дезінформації, серед них Китай, Сінгапур, Білорусь та декілька африканських країн. На нашу думку, в Україні повинна існувати юридична відповідальність за поширення дезінформації. Така необхідність пов'язана з наявністю агресивного сусіда на сході нашої держави та підвищеним інтересом Російської Федерації до суспільно-політичного становища в Україні. Разом з тим, варто розробити чітку систему оцінки дезінформації, яка забезпечить пропорційність шкоди та покарання, а

відповідно, кримінальна відповідальність повинна наставати у виключних найтяжчих випадках.

Вбачається доцільним розділяти дезінформацію на такі типи:

- дезінформація, яка є кримінальним правопорушенням;
- дезінформація, яка не тягне за собою кримінального покарання, але може спричинити цивільний позов або адміністративні санкції;
- дезінформація, яка обґрунтовано не може спричинити будь-яку з цих санкцій, проте все ж викликає занепокоєння щодо шкідливого впливу на суспільно важливі сфери життя.

Аналізуючи природу дезінформації з метою її типізації, необхідно виокремити відповідні критерії. Це дозволить чітко визначати рівень впливу дезінформації та ступінь шкоди в залежності від мети її поширення. На нашу думку, до таких критеріїв варто віднести зміст дезінформації, контекст, місце поширення, форму та спосіб поширення, суб'єкт поширення.

Зміст дезінформації може бути повністю вигаданим або базуватися на реальних фактах, якими маніпулюють або перекручують. Повністю фейкові повідомлення характеризуються короткочасною дією та гучним просуванням. В іншому випадку дія дезінформації триваліша, а ефект сильніший. Найвідомішим прикладом дезінформації, заснованої на цілковитій брехні, є створена російськими пропагандистами новина про розіп'ятого хлопчика в Слов'янську. Хоч даний фейк швидко розвінчали, проте він підсилив образ «жорстокого ворога». Такий прийом прийнято називати технологією розлюднення, вона неодноразово застосовувалася під час бойових дій. Так, під час Першої світової війни у 1915 році з'явилася історія про те, що німецькі солдати вибрали з групи полонених молодого канадського солдата та розіп'яли на дверях комори. Пізніше підтвердилася її неправдивість [17].

Маніпуляція правдою в контексті дезінформації може здійснюватися шляхом хибної аргументації фактів, перекручування інформації, виривання з контексту, неповного викладу тощо.

При оцінці дезінформації важливо брати до уваги статус і публічність особи, яка її поширює. Так, у Рішенні ЄСПЛ у справі Савва Терентьев проти Росії (*Savva Terentyev v. Russia*, №10692/09) від 24 серпня 2018, яка стосувалася засудження заявника за розпалювання ненависті після публікації образ щодо співробітників поліції в коментарях до блогу, Суд звернув увагу на малий рівень зацікавленості громадськості до вказаного допису [18]. Це означає, що при оцінці шкоди від дезінформації суди повинні враховувати рівень поширення відповідного контенту.

Вплив статусу поширювача фейку на ефект від дезінформації наглядно демонструє ситуація, коли у 2021 році Twitter заблокував обліковий запис президента США Дональда Трампа через поширення дезінформації, оскільки приблизно 30% його найпопулярніших дописів містили фейки про вибори у Штатах. В сумі ці пости поширювались близько 4 млн. разів, а відреагували на них лайками більше 22 млн. користувачів [19].

Важливим фактором дієвості і сприйняття дезінформації є контекст, в який вона поміщена. Варто звернути увагу, що вагомість контексту визнає і ЄСПЛ. Так, у справі Дмитрієвський проти Росії від 03.10.2017р. при оцінці висловлювань, Суд наголосив на необхідності оцінки таких факторів як соціальні та політичні обставини, мова ворожнечі (манера, в якій були подані висловлювання), вплив (прямий і непрямий). Проте, Суд має індивідуальний підхід до розгляду кожної справи з цього питання, ретельно вивчаючи взаємодію всіх означених вище факторів [20].

Неприятнь найкраще розпалюється тоді, коли між сторонами існують суперечки і конфлікти, фейки про військових актуальніші на територіях бойових дій тощо. Отже контекст включає в себе «чутливе» середовище, період поширення інформації, передбачувану реакцію на неї. Прикладом такого чутливого середовища є пандемія коронавірусної інфекції, в умовах якої дезінформаційні повідомлення про вакцинацію дуже швидко поширюються і призводять до цілком реальних наслідків у вигляді протестних акцій, низького рівня імунізації, високої смертності тощо. Таким чином, дезінформація, яка

поміщена в сприятливий контекст стає особливо небезпечною, породжуючи агресію, міжнаціональну та міжетнічну ненависть, може вплинути на вибори та інші важливі суспільно-політичні процеси.

Місця поширення дезінформації є аналогічними звичайній інформації (друковані матеріали, телебачення, радіо, інтернет), проте мають свої особливості. Друковані матеріали сьогодні не є домінуючим джерелом розповсюдження дезінформації, проте їх роль як засобу агітації зростає під час виборчого процесу. Вони легко поширюються серед окремих груп населення, особливо малозабезпечених, оскільки роздаються безкоштовно в місцях масового скупчення людей.

Вплив радіо на поширення деструктивного інформаційного впливу в Україні є мінімальним, оскільки його популярність стрімко падає. Разом з тим на 2019 рік за даними Європейського мовного союзу радіо залишається тим засобом масової інформації, якому європейці довіряють найбільше [21]. Найбільш вагому роль радіо, як місце поширення дезінформації, відіграє в країнах з низьким рівнем розвитку, де громадяни не можуть собі дозволити використання телебачення або інтернету. Відповідно в таких країнах радіо стає єдиним доступним джерелом інформації, наприклад країни Африки.

Дієвим майданчиком для поширення дезінформації є телебачення. В Україні за даними щорічного опитування USAID-Internews на 2020 рік 41% населення довіряє телебаченню [22], а в Європі – 49% (за інформацією Європейського мовного союзу на 2019р.) [21]. Тому ТБ може становити серйозну загрозу в сфері здійснення шкідливого інформаційного впливу. Європейською конвенцією про транскордонне телебачення передбачено, що телемовник забезпечує об'єктивне висвітлення фактів і подій та сприяє вільному формуванню думок [23], що можна вважати правовим запобіжником від поширення дезінформаційного контенту.

В Україні ризики здійснення шкідливого інформаційного впливу через телебачення зростають у зв'язку з тим, що найпопулярніші канали належать олігархам. Відповідно останні мають інструмент маніпулювання громадською

думкою, який вони можуть використовувати з політичною або економічною метою.

Найпопулярнішим місцем отримання інформації в Україні є Інтернет, а саме соціальні мережі. В підсумках опитування USAID-Internews за 2020 рік зазначається, що 62% респондентів отримують інформацію із соцмереж, 48% — з сайтів новин [22]. Соцмережі - це зручна платформа для поширення дезінформації, оскільки вигідний агентам впливу контент за відсутності редакційного контролю створюється легко і безкоштовно, а поширюється миттєво і стає вірусним. Наприклад, 44% (приблизно 90 мільйонів) американців визнали, що під час президентських виборів 2020 року помічали дезінформацію у Facebook, а 35% повірили їй [24].

Варто звернути увагу на те, що у 2020 році в Україні спостерігалась тенденція до зменшення споживання новин із усіх джерел, оскільки аудиторія відчувала перенасиченість негативною інформацією [22]. Це свідчить, на нашу думку, не так про погіршення соціально-економічної ситуації в державі (хоч і це ми не заперечуємо), як про багатократне зростання об'ємів шкідливого інформаційного впливу ззовні.

На сприйняття дезінформації впливають форми та способи її поширення. Неправдива або маніпулятивна інформація може бути представлена у текстовій, аудіо або відеоформах. Дезінформація у формі тексту легко створюється, швидко поширюється, адже більшість публікацій в інтернет-виданнях, соціальних мережах є текстовими. Відеоформа дезінформації розвивалася на телебаченні, а з появою Інтернету та соціальних мереж (відеоблогінг) стала доступнішою. Контент в аудіоформі використовується в усному мовленні, ораторському мистецтві, на радіо тощо. Дана форма дезінформації була досить успішною у нацистській Німеччині через ораторські здібності Адольфа Гітлера. Люди можуть поширювати дезінформаційні повідомлення у повсякденному житті у вигляді чуток від сусідів, колег, пасажирів у транспорті.

Одним з останніх варіантів аудіовізуальної форми дезінформації є «дівфейки». Це підроблені матеріали, які створюються з використанням

штучного інтелекту. Заміна візуального і звукового контенту створює ілюзію реальності. За допомогою дідфейків можна дискредитувати публічних осіб, приписувати людям не їхні слова, вчиняти шантаж та інше. У січні 2020 року під час передвиборчої кампанії в США Facebook заборонив на своїй платформі маніпуляцію дідфейками. В компанії заявили, що будуть видаляти контент, який відредагований такими способами, який не є очевидними для пересічної людини і, ймовірно, введе когось в оману, та створений за допомогою алгоритмів штучного інтелекту або машинного навчання [25].

Сьогодні в жодній країні світу нема усталеного законодавства і практики протидії дідфейкам. В грудні 2018 року в Конгресі США був представлений законопроект, який встановлює нове кримінальне правопорушення, пов'язане зі створенням або розповсюдженням підроблених аудіовізуальних матеріалів, які виглядають реалістичними. У проекті «deep fake» визначається як аудіовізуальний запис, створений або змінений таким чином, що спостерігач його може вважати автентичною поведінкою особи. Законопроект криміналізує використання дідфейків у порно та з метою шахрайства, проте містить виняток: особа не може притягатись до відповідальності, якщо діє в рамках Першої поправки Конституції США (право на свободу вираження) [26].

Зазначимо, що законодавство штату Нью-Йорк для регламентації такої діяльності використовує термін «digital replica» – цифрова копія, а не «deep fake». І розглядає його в контексті захисту права на приватність. Законом заборонено використовувати чуже обличчя без згоди з метою торгівлі [27]. Важливо також визначати не лише явища, а й цільові групи, на які направлене законодавство. Це, в першу чергу, стосується аспектів кримінальної відповідальності. Наприклад, у вказаному вище законопроекті Конгресу США увага концентрується на двох групах: автори підробок, якщо вони діють з незаконним умислом, та поширювачі (ЗМІ, соціальні мережі) [27].

Розуміючи, що «deep fakes» має значний вплив на соціально вагомій сфері, а особливо на виборчий процес, законотворці штату Каліфорнія активно розробляють поправки до цивільного процесуального та виборчого

законодавства, які стосуються заборони використання «суттєво оманливих аудіо чи візуальних носіїв інформації», а такими визнаються зображення або аудіо- чи відеозапис зовнішності, мови чи поведінки кандидата, які були навмисно змінені таким чином, щоб зображення чи аудіо- чи відеозапис неправдиво видавалися розумній особі автентичними і підштовхували особу до принципово іншого розуміння або враження поданого змісту зображення чи аудіо- чи відеозапису, ніж це було б, якби людина почула або побачила незмінну оригінальну версію цього зображення або аудіо- чи відеозапису [28].

Очевидно, що сьогодні уважний користувач може розпізнати дідфейк самостійно: помічати мерехтіння обличчя, погану синхронізацію звуків і рухів губ, невідповідне анатомії моргання тощо. Проте, з розвитком штучного інтелекту якість дідфейків зростатиме, що становить серйозну загрозу в контексті дезінформаційного впливу.

Розглядаючи способи поширення дезінформації, можемо відмітити, що найдієвішими в умовах сучасності є таргетовані повідомлення та контрольована не автентична поведінка. Таргетовані повідомлення працюють завдяки збору інформації про особу в Інтернеті з відкритих джерел. Спеціальне програмне забезпечення збирає дані про підписки в соціальних мережах, коментарі, «лайки», в результаті чого можна визначити цільову аудиторію для просування контенту певної тематики. Разом з тим, такі алгоритми породжують правову дискусію в контексті захисту персональних даних. У рішенні Суду Європейського Союзу (справа С-673/17) від 01.10.2019 року вказується, що згода користувача на використання сайтом файлів “cookies” (один з способів відслідковувати поведінку користувача) повинна бути свідомою і явною. Інтернет-ресурси зобов’язані надавати користувачам інформацію про доступ до вказаних файлів третіх сторін та про термін зберігання даних про користувача [29].

Одним з популярних способів є контрольована не автентична поведінка, яка зводиться до створення багатьох фейкових акаунтів, які залучають максимальну кількість користувачів і одночасно поширюють однакові

наративи, посилаючись один на одного чи на спільне джерело. Часто такі фейкові акаунти маскуються під медіа або інші публічні сторінки та використовуються для маніпулювання у сфері суспільно важливих тем. Метою такої діяльності є створення інформаційної завіси, в якій користувач відповідної мережі отримує тільки те, що вигідно поширювачам дезінформаційних повідомлень, а інформація з інших джерел туди не потрапляє.

Найбільші соціальні мережі здійснюють діяльність по відстеженню контрольованої не автентичної поведінки та блокують її. Так, Facebook щомісяця публікує звіти з цього напрямку діяльності. Наприклад, в травні 2021 року було припинено діяльність мережі з Росії та Судану, яка була націлена на поширення дезінформації серед громадян Судану. В результаті було видалено 83 облікові записи Facebook, 30 сторінок, 6 груп і 49 облікових записів Instagram, якими керували жителі Судану від імені фізичних осіб у Росії. Внутрішнє розслідування соціальної мережі виявило певний зв'язок із мережею, яка була видалена в жовтні 2019 року, і Facebook пов'язав цю активність з діяльністю Російського агентства інтернет-досліджень [30].

ВИСНОВКИ ДО РОЗДІЛУ 1

Дезінформація, як десятиліттями напрацьована російськими спецслужбами зброя в інформаційній площині, становить серйозну загрозу демократичному суспільству та національній безпеці України зокрема, а тому потребує детального вивчення з метою розробки стратегії ефективної протидії та притягнення до відповідальності винних в її поширенні осіб.

Як і з будь-яким іншим поняттям, у питанні трактування терміну «дезінформація» існує багато невизначеностей, а наукова спільнота і український законодавець досі не знайшла консенсусу. Різноманіття думок ускладнює боротьбу з цим явищем, оскільки без єдиного визначення неможливо узаконити правовий механізм протидії дезінформації, який не перетворився б на інструмент цензури.

Вбачається неправильним асоціювати дезінформацію виключно з брехнею, неправдивою інформацією чи фейковими новинами. Розуміння даної категорії повинно ґрунтуватися на її основній особливості – наявності умислу на створення і поширення.

Вважаємо доцільним **дезінформацію** визначати як відомості неправдивого та/або маніпулятивного характеру, які цілеспрямовано поширюються з метою впливу на важливу суспільну сферу шляхом формування необхідної громадсько-політичної думки.

На нашу думку, особливо небезпечні епізоди систематичного поширення дезінформації повинні тягнути за собою кримінальну відповідальність, але лише як крайня міра покарання у виключних випадках. Разом з тим, для оцінки ступеню нанесеної дезінформацією шкоди варто брати до уваги такі критерії як її зміст, контекст, в який вона поміщається, суб'єкт поширення, місце, форма та спосіб поширення.

РОЗДІЛ 2. МІЖНАРОДНИЙ ДОСВІД БОРОТЬБИ З ДЕСТРУКТИВНИМ ІНФОРМАЦІЙНИМ ВПЛИВОМ

2.1. Ініціативи міжнародних організацій у протидії дезінформаційному впливу

Протягом останніх років міжнародною спільнотою прийнято декілька ключових документів та стандартів у сфері протидії дезінформації. Так, на початку квітня 2016 Єврокомісія ухвалила «Спільні принципи протидії гібридним загрозам — відповідь Європейського Союзу». В документі наголошується в тому числі і на необхідності вироблення державами-членами узгоджених механізмів реалізації стратегічних комунікацій для протидії дезінформації та публічного викриття гібридних загроз. Також зазначається, що провокатори можуть систематично поширювати дезінформацію, у тому числі в межах цілеспрямованих акцій у соціальних мережах з метою радикалізації окремих осіб та дестабілізації суспільства. Вказується, що Служби зовнішніх зв'язків ЄС повинні забезпечити цілеспрямовану комунікацію для реагування на дезінформацію [31].

У листопаді 2016 Європейський парламент прийняв Резолюцію «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін». Документ складається з таких розділів: стратегічні комунікації ЄС у контексті протидії пропаганді; викриття російської дезінформації та пропаганди; боротьба з інформаційними війнами ІДІЛ, дезінформацією та радикалізацією; стратегія ЄС з протидії пропаганді. Дезінформація та пропаганда в Резолюції визнаються складовими частинами гібридної війни. Європарламент закликає інституції ЄС проводити моніторинг джерел фінансування антиєвропейської пропаганди, збільшити видатки на підтримку свободи ЗМІ у країнах-сусідах ЄС, наголошує на необхідності зміни характеру «позитивних» меседжів ЄС з обороняючих на наступальні, а також вказує на існуванні різниці між пропагандою та критикою, але не розкриває ці поняття і не встановлює межі між ними [32].

У Кодексі практики Європейського Союзу щодо протидії дезінформації запропоновано співпрацю з онлайн-платформами, соціальними мережами та рекламною індустрією для боротьби з поширенням дезінформації та фейків. Кодекс зобов'язує підписантів розробити політику щодо протидії недобросовісній рекламі, зокрема, політичній, неправомірному використанню ботів. Також вказується на необхідність оприлюднення інформації щодо замовників політичної і тематичної реклами, інформації про те, чому ця реклама спрямована на певну особу, покращення пошукових можливостей для користувачів тощо [33].

Facebook, Twitter і Google підписали кодекс практики Європейської Союзу щодо протидії дезінформації і повідомили, що вони вжили заходів для підвищення прозорості на своїх платформах, включаючи надання загальнодоступних бібліотек політичної реклами для ЄС, співпрацюють з сторонніми організаціями, які перевіряють факти, щоб виявляти оманливий контент, пов'язаний із виборами, та блокувати фейкові акаунти [34].

Парламентською асамблеєю Ради Європи у 2020 році прийнято Резолюцію 2326 “Демократія зламана? Як відповісти?”, в якій висловлено стурбованість у зв'язку з поширенням дезінформаційних кампаній, спрямованих на формування суспільної думки, тенденцій маніпуляцій та іноземного втручання у виборчі процеси. В документі йдеться про необхідність вдосконалення процесів у мережі Інтернет, які б дозволили боротися з дезінформацією, а також про посилення співпраці та інвестування у якісну журналістику [35].

Комітет Міністрів Ради Європи надав декілька важливих для протидії шкідливому інформаційному впливу рекомендацій. Так, в Рекомендації CM/Rec(2018)2 про роль та відповідальність інтернет-посередників йдеться про посилення відповідальності провайдерів за порушення прав їхніх клієнтів. Зокрема, це зобов'язання щодо модерування контенту, контролю у сфері захисту персональних даних, тобто забезпечення гарантій дотримання прав людини у мережі [36]. Крім того ухвалено Рекомендацію CM / Rec (2020) 1

щодо впливу алгоритмічних систем на права людини. Саме алгоритмічні системи застосовуються для поширення цільової реклами, політичної в тому числі, що передбачає і небезпеку поширення дезінформації [37].

У 2017 році спеціальні доповідачі ООН, ОБСЄ, Організації американських держав з питань свободи вираження поглядів та Спеціальна Африканська комісія з прав людини і народів видали Спільну декларацію щодо свободи висловлювання та фейкових новин, дезінформації та пропаганди. В документі наголошується на необхідності скасування кримінальних законів про дифамацію, неприпустимості завідомо неправдивих заяв державних структур, створення безпечного простору для свободи вираження поглядів, саморегуляції ЗМІ (етика та стандарти журналістської діяльності). В документі наведені загальні принципи, яких необхідно дотримуватися в процесі боротьби з шкідливим інформаційним впливом, серед яких:

- держави можуть обмежувати право на свободу вираження поглядів відповідно до вимог міжнародного права, таке обмеження повинно бути необхідним і пропорційним для захисту цих інтересів;

- посередники не повинні нести відповідальність за будь-який контент третьої сторони, якщо вони не втручаються в цей зміст або не відмовляться видалити його за наказом уповноваженого наглядового органу та мають для цього технічні можливості;

- передбачити захист від відповідальності осіб, які перерозповсюджували через посередників дезінформаційні повідомлення, проте не є їх авторами і не вносили до них змін;

- блокування цілих веб-сайтів, IP-адрес, портів або мережевих протоколів державою повинно бути крайнім заходом, який може бути виправданий лише там, де це передбачено законом і є необхідним для захисту права людини чи іншого законного суспільного інтересу;

- системи фільтрації контенту, які встановлені урядом і не контролюються кінцевим користувачем, не є виправданим для обмеження свободи вираження поглядів та інші [11].

Розуміючи всю складність проблеми дезінформаційного впливу, міжнародні організації створюють постійно діючі органи для поширення власних наративів, оперативного реагування та дослідження нових проявів інформаційної агресії. Так, у вересні 2015 року розпочала роботу оперативна робоча група зі стратегічних комунікацій Європейського Союзу — East StratCom Task Force. Діяльність групи спрямована на: роз'яснення ключових аспектів політики Європейського Союзу, створення його позитивного іміджу та протидія дезінформації; ефективну комунікацію та просування політики ЄС щодо Східного партнерства; загальний розвиток медійного простору в країнах Східного партнерства та країнах-членах ЄС, що передбачає сприяння свободі ЗМІ; вдосконалення механізмів, що уможливають передбачення, оцінку та реагування ЄС на дезінформацію, яка поширюється зовнішніми суб'єктами та інше [38]. Оперативна група випускає щотижневий Огляд дезінформації та публікує його на своєму офіційному веб-ресурсі. Результати діяльності групи дозволили краще зрозуміти тактику і техніку державних і недержавних суб'єктів в сфері дезінформації та починати активно протидіяти цьому явищу.

В квітні 2017 представниками країн НАТО та ЄС було прийняте рішення про створення Європейського центру протидії гібридним загрозам, який з вересня 2017 працює у Фінляндії. Засновниками центру стали 12 країн: Фінляндія, Швеція, Норвегія, Великобританія, Іспанія, США, Франція, Польща, ФРН, Естонія, Латвія і Литва. Його метою є протидія «новим загрозам, спрямованим на дестабілізацію ситуації в європейських країнах». Основними напрямками діяльності Центру є: проведення досліджень, аналіз гібридних загроз та методів боротьби з ними; організація спільного навчання для країн-учасниць; проведення консультацій на стратегічному рівні між учасниками ЄС та НАТО [39].

2.2. Правова та організаційна практики протидії дезінформації в інших країнах

Зважаючи на необхідність побудови дієвої системи протидії шкідливому інформаційному впливу та стримування поширення дезінформації, особливо

такої, яка шкодить національним інтересам, розробка відповідних стратегій стала пріоритетним напрямком для багатьох демократичних держав. Найбільш актуальною для європейських країн є російська пропаганда і переважно реакція на неї втілюється в антидезінформаційних стратегіях. Аналітичний центр European Values поділив країни на декілька груп в залежності від їх сприйняття проблеми російської дезінформаційної агресії.

Такі країни як Кіпр, Греція, Угорщина чи Італія, які безпосередньо співпрацюють із пропагандистськими зусиллями Кремля або заперечують цю проблему як таку. Їх позиція може бути спричинена взаємною легітимацією урядів і режимів або з економічних причин. Важливу роль відіграє географічне розташування. Країни в Західній Європі переважно не мають безпосереднього досвіду з Кремлем, а тому не відчують необхідності говорити про це. Є країни, які сумніваються. Є ті, які розуміють існування проблеми, але вважають це проблемою Східної Європи. Країни з «історичною нейтральністю», як Ірландія, уникають будь-яких суперечливих кроків, які необхідно вжити проти будь-якої іншої держави. Окремо аналітичний центр виділяє ряд країн, що «прокинулись»: ті, які вже потрапили під низку серйозних атак. Це, наприклад, Німеччина після кібератак на її установи, це напади на кампанію Макрона у Франції. Це Нідерланди та кампанія дезінформації навколо МН17. Ці країни починають щось робити; у них іще немає комплексних стратегій, але вони створюють деякі установи, переглядають свої інструменти. Вони часто вважають це проблемою для власної внутрішньої безпеки. Існує група країн з найбільш успішною практикою, – це Латвія, Литва, Естонія, Швеція та Великобританія. І це країни, які мають історичний досвід із Росією та її зусиллями щодо «операцій впливу» [40].

Сьогодні Фінляндія вважається найбільш стійкою до фейків. Країна потерпала від шкідливого інформаційного впливу зі сторони Росії з того часу, як вийшла з її складу. Коли у 2015 році діяльність російських пропагандистів активізувалася, президент Фінляндії закликав всіх своїх громадян взяти на себе відповідальність за боротьбу з дезінформацією. Через рік, Фінляндія залучила

американських експертів для навчання чиновників і отримати досвід як розпізнати фейкові новини, зрозуміти, чому вони стають вірусними, і розробити стратегії боротьби з ними. Також була реформована система освіти: впровадили навчальні курси для школярів щодо виявлення дезінформації, критичного мислення, фактчекінгу. Результативність фінського підходу до протидії деструктивному інформаційному впливу підтверджується тим, що експерти не знайшли жодних доказів російського втручання у голосування під час останніх виборів в країні. Це може бути ознакою того, що поширювачі дезінформації перестали думати про фінський електорат як про м'яку мішень [34].

Однією з перших країн, яка на законодавчому рівні почала боротися з дезінформацією, була Федеративна Республіка Німеччина. У 2015 році було створено робочу групу з розробки законопроекту щодо протидії поширенню антиправової інформації в соціальних мережах [41]. Уряд країни усвідомлював масштаби поширення фейкової інформації на різних інтернет-платформах, тому намагався домовитися з найбільшими компаніями Facebook, Google і Twitter про видалення шкідливого контенту. Проте показники видалення не задовільнили керівництво держави. На початку 2017 року Facebook видалив лише 39% фейкового контенту, Twitter – 1 %, Google YouTube – 90 % [42].

В результаті активізувалася діяльність уряду по розробці законопроекту, метою якого мало бути нормативне регламентування поширення інформації в мережі Інтернет. 1 жовтня 2017 року було прийнято Закон «Про регулювання соціальних мереж», який зобов'язав операторів соціальних мереж, які мають понад два мільйони зареєстрованих акаунтів (перш за все Twitter, Facebook та YouTube), протягом 24 годин після надходження скарги видаляти контент, який містить очевидно протиправну інформацію (порушення відповідних розділів Кримінального кодексу Німеччини), а саме: поширення пропагандистських матеріалів антиконституційного характеру, підготовка і підбурювання до загрозливого безпеки держави насильницького злочину, заклик до вчинення злочину, створення злочинних об'єднань чи терористичних організацій,

розпалювання ненависті, поширення зображень насильства, заохочення і схвалення злочинів, образа віросповідань, наклеп, порушення недоторканності приватного життя шляхом фотографування тощо [41].

Якщо оператори соціальних мереж отримують більше 100 скарг на рік, то Закон їх зобов'язує двічі на рік звітуватися перед урядом про видалений контент («Звіт щодо прозорості»). Вперше за порушення норм даного закону санкції було застосовано до компанії Facebook в липні 2019 року, на яку Федеральним бюро юстиції Німеччини накладено штраф у розмірі 2 мільйони євро. Підставою стало опублікування недостовірної інформації про кількість отриманих скарг, що описувало хибні масштаби нелегального контенту на платформі і те, як Facebook з ним працює [43].

Такі дії Німеччини були неоднозначно сприйняті світовою спільнотою, ми в даному питанні погоджуємося з позицією науковця Р. Черниша, який зазначив, що розробка вище вказаного Закону та його імплементація до національного законодавства саме європейською правовою державою стало прецедентом, який впливатиме на розвиток соціальних мереж, організацію комунікації користувачів, регламентацію правил щодо поширення інформації [41].

У Франції в листопаді 2017 керівництво Вищої ради з аудіовізуальних засобів заявило, що буде вести постійний перегляд програм, які транслюватиме російський телеканал Russia Today у Франції. Крім цього, Рада з аудіовізуальних засобів проводить моніторинг діяльності сайту російського агентства новин Sputnik [44].

На початку січня 2018 року Президент Франції Еммануель Макрон заявив про підготовку законопроекту, орієнтованого на боротьбу з поширенням неправдивої інформації в періоди виборчих кампаній. На Національних зборах 20 листопада 2018 року було ухвалено закон «Проти маніпуляції інформацією». Він, зокрема, дозволяє суддям ідентифікувати фейкові новини і швидко припиняти їхнє поширення. Французькому органу мовлення (Вища

аудіовізуальна рада) дозволено блокувати телевізійні медіа, які контролюються з-за кордону і діють проти державних інтересів [45].

Законотворці приділили особливу увагу втручанням іноземних держав та їхніх засобів масової інформації у виборчий процес Франції. Була спрощена процедура подачі партіям та окремими кандидатами судових позовів з вимогою припинити поширення підробленої інформації. Суди розглядають такі справи впродовж 48 годин. Закон також передбачає спеціальне регулювання для інтернет-платформ, які зобов'язали надавати інформацію про замовний контент [46].

В порівнянні з іншими європейськими країнами, законодавство Великобританії в сфері протидії дезінформаційному впливу є досить обмеженим. Проте, країна демонструє злагоджену міжпарламентську взаємодію у даному питанні. У 2019 році, після тривалих обговорень теми дезінформації та фейкових новин у профільному комітеті Нижньої палати Парламенту з питань цифрових технологій, культури, медіа і спорту, була підготовлена внутрішня рекомендаційна доповідь. Особлива увага у вказаному документі приділяється проблемі поширення під час виборчих кампаній «дезорієнтуючої шкідницької дезінформації». В Доповіді рекомендується: створити робочу групу для дослідження шляхів протидії розповсюдженню дезінформації на платформах соціальних медіа; на час проведення політичних кампаній усі подані рекламні матеріали обов'язково повинні містити інформацію про замовників та бути загальнодоступними, а не відкриватися тільки таргетованим користувачам; покласти на соціальні медіа юридичну відповідальність за будь-який розміщений на їхніх платформах агресивний протиправний контент; британським регуляторам здійснювати аудит рекламної індустрії, яка використовує соціальні медіа, встановити граничні межі фінансування політичних кампаній тощо [47].

Також британські парламентарі представили законопроект, так звану «Білу книгу про шкоду, заподіяну в інтернеті», в якому рекомендовано великим інтернет-компаніям (наприклад Facebook або Twitter) щорічно складати та

оприлюднювати доповіді з аналізом дезінформаційного контенту, який було розміщено на їхніх платформах, та вжитих заходів по його знешкодженню. Разом з тим, законопроект не передбачає створення спеціального державного регулятора онлайн-медіа [48].

Варто зазначити, що Великобританія завжди розглядала питання протидії шкідливому інформаційному впливу на стратегічному, тактичному та оперативному рівнях в площині національної безпеки та оборони. Питання протидії дезінформації висвітлені у документі Стратегія національної безпеки та стратегічна оборона і стратегічний огляд 2015 та урядовому документі «Огляд ресурсів національної безпеки» [49-50].

У 2016 році створено Національний центр кібербезпеки під керівництвом Центру урядового зв'язку (спеціалізована британська спецслужба, яка займається питаннями технікокомунікативної розвідки та контррозвідки). Одним із завдань Центру є протидія дезінформації [51]. В січні 2018 р. британський уряд повідомив про створення Національного управління з безпеки комунікацій, який спеціалізується на протидії дезінформації, фейковим новинам та шкідливим наративам, що поширюються державними та позадержавними суб'єктами [52].

Аналіз законодавства європейських країн у сфері протидії шкідливому інформаційному впливу свідчить про те, що відповідна діяльність регулюється в межах цивільного законодавства, жодна з розглянутих країн не криміналізувала поширення дезінформації. Проте є ряд країн, які пішли іншим шляхом. Так, у Малайзії діє Закон про протидію фейковим новинам, яким передбачається покарання у виді позбавлення волі на строк до шести років і \$123 тис. штрафу за поширення і створення новин, інформації, даних або доповідей, помилкових повністю або частково. Цей Закон поширюється не тільки на фізичних осіб, а також й на провайдерів. При цьому під дію Закону також підпадають не тільки громадяни, а й публікації, які створюються в інших країнах за участю малайзійців. Правозастосовна практика містить приклади

притягнення до кримінальної відповідальності громадян, які через Інтернет критикували процес виборів у країні [53].

У 2019 році в Сінгапурі прийнято Закон про захист від неправдивої інформації та маніпуляцій в онлайн, який спрямований на протидію поширення фейкових новин. Даний нормативно-правовий акт надає право урядовим міністрам вимагати від окремих осіб та інтернет-платформ виправлення або видалення того, що вони вважають неправдивою інформацією, яка шкодить суспільним інтересам, або блокування веб-сайтів, які, на їхню думку, займаються пропагандою шкідливої неправдивої інформації. За невиконання передбачених законом вимог передбачено кримінальну відповідальність – до 10 років ув'язнення та штрафи. Фізичні особи або інтернет-платформи можуть оскаржувати вимогу в міністрів або в судовому порядку [54].

Криміналізовано поширення дезінформації і в Казахстані, хоча законодавець і не використовує термін «дезінформація», а оперує поняттям «завідомо неправдива інформація». Так, ст. 274 Кримінального кодексу Казахстану передбачає санкцію позбавлення волі до 7 років за поширення такої інформації, що створює небезпеку порушення громадського порядку або заподіяння істотної шкоди правам і законним інтересам громадян, організацій або інтересам суспільства чи держави, що охороняються законом [55]. Істотною шкодою є: порушення конституційних прав та свобод людини й громадянина, порушення штатної роботи організацій та установ, державних органів, провокування зриву важливих військових заходів, боєздатності військових частин тощо. Обтяжуючими обставинами є: поширення подібної інформації групою осіб або з використанням службового становища, що спричинило великі збитки, або з використанням мережі Інтернет чи ЗМІ. Разом з тим, наслідки не є обов'язковою ознакою даного складу злочину [53].

ВИСНОВКИ ДО РОЗДІЛУ 2

Важливим кроком у протидії деструктивному інформаційному впливу вбачається усвідомлення існування даної проблеми на міжнародному рівні та об'єднання зусиль в даному напрямку, адже з розвитком засобів комунікації поширення дезінформації стерло кордони і створило загрозу для всього демократичного суспільства і кожної окремо взятої особи.

У питаннях протидії дезінформаційному впливу міжнародна спільнота застосовує підхід, за якого дезінформація розглядається як загроза для прав людини (наприклад, для прав на свободу думки, совісті, вільне волевиявлення під час виборів, повагу до приватного життя тощо). При цьому сфера шкідливого інформаційного впливу регулюється більше в рамках м'якого права, тобто спрямована на з'ясування причин, модерацію контенту, а не його масове блокування і притягнення до відповідальності причетних осіб.

«Підхід Європейського Союзу полягає в тому, щоб підсилити і надати можливості широкому колу учасників, серед яких громадянське суспільство, медіа, академічні кола, приватний сектор, а особливо онлайн-платформи та рекламодавці, щоб захистити наші демократії від іноземного втручання та дезінформації,» - зазначає заступник голови Представництва Євросоюзу в Україні Ремі Дюфло [56].

В рамках міжнародних стандартів кожна держава впроваджує політику та законодавство щодо протидії дезінформаційному впливу на національному рівні. Варто зазначити, що діяльності в сфері протидії шкідливому інформаційному впливу окремих країн ЄС є значно послідовнішою та жорсткішою, ніж діяльність спільних інституцій. Разом з тим, європейські країни регулюють поширення шкідливого інформаційного впливу в межах цивільного законодавства, тоді як Малайзія, Сінгапур, Казахстан та деякі інші країни криміналізували вказаний вид діяльності.

РОЗДІЛ 3. ПРОТИДІЯ ДЕСТРУКТИВНОМУ ІНФОРМАЦІЙНОМУ ВПЛИВУ В УКРАЇНІ

3.1. Нормативно-правове регулювання

Проблема нормативно-правового регулювання протидії деструктивному інформаційному впливу була досліджена нами в науковій статті «Національні інтереси держави та можливість обмеження права на свободу слова: питання співвідношення» [1]. Зокрема, звертаємо увагу на те, що у тому випадку, коли державні інституції починають певним чином регламентувати процес поширення інформації, то одразу виникає дискусія про співіснування демократичного суспільства з впливом на інформаційну сферу. Хоча обмеження права на вільне вираження своїх поглядів не є унікальним для України, а визнане необхідним і в інших демократичних інституціях та міжнародній практиці. Наприклад, в ч. 2 ст. 10 Конвенції про захист прав людини і основоположних свобод аналогічно закріплено можливість існування для права вираження поглядів формальностей, умов, обмежень або санкцій, що встановлені законом і є необхідними в демократичному суспільстві [57].

Також, потрібно виходити з того, що усі права людини і громадянина передбачені Конституцією України є рівними за своєю юридичною силою. Тому досить дискусійною є ситуація, за якої не викликає непорозумінь, наприклад, законне обмеження права на «...свободу та особисту недоторканність» в межах проведення негласних слідчих (розшукових) дій), при цьому, законне обмеження права на «... свободу думки і слова, на вільне вираження своїх поглядів і переконань» на думку окремих науковців та представників громадськості є недопустимим [58].

Виходячи з цього, перед науковцями, практиками, громадськими діячами постає нелегке завдання - досягти балансу між свободою громадянина та національною безпекою в інформаційному полі. При цьому, не допустити виникнення двох протилежних загроз - втрати національного суверенітету та авторитаризму. У вказаному контексті, слід відмітити, що конституційна можливість обмеження права на збирання, зберігання, використання і

поширення інформації є підґрунтям для протидії негативному інформаційному впливу, який ще в 2007 році в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» був визнаний загрозою інформаційній безпеці держави [59].

На сьогодні діє низка нормативно-правових актів, які встановлюють обмеження на поширення певного виду інформації у відповідній сфері діяльності. Зокрема, Закон України «Про телебачення і радіомовлення» у ст. 6 забороняє використання телерадіоорганізацій для поширення такого деструктивного контенту як заклики до насильницької зміни конституційного ладу України, до розв'язування агресивної війни, до розпалювання національної, расової чи релігійної ворожнечі та ненависті; необґрунтований показ насильства; пропаганда винятковості, зверхності або неповноцінності осіб за ознаками їх релігійних переконань, ідеології, належності до тієї чи іншої нації або раси, фізичного або майнового стану, соціального походження; трансляції, у яких надаються послуги з ворожіння, нетрадиційної медицини, які можуть завдати шкоди фізичному, психічному чи моральному розвитку дітей та підлітків; розповсюдження і реклама порнографічних матеріалів та предметів; пропаганда наркотичних і психотропних речовин [60].

Варто звернути увагу на те, що у 2015 році наша держава відреагувала на зовнішні виклики у формі російської агресії і окупації Криму та спробувала мінімізувати деструктивний інформаційний вплив щодо даної тематики у телепросторі країни, а тому доповнила вище вказаний перелік заборонами трансляції телепередач, виготовлених після 1 серпня 1991 року, що містять популяризацію або пропаганду органів держави-агресора та їхніх окремих дій, що виправдовують чи визнають правомірною окупацію території України, а також трансляції аудіовізуальних творів, одним із учасників яких є особа, внесена до Переліку осіб, які створюють загрозу національній безпеці [60].

Аналогічні обмеження були введені і в інших сферах, які прямо чи опосередковано здійснюють інформаційний вплив в Україні. На сьогодні в Україні на законодавчому рівні заборонено використання засобів масової

інформації (далі ЗМІ) з метою популяризації або пропаганди держави-агресора та її органів влади, представників органів влади держави-агресора та їхніх дій, що створюють позитивний образ держави-агресора, виправдовують чи визнають правомірною окупацію території України (стаття 3 ЗУ «Про друковані засоби масової інформації (пресу) в Україні») [61], заборонено розповсюджувати та демонструвати фільми, які популяризують органи держави-агресора або радянські органи держбезпеки (стаття 15-1 ЗУ «Про кінематографію») [62], заборонено у видавничій справі випускати продукцію аналогічної тематики (стаття 28 ЗУ «Про видавничу справу») та введено дозвільний режим на ввезення видавничої продукції з території країни-агресора (стаття 28-1 ЗУ «Про видавничу справу») [63].

В контексті діючих заборон, варто наголосити, що ч. 3 ст. 15 Конституції України заборонена цензура [64]. У ст. 24 Закону України «Про інформацію» під цензурою, яка забороняється, розуміється будь-яка вимога, спрямована, зокрема, до журналіста, засобу масової інформації, його засновника (співзасновника), видавця, керівника, розповсюджувача, узгоджувати інформацію до її поширення або накладення заборони чи перешкоджання в будь-якій іншій формі тиражуванню або поширенню інформації. Разом з тим, така заборона не поширюється на випадки, коли попереднє узгодження інформації здійснюється на підставі закону, а також у разі накладення судом заборони на поширення інформації [65].

Таким чином, у держави є механізм впливати на інформаційне середовище, проте він недостатньо дієвий у масштабах того шкідливого інформаційного впливу, з яким Україна, як і все демократичне суспільство, стикнулася сьогодні. Тому часто дії влади є ситуативними хоч і виправданими з точки зору захисту національних інтересів, проте дискусійними в площині свободи слова. Наглядним прикладом є припинення діяльності ряду українських телеканалів в результаті прийнятого Рішення Ради національної безпеки і оборони України від 2 лютого 2021 року Про застосування персональних спеціальних економічних та інших обмежувальних заходів

(санкцій), яке введено в дію Указом Президента України від 2 лютого 2021 року № 43/2021 [66]. Даний крок влади був цілком виправданий і схваленим європейською спільнотою, проте правники та медійники розпочали дискусію про те, як цей прецедент вплине на свободу слова в Україні.

Варто погодитися з Пітером Стано, речником ЄС із закордонних справ і політики безпеки, який неоднозначно оцінив закриття українських телеканалів: «Як передбачено Угодою про асоціацію між Україною та ЄС, ЄС надає найбільше значення незалежності та свободі ЗМІ. Постійні проросійські кампанії дезінформації впливали і продовжують впливати на українські медіа. Хоча спроби України захистити свою територіальну цілісність та національну безпеку, а також захиститися від маніпуляцій інформацією є законними, зокрема, враховуючи масштаби дезінформаційних кампаній, що зачіпають Україну, в тому числі з-за кордону, це не повинно відбуватися за рахунок свободи засобів масової інформації та повинно здійснюватися з повною повагою основних прав і свобод та з дотриманням міжнародних стандартів» [67].

На нашу думку, у цілому, обмеження свободи слова є можливим за умови його відповідності чітко визначеним вимогам. Наприклад:

- передбачатися законом – чітко визначатися у нормативному-правовому акті, які саме дії є забороненими і тягнуть за собою відповідальність, щоб кожна особа могла розуміти наслідки своїх дій;

- переслідувати законну мету – тобто спрямовані виключно на захист інтересів національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я, життя або моралі, для недопущення розголошення державної таємниці або для підтримання авторитету і безсторонності суду;

- не переходити межу необхідності для демократичного суспільства – тобто рівень втручання держави має бути мінімальним, держава повинна припинити обмеження, як тільки буде досягнута мета втручання тощо.

Існування чітких механізмів реагування на шкідливий інформаційний вплив повинно забезпечити прозорість вказаного процесу. Чинне законодавство України передбачає відповідальність за поширення неправдивої інформації на декількох рівнях: цивільно-правовому, адміністративному та кримінальному.

Цивільний кодекс України в ст. 277 закріплює за фізичною особою право на відповідь та на спростування поширеної про неї (або членів її сім'ї) недостовірної інформації, а в статті 280 – право на відшкодування майнової чи моральної шкоди [68]. Адміністративна відповідальність настає за поширювання неправдивих чуток, що можуть викликати паніку серед населення або порушення громадського порядку, і тягне за собою накладення штрафу від десяти до п'ятнадцяти неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до одного місяця з відрахуванням двадцяти процентів заробітку (ст. 173-1 КУпАП) [69].

У кримінальному законодавстві вже не йде мова про факт достовірності інформації, що поширюється, а оцінюється ступінь загрози, яку вона може нанести. Зокрема, у ст. 109 КК України злочином визнаються публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій, а в статті 110 - публічні заклики чи розповсюдження матеріалів із закликами до вчинення дій, метою яких є зміни меж території або державного кордону України. Також передбачено кримінальну відповідальність за публічні заклики до вчинення терористичного акту (ст. 258-2 КК України), за заклики до вчинення дій, що загрожують громадському порядку (ст. 295 КК України), за публічні заклики і поширення матеріалів із закликами до вчинення дій, що мають ознаки жорстокого поводження з тваринами (ст. 299 КК України) [70].

Кримінальними правопорушеннями проти миру, безпеки людства та міжнародного правопорядку національним законодавством визнаються публічні заклики до агресивної війни або до розв'язування воєнного конфлікту, а також виготовлення матеріалів із закликами до вчинення таких дій з метою їх розповсюдження (ст. 436 КК України), пропаганда комуністичного та націонал-

соціалістичного (нацистського) тоталітарних режимів (ст. 436-1 КК України), публічні заклики до геноциду, а також виготовлення матеріалів із закликами до геноциду з метою їх розповсюдження (ст. 442 КК України) [70].

3.2. Державні інституції в боротьбі з дезінформацією

З метою виявлення і реагування на шкідливий інформаційний вплив в Україні сьогодні діють дві структури: Центр протидії дезінформації при РНБО і Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики.

Варто зазначити, що відповідно до чинного законодавства РНБО не має повноважень безпосередньо впливати на інформаційну діяльність. Згідно із ст. 107 Конституції України РНБО координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони [64]. Компетенція та функції РНБО визначаються Законом України «Про Раду національної безпеки і оборони України». Згідно зі ст. 3 цього закону функціями РНБО є: внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки і оборони; координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони у мирний час; координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України [71].

Разом з тим, ст. 14 вказаного закону передбачено, що для опрацювання і комплексного вирішення проблем міжгалузевого характеру, забезпечення науково-аналітичного та прогнозного супроводження діяльності Ради національної безпеки і оборони України за її рішенням в рамках коштів, передбачених Державним бюджетом України, можуть утворюватися міжвідомчі комісії, робочі та консультативні органи [71].

Центр протидії дезінформації при РНБО створено Рішенням Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації», яке введено в дію Указом

Президента України від 19 березня 2021 року № 106/2021 [72]. Чим має займатися даний робочий орган більш зрозуміло стає з Положення про Центр протидії дезінформації, яке затверджено Указом Президента України від 7 травня 2021 року № 187/2021. Згідно з Положенням, Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою [73].

Серед основних завдань Центру вказується аналіз і моніторинг, виявлення та вивчення поточних і прогнозованих загроз, забезпечення інформаційно-аналітичними матеріалами, підготовка та внесення пропозицій РНБО щодо визначення концептуальних підходів у відповідній сфері, координація діяльності та взаємодії органів виконавчої влади, здійснення системних заходів, удосконалення системи правового та наукового забезпечення. Також Центр має брати участь у розбудові системи стратегічних комунікацій, у розробленні та реалізації Стратегії інформаційної безпеки України, у створенні інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них тощо. З метою виконання покладених на нього завдань Центр може у встановленому законом порядку отримувати статистичні дані, інформацію, довідкові та інші матеріали від органів державної влади, а також користуватися їх базами даних. Центр також може створювати платформи для обговорення та вивчення питань дезінформації, а саме: бути замовником науково-дослідних робіт, проводити конференції, семінари, наради, встановлювати партнерські відносини з міжнародними суб'єктами, брати участь у структурованих діалогах та інше [73].

Вбачається, що Центр протидії дезінформації є виключно дорадчим і суть його роботи зводиться до інформаційно-аналітичної діяльності, оскільки даній структурі не надано жодного повноваження, яке б дозволило припинити

конкретний прояв здійснення шкідливого інформаційного впливу. Центру навіть не довірили вносити санкційні пропозиції, так як стаття 5 Закону України «Про санкції» містить вичерпний перелік суб'єктів, які можуть вносити пропозиції щодо застосування, скасування та внесення змін до санкцій [74].

Варто звернути увагу, що одним із завдань Центру протидії дезінформації є підготовка та внесення РНБО пропозицій щодо координації діяльності та взаємодії органів виконавчої влади з питань національної безпеки в інформаційній сфері [73]. Зауважимо, що згідно з Положенням про Міністерство культури та інформаційної політики України, координація діяльності органів виконавчої влади з питань інформаційної безпеки є завданням саме цієї структури [75]. Очевидно, що робота по боротьбі з інформаційними загрозами і дезінформацією певний час фактично не здійснювалася через відсутність правових механізмів. Проте у березні 2021 року такий механізм з'явився і ним став Центр стратегічних комунікацій та інформаційної безпеки (ЦСКІБ) при Міністерстві культури та інформаційної політики. Робота Центру сфокусована на комунікаційній протидії зовнішнім загрозам, зокрема, інформаційним атакам Російської Федерації.

«ЦСКІБ спрямований на об'єднання зусиль громадських організацій та влади у боротьбі із дезінформацією, швидке реагування на фейки, а також на промоцію українських наративів. У структурі діятиме при МКІП, але у співпраці з Центром протидії дезінформації РНБО, за яким лишається безпекова функція і перспектива міжнародного хаб» [76].

ЦСКІБ зосередить свою роботу на: стратегічних комунікаціях, що включатимуть розробку контрнативів РФ, проведення інформкампаній, включення українських наративів у щоденну комунікацію Уряду; створення онлайн-ресурсу, який активно реагуватиме на інформатаки; регулярному сповіщенні про гібридну агресію з боку Росії на міжнародному рівні, спільне напрацювання механізмів з протидії дезінформації з міжнародними партнерами [76].

3.3. Стратегічний підхід в протидії шкідливому інформаційному впливу

Варто зауважити, що українська влада більш стратегічно і предметно почала підходити до протидії шкідливому інформаційному впливу. Рада національної безпеки і оборони України 15 жовтня 2021 року схвалила Стратегію інформаційної безпеки [77]. Цей документ набере чинності після затвердження відповідного рішення Указом Президента України. Звернемо увагу, що чинною залишається Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року № 47/2017.

Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни [78]. Таким чином, документ є методом реагування саме на агресію з боку Російської Федерації, і розглядається як спеціальна і тимчасова необхідність впровадження певних заходів додатково до існуючого інформаційного законодавства, яка буде припинена із завершенням російської агресії. Документ є уточнюючим і не передбачає зміну формату суспільних відносин в інформаційній сфері, а опирається на чинне законодавство та діючі правові механізми для виконання конкретного завдання – протидії шкідливому інформаційному впливу Російської Федерації.

Зауважимо, що на ситуативний характер діючої Доктрини вказує і перелік визначених загроз з боку країни-агресора. Зокрема, актуальними загрозами є здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу ЗСУ 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, проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у

світі, інформаційне домінування держави-агресора на тимчасово окупованих територіях тощо [78].

Відповідно, Доктриною визначаються пріоритети державної політики щодо забезпечення інформаційної безпеки, забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію, відкритості та прозорості держави перед громадянами, формування позитивного міжнародного іміджу України. Доктрина, на виконання поставлених завдань, залучає доволі широке коло суб'єктів, ставлячи завдання перед Радою національної безпеки і оборони України, Кабінетом Міністрів України, Міністерством інформаційної політики України, Міністерством закордонних справ України, Міністерством оборони України, Міністерством культури України, Державним агентством України з питань кіно, Національною радою України з питань телебачення і радіомовлення, Державним комітетом телебачення і радіомовлення України, Службою безпеки України, розвідувальними органами України, Державною службою спеціального зв'язку та захисту інформації України, Національним інститутом стратегічних досліджень [78]. Таким чином до вирішення відповідних завдань залучаються існуючі механізми реагування згідно з повноваженнями і не відбувається нарощення нових державних органів з дублюючим функціоналом.

Звернімо детальніше увагу на Стратегію інформаційної безпеки. Метою Стратегії є створення умов для забезпечення інформаційної безпеки України, спрямованої на захист життєво важливих інтересів громадянина, суспільства та держави у протидії внутрішнім та зовнішнім загрозам, забезпечення захисту державного суверенітету і територіальної цілісності України, підтримка соціальної та політичної стабільності, оборони держави, забезпечення прав та свобод кожного громадянина [79]. Вбачається, що документ передбачає загальні засади інформаційної безпеки без прив'язки до джерела виникнення загрози і «планує» змінити формат інформаційних відносин, а відтак її норми діятимуть після закінчення російської агресії.

Перш за все варто наголосити, що Стратегія у формулюванні своєї мети оперує законодавчо невизначеними поняттями, такими як «життєво важливі інтереси», «соціальна стабільність», «політична стабільність», що розмиває межі необхідності втручання держави в інформаційні права, чим створює загрозу демократичному суспільству. Разом з тим в документі аналізується широке коло загроз інформаційній безпеці, що логічно потребує державного втручання майже у всі сфери інформаційної діяльності в Україні. Зокрема, загрозами інформаційній безпеці держави на глобальному рівні визнається збільшення кількості глобальних дезінформаційних кампаній, інформаційна політика Російської Федерації як загроза для України та інших демократичних країн, інституалізація соціальних мереж, зміна балансу інформаційних відносин та захист особистих прав людини, низький рівень медіаграмотності громадян у поєднанні із стрімким поширенням цифрових технологій. На національному рівні, згідно із Стратегією, існують такі загрози: інформаційний вплив на населення з боку іноземних держав, інформаційне домінування держави-агресора на тимчасово окупованих територіях, обмежені можливості реагування на дезінформаційні кампанії, несформованість системи стратегічних комунікацій, проблема унормування медіавідносин та захисту професійної діяльності журналістів, маніпуляція свідомістю громадян щодо вступу України в ЄС та НАТО, інформаційні потреби на місцевому рівні, недостатній рівень інформаційної культури та медіаграмотності населення для протидії маніпулятивним та інформаційним впливам [79].

Вбачається, що документ охоплює всі поточні та можливі майбутні небезпеки для інформаційного середовища. Разом з тим у Стратегії не визначено ступінь небезпеки конкретної загрози, а відповідно і не оцінено величину шкоди для держави і суспільства, що уповільнює організацію системи державних пріоритетів у процесі реагування на загрози. Відсутність визначених першочергових і наступних цілей призводить до неефективності використання наявних ресурсів, які і без того є обмеженими.

Беручи до уваги визначені в Стратегії пріоритети держави, чітко прослідковується спроба переформатувати всю сферу поширення інформації, оскільки крім протидії російському дезінформаційному впливу, документ визначає пріоритетом інформаційної безпеки виключно культурні сегменти, наприклад забезпечення всебічного розвитку української культури та утвердження національної самоідентичності. Крім того, з метою досягнення стратегічної цілі з підвищення рівня медіакультури та медіаграмотності суспільства, документ ставить задачу удосконалити законодавство України у сфері реклами, що включатиме лібералізацію норм у цій сфері та більш жорстку відповідальність за трансляцію прихованої реклами. В Стратегії передбачено удосконалення законодавства України, що регулює питання правового статусу журналістів, провадження ними своєї професійної діяльності, відповідальності за правопорушення, вчинені проти журналістів, членів їх родин та майна, а також за перешкоджання їх професійній діяльності, удосконалення законодавства про захист права на доступ до публічної інформації, про захист персональних даних тощо [79].

Механізмом реалізації цілей Стратегії визначено розподіл обов'язків серед таких державних органів як Рада національної безпеки і оборони України, Кабінет Міністрів України, Служба безпеки України, розвідувальні органи України, Національна рада України з питань телебачення і радіомовлення. Крім того, реалізація має здійснюватися органами виконавчої влади у взаємодії з органами місцевого самоврядування та інститутами громадянського суспільства згідно з планом заходів, який затверджується Кабінетом Міністрів України [29], водночас документ прийнято не як програму Кабміну, а у вигляді рішення РНБО, до компетенції якої не відносяться питання розвитку інформаційної та культурної сфери, регулювання реклами чи журналістської діяльності. При цьому, у Стратегії не визначено головний орган державної влади, який нестиме відповідальність і звітуватиме щодо реалізації документу, механізмів моніторингу його ефективності, що послаблює організацію її виконання.

У цілому можна говорити про стратегічно правильний напрямок руху державної влади в Україні у боротьбі зі шкідливим інформаційним впливом, проте непрозорість процедур та підстав втручання в інформаційну діяльність, які запропоновані в Стратегії, відсутність конкретизації у визначенні термінології, відсутність диференціації загроз та змішування пріоритетів створюють підґрунтя для порушення свободи слова в Україні.

ВИСНОВКИ ДО РОЗДІЛУ 3

В Україні існує механізм впливу на інформаційне середовище, проте він недостатньо дієвий у масштабах того шкідливого інформаційного впливу, з яким Україна, як і все демократичне суспільство, стикнулася сьогодні. На нашу думку, існуючі механізми реагування на здійснення шкідливого інформаційного впливу є недостатніми. Законодавець оперує категоріями «недостовірна інформація», «неправдиві чутки», «заклики», проте арсенал сучасних інформаційних воєн значно ширший. Основними технологіями шкідливого інформаційного впливу у XXI столітті є дезінформація, пропаганда, поширення фейкової інформації. Проте, жодна із вказаних категорій системно не присутня в нормативно-правовому полі України [1].

Попри відсутність нормативно визначеного поняття «дезінформація» та пов'язаних із нею дефініцій, в Україні розуміють необхідність протистояння шкідливому інформаційному впливу. Основним викликом у цій сфері для нашої країни залишається деструктивний контент, який продукує Російська Федерація. З метою виявлення і реагування на шкідливий інформаційний вплив в Україні сьогодні діють дві структури: Центр протидії дезінформації при РНБО і Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики.

В Україні схвалено два планових документа, які спрямовані на протидію деструктивному інформаційному впливу: Стратегія інформаційної безпеки та Доктрина інформаційної безпеки України. Обидва документи є програмними, їх правовий характер не містить норм прямої дії, а отже не можна притягнути до кримінальної відповідальності, посилаючись на них. Реальні правові наслідки за відповідні діяння можуть настати лише за умови прийняття спеціальних нормативно-правових актів, які за основу братимуть засади і принципи, визначені Стратегією та Доктриною.

ВИСНОВКИ

Проведене дослідження дає змогу дійти таких висновків:

1. В науці та юридичній практиці не існує єдиного підходу до визначення дезінформації, що ускладнює боротьбу з нею, оскільки неможливо узаконити правовий механізм протидії цьому явищу, який не перетворився б на інструмент цензури. Основною особливістю даної категорії, на нашу думку, варто вважати наявність умислу на її створення та поширення. Вважаємо доцільним **дезінформацію** визначати як відомості неправдивого та/або маніпулятивного характеру, які цілеспрямовано поширюються з метою впливу на важливу суспільну сферу шляхом формування необхідної громадсько-політичної думки. Вбачаємо необхідним ввести дану категорію в правове поле України.

2. У зв'язку із неоднозначністю та складністю явища дезінформації, потрібно визначити критерії, відповідно до яких здійснюватиметься оцінка реальної шкоди, яку вона може спричинити. На нашу думку, при визначенні ступеню нанесеної дезінформацією шкоди варто брати до уваги її зміст, контекст, в який вона поміщається, суб'єкт поширення, місце, форма та спосіб поширення.

3. Міжнародна спільнота розглядає деструктивний інформаційний вплив в контексті загрози демократичним цінностям, а тому об'єднує зусилля в даному напрямку. Разом з тим, протидія вказаному явищу в Європі ґрунтується на з'ясуванні причин, модерації контенту, фактчекінгу, а не притягненні до відповідальності причетних осіб. Важливим кроком в протидії дезінформації вважаємо налагодження співпраці міжнародних урядових організацій з найбільшими онлайн-платформами, оскільки на сьогодні соціальні мережі є найзручнішим майданчиком поширення дезінформації. Facebook, Twitter і Google підписали кодекс практики Європейської Союзу щодо протидії дезінформації і вживають заходів по блокуванню фейків. На нашу думку, такі кроки стосовно онлайн-платформ є дієвими, але недостатніми, оскільки дезінформаційні повідомлення поширюються швидше ніж спростовуються і до

моменту видалення «встигають» викликати необхідну реакцію у кінцевого споживача. Виходячи з цього, вбачається необхідним на рівні ООН розглянути питання про зміну алгоритмів соціальних мереж, які спрямовані на побудову так званих «інформаційних бульбашок» навколо користувача.

4. В рамках міжнародних стандартів кожна держава впроваджує політику та законодавство щодо протидії дезінформаційному впливу на національному рівні. Варто зазначити, що діяльності в сфері протидії шкідливому інформаційному впливу окремих країн ЄС є значно послідовнішою та жорсткішою, ніж діяльність спільних інституцій. Разом з тим, європейські країни регулюють поширення шкідливого інформаційного впливу в межах цивільного законодавства, тоді як Малайзія, Сінгапур, Казахстан та деякі інші країни криміналізували вказаний вид діяльності.

5. В Україні нормативно не визначено поняття «дезінформація» та пов'язаних з вказаним терміном дефініцій, не розроблено критеріїв, згідно з якими інформацію варто відносити до деструктивної, також відсутня класифікація шкоди, якої вона може завдати, не розроблено єдиного унормованого механізму реагування на появу в інформаційному середовищі дезінформації. Нормативно-правова регламентація протидії деструктивному інформаційному впливу в Україні на сьогоднішній день потребує системного і комплексного підходу, цьому сприяють подальші наукові дослідження та врахування міжнародного досвіду у вказаній сфері.

6. З метою виявлення і реагування на шкідливий інформаційний вплив в Україні сьогодні діють дві структури: Центр протидії дезінформації при РНБО, суть роботи якого зводиться до інформаційно-аналітичної діяльності, та Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики, діяльність котрого направлена на розвиток стратегічних комунікацій. Разом з тим, жодна з вказаних інституцій не наділена повноваженнями, які б дозволили припинити конкретний прояв здійснення шкідливого інформаційного впливу.

7. В Україні схвалено два планових документа, які спрямовані на протидію деструктивному інформаційному впливу: Стратегія інформаційної безпеки та Доктрина інформаційної безпеки України. Обидва документи є програмними, їх правовий характер не містить норм прямої дії, а отже не можна притягнути до кримінальної відповідальності, посилаючись на них. Реальні правові наслідки за відповідні діяння можуть настати лише за умови прийняття спеціальних нормативно-правових актів, які за основу братимуть засади і принципи, визначені Стратегією та Доктриною.

8. На нашу думку, протидія шкідливому інформаційному впливу повинна бути комплексною і узгодженою. Важливу роль в даному процесі відіграє взаємодія державних органів, засобів масової інформації та громадянського суспільства. Першочерговими кроками в боротьбі з поширенням деструктивного інформаційного впливу повинно бути: формування дезінформаційного імунітету в суспільстві шляхом навчання, консультацій, просування українських наративів; розробка чітких правових механізмів реагування на поширення дезінформації; створення системи саморегуляції журналістського середовища; активна участь громадянського суспільства у фактчекінгових ініціативах, їх співпраця з міжнародними організаціями.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Черниш Р.Ф., Осічнюк Л.І. Національні інтереси держави та можливість обмеження права на свободу слова: питання співвідношення. Проблеми законності. 2021. № 155. С. 77-89.
2. Etymology Corner – Collins Word of the Year 2017. URL: <https://blog.collinsdictionary.com/language-lovers/etymology-corner-collins-word-of-the-year-2017/> (дата звернення 05.12.2021).
3. Merriam-Webster. (n.d.). Disinformation. In Merriam-Webster.com dictionary. Retrieved November 29, 2021. URL: <https://www.merriam-webster.com/dictionary/disinformation> (дата звернення 05.12.2021).
4. Herbert Romerstein. Disinformation as a KGB Weapon in the Cold War // Journal of Intelligence History. — 2001. — Т. 1. — С. 54-67. — DOI:10.1080/16161262.2001.10555046. URL: <https://www.tandfonline.com/doi/abs/10.1080/16161262.2001.10555046> (дата звернення 05.12.2021).
5. История российской внешней разведки: Очерки: в 6т. / Международные отношения. Москва, 2014. Т. 2: 1917-1933 годы / глав. ред. Е.М. Примаков. 272с.
6. Контрразведовательный словарь КГБ / под ред. В.Ф. Никитченко (ответственный редактор), П.С. Дмитриева (ответств. секретарь) и др. Научно-издательский отдел КГБ. Москва, 1972.
7. Пачепа И.М., Рычлак Р. Дезинформация. Тайная стратегия абсолютной власти. Москва, 2016. 526 с.
8. Засурский Я.Н. Техника дезинформации и обмана. Москва: Книга по Требованию, 2013. 244 с. URL: <https://www.bookvoed.ru/files/3515/10/90/25.pdf> (дата звернення 05.12.2021).
9. Cambridge dictionary. Значение disinformation в английском. URL: <https://dictionary.cambridge.org/ru/%D1%81%D0%BB%D0%BE%D0%B2%D0%B0%D1%80%D1%8C/%D0%B0%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9/disinformation> (дата звернення 05.12.2021).

10. EU Code of Practice on Disinformation. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454 (дата звернення 05.12.2021).

11. Joint declaration on freedom of expression and “fake news”, disinformation and propaganda. FOM.GAL/3/17 3 March 2017. URL: <https://www.osce.org/files/f/documents/6/8/302796.pdf> (дата звернення 05.12.2021).

12. Дезінформація и свобода мнень и их свободное выражение: Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнень и их свободное выражение Айрин Хан. 2021. URL: <https://undocs.org/ru/A/HRC/47/25> (дата звернення 05.12.2021).

13. Misinformation vs. Disinformation: Get Informed On The Difference. URL: <https://www.dictionary.com/e/misinformation-vs-disinformation-get-informed-on-the-difference/> (дата звернення 05.12.2021).

14. Кіца М. Особливості та методи виявлення фейкової інформації в українських ЗМІ. URL: <http://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/16109/kitsa.pdf> (дата звернення 05.12.2021).

15. Про протидію дезінформації: законопроект. URL: <https://mkp.gov.ua/files/InformPolityka.pdf> (дата звернення 05.12.2021).

16. Український законопроект про дезінформацію не буде ефективним. URL: <https://tinyurl.com/ydj3h48c> (дата звернення 05.12.2021).

17. Украинка, распространявшая фейк про «распятого мальчика», теперь жалуется на жизнь в РФ. URL: <https://nv.ua/ukraine/politics/chto-sluchilos-s-zhenshchinoy-kotoraya-zayavila-o-raspyatom-malchike-na-donbasse-video-50153557.html> (дата звернення 05.12.2021).

18. Савва Терентьев проти Росії (Savva Terentyev V. Russia): рішення ЄСПЛ №10692/09 від 24.08.2018. URL: <https://cedem.org.ua/library/savva-terentyev-proty-rosiyi-savva-terentyev-v-russia/> (дата звернення 01.12.2021).

19. Trump's election lies were among his most popular tweets. 2021. URL: <https://www.cnn.com/2021/01/13/trump-tweets-legacy-of-lies-misinformation-distrust.html> (дата звернення 01.12.2021).

20. Наявність мови ворожнечі має аналізуватися залежно від конкретної справи – ЄСПЛ. URL: <https://cedem.org.ua/news/nayavnist-movy-vorozhnechi-maye-analizuvatysya-zalezjno-vid-konkretnoyi-spravy-yespl/> (дата звернення 05.12.2021).

21. Market Insights Trust In Media 2020. Media Intelligence Service. April 2020. URL: https://medienorge.uib.no/files/Eksterne_pub/EBU-MIS-Trust_in_Media_2020.pdf (дата звернення 01.12.2021).

22. Ставлення населення до ЗМІ та споживання різних типів медіа у 2020р.: щорічне опитування USAID-Internews. URL: <https://internews.in.ua/wp-content/uploads/2020/10/2020-Media-Consumption-Survey-FULL-FIN-Ukr-1.pdf> (дата звернення 01.12.2021).

23. Про транскордонне телебачення: Європейська конвенція ETS N 132. URL: https://zakon.rada.gov.ua/laws/show/994_444#Text (дата звернення 01.12.2021).

24. How Facebook Failed Voters and Nearly Set Democracy Aflame. 2021. URL: https://secure.avaaz.org/campaign/en/facebook_election_insurrection/ (дата звернення 01.12.2021).

25. Facebook bans deepfake videos ahead of the 2020 election. URL: <https://www.theverge.com/2020/1/7/21054504/facebook-instagram-deepfake-ban-videos-nancy-pelosi-congress> (дата звернення 05.12.2021).

26. Malicious Deep Fake Prohibition: Act of 2018 S. 3805. URL: <https://www.congress.gov/bill/115th-congress/senate-bill/3805/text> (дата звернення 05.12.2021).

27. Elections: deceptive audio or visual. Assembly Bill No. 730. URL: https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730 (дата звернення 05.12.2021).

28. A08155 Summary: Legislative information. URL: https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A08155&term=2017&Summary=Y&Actions=Y&Text=Y (дата звернення 05.12.2021).

29. Judgment Of The Court (Grand Chamber) / 1 October 2019 In Case C 673/17. URL: <https://curia.europa.eu/juris/document/document.jsf?docid=218462&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=17209953> (дата звернення 05.12.2021).

30. Coordinated Inauthentic Behavior Report. May 2021. URL: <https://about.fb.com/wp-content/uploads/2021/06/May-2021-CIB-Report.pdf> (дата звернення 05.12.2021).

31. Joint communication to the European Parliament and the council Joint Framework on countering hybrid threats a European Union response. URL: <http://bit.ly/2t0uwSh> (дата звернення 01.12.2021).

32. Золотухін Д. Протидія інформаційній агресії Росії на рівні законодавчих актів: Резолюція Європарламенту. URL: <http://bit.ly/2mVqXzW> (дата звернення 01.12.2021).

33. Кодекс практики Європейського Союзу щодо протидії дезінформації: Неофіційний переклад. URL: https://www.nrada.gov.ua/wp-content/uploads/2019/09/Kodeks-praktyky-YES-shhodo-protydiyidezy_pereklad.docx (дата звернення 05.12.2021).

34. Finland is winning the war on fake news. What it's learned may be crucial to Western democracy. URL: <https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/> (дата звернення 05.12.2021).

35. Democracy hacked? How to respond: Resolution 2326 (2020). URL: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=28598&lang=en> (дата звернення 05.12.2021).

36. Про ролі та обов'язки Інтернет-посередників: Рекомендація CM/Rec(2018)2 Комітету Міністрів державам-членам Ради Європи від 07.03.2018. URL: <https://thedigital.gov.ua/storage/uploads/files/>

normative_document/archive/5bcf04496e848695859521.pdf (дата звернення 05.12.2021).

37. Щодо впливу алгоритмічних систем на права людини: Рекомендація СМ / Rec (2020) 1 Комітету Міністрів державам-членам Ради Європи від 08.04.2020. URL: <https://www.echr.com.ua/document/rekomendaciya-sm-rec-20201-vid-08-04-2020/> (дата звернення 05.12.2021).

38. Як Євросоюз протидіє російській пропаганді. URL: <http://icps.com.ua/yak-vrosoyuz-protydi-rosiyskiy-propahandi/> (дата звернення 01.12.2021).

39. The European Centre of Excellence for Countering Hybrid Threats. URL: <https://www.hybridcoe.fi/about-us/> (дата звернення 05.12.2021).

40. Як у ЄС протидіють дезінформації Кремля, а як в Україні? URL: <https://www.radiosvoboda.org/a/29262016.html> (дата звернення 05.12.2021).

41. Черниш Р. Правовий досвід країн європейського союзу у сфері протидії поширенню фейкової інформації. Підприємництво, господарство і право. 2019. № 10. С. 123-128. URL : <http://pgp-journal.kiev.ua/archive/2019/10/22.pdf> (дата звернення: 13.11.2021).

42. Facebook and Twitter Could Face Fines in Germany Over Hate Speech Posts. URL : <https://www.nytimes.com/2017/03/14/technology/germany-hate-speech-facebook-tech.html> (дата звернення 01.12.2021).

43. Zwei Millionen Euro Strafe für Facebook. URL: <https://www.zdf.de/nachrichten/heute/facebook-soll-zwei-millionen-euro-strafe-zahlenwegen-verstoss-gegen-netzdg-100.html> (дата звернення 01.10.2019).

44. Le CSA promet de surveiller «constamment» la chaîne russe RT. URL: <http://bit.ly/2DZnK5U> (дата звернення 05.12.2021).

45. Against information manipulation. URL: <https://www.gouvernement.fr/en/against-information-manipulation> (дата звернення 05.12.2021).

46. «Стоп-фейк» по-французьки: парламент ухвалив жорсткий закон. URL: <https://www.ukrinform.ua/rubric-world/2585916-stop-fejkpofrancuzki-parlament-uhvaliv-zorstkij-zakon.html> (дата звернення 01.12.2021).

47. Disinformation and ‘fake news’: Final Report House of Commons / Digital, Culture, Media and Sport Committee / Eighth Report of Session 2017–19 / Report, together with formal minutes relating to the report / Ordered by the House of Commons to be printed 14 February 2019. URL: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcmds/1791/1791.pdf> (дата звернення 01.12.2021).

48. Online Harms White Paper: Department for Digital, Culture, Media & Sport and Home Office. 8 April 2019. URL: <https://www.gov.uk/government/consultations/online-harms-white-paper> (дата звернення 01.12.2021).

49. National Security Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf (дата звернення 01.12.2021).

50. National Security Capability Review / Including the second annual report on implementation of the National Security Strategy and Strategic Defence and Security Review 2015. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf (дата звернення 01.12.2021).

51. About the NCSC. URL: <https://www.ncsc.gov.uk/section/about-ncsc/what-we-do> (дата звернення 01.12.2021).

52. New national security unit set up to tackle fake news in UK. URL: <https://www.theguardian.com/politics/2018/jan/23/new-national-security-unit-will-tackle-spread-of-fake-news-in-uk> (дата звернення 01.12.2021).

53. Маляренко В.І. Кращі практики зарубіжного досвіду боротьби з фейками та дезінформацією. Інформація і право. 2021. №3(38). С. 21-27. DOI: [https://doi.org/10.37750/2616-6798.2021.3\(38\).243793](https://doi.org/10.37750/2616-6798.2021.3(38).243793).

54. У Сінгапурі ухвалили закон проти фейків і маніпуляцій. URL: <https://detector.media/infospace/article/167132/2019-05-09-u-singapuri-ukhvalyly-zakon-proty-feykiv-i-manipulyatsiy/> (дата звернення 01.12.2021).

55. Уголовный кодекс Республики Казахстан: Закон № 226-V ЗРК от 03.07.2014. По состоянию на: 02.07.2021. URL: https://online.zakon.kz/Document/?doc_id=31575252&sub_id=2740000&pos=4045;-54#pos=4045;-54 (дата звернення 01.12.2021).

56. Протидія дезінформації: європейські підходи та стандарти. 2021. URL: <https://www.coe.int/uk/web/kyiv/-/responding-to-disinformation-european-practices-and-standards> (дата звернення 01.12.2021).

57. Конвенція про захист прав людини і основоположних свобод від 04.11.1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення 05.11.2021).

58. Обмеження свободи слова во благо: за і проти. URL: <https://video.detector.media/reports/obmezheniya-svobody-slova-vo-bлаго-za-i-proty-i708> (дата звернення 05.11.2021).

59. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 р. № 537-V. URL: <https://zakon.rada.gov.ua/laws/show/537-16#Text> (дата звернення: 05.11.2021).

60. Про телебачення і радіомовлення : Закон України від 21.12.1993 р. № 3759-XII. Дата оновлення: 23.07.2021. URL: <https://zakon.rada.gov.ua/laws/show/3759-12#Text> (дата звернення: 09.11.2021).

61. Про друковані засоби масової інформації (пресу) в Україні : Закон України від 16.11.1992 р. № 2782-XII. Дата оновлення: 03.07.2020. URL: <https://zakon.rada.gov.ua/laws/show/2782-12#top> (дата звернення: 09.11.2021).

62. Про кінематографію : Закон України від 13.01.1998 р. № 9/98-ВР. Дата оновлення: 16.10.2020. URL: <https://zakon.rada.gov.ua/laws/show/9/98-%D0%B2%D1%80#top> (дата звернення: 09.11.2021).

63. Про видавничу справу : Закон України від 05.06.1997 р. № 318/97-ВР. Дата оновлення: 16.10.2020. URL: <https://zakon.rada.gov.ua/laws/show/318/97-%D0%B2%D1%80#top> (дата звернення: 09.11.2021).

64. Конституція України від 28.06.1996 р. № 254к/96-ВР. Дата оновлення: 01.01.2020. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> (дата звернення 01.11.2021).

65. Про інформацію: Закон України від 02.10.1992 р. № 2657-ХІІ. Дата оновлення: 16.07.2020. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#top> (дата звернення: 10.11.2021).

66. Про рішення Ради національної безпеки і оборони України від 2 лютого 2021 року Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій) : Указ Президента України від 02.02.2021 р. № 43/2021. URL: <https://www.president.gov.ua/documents/432021-36441> (дата звернення: 10.11.2021).

67. США та ЄС підтримали санкції проти Козака та каналів «112-Україна», ZIK та NewsOne. URL: <https://suspilne.media/101828-ssa-pidtrimali-sankcii-proti-kozaka-ta-jogo-telekanaliv/> (дата звернення: 10.11.2021).

68. Цивільний кодекс України : Закон України від 16.01.2003 р. № 435-ІV. Дата оновлення: 06.10.2021. URL: <https://zakon.rada.gov.ua/laws/show/435-15#top> (дата звернення: 11.11.2021).

69. Кодекс України про адміністративні правопорушення : Закон України від 07.12.1984 р. № 8073-Х. Дата оновлення: 01.10.2021. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text> (дата звернення: 11.11.2021).

70. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. Дата оновлення: 04.11.2021. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#top> (дата звернення: 11.11.2021).

71. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 р. № 183/98-ВР. Дата оновлення: 11.01.2019. URL: <https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#top> (дата звернення: 13.11.2021).

72. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року Про створення Центру протидії дезінформації: Указ Президента України від 19.03.2021 р. № 106/2021. URL: <https://www.president.gov.ua/documents/1062021-37421> (дата звернення: 13.11.2021).

73. Питання Центру протидії дезінформації : Указ Президента України від 07.05.2021 р. № 187/2021. URL: <https://www.president.gov.ua/documents/1872021-38841> (дата звернення: 13.11.2021).

74. Про санкції : Закон України від 14.08.2014 р. № 1644-VII. Дата оновлення: 01.07.2021. URL: <https://zakon.rada.gov.ua/laws/show/1644-18#top> (дата звернення: 13.11.2021).

75. Про затвердження Положення про Міністерство культури України : Постанова Кабінету Міністрів України від 03.09.2014 р. № 495. Дата оновлення: 30.08.2019. URL: <https://zakon.rada.gov.ua/laws/show/495-2014-%D0%BF#Text> (дата звернення: 14.11.2021).

76. Презентовано Центр стратегічних комунікацій та інформаційної безпеки. URL: <https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki> (дата звернення: 05.12.2021).

77. РНБО схвалила план оборони України, стратегії інформаційної безпеки, біобезпеки та біологічного захисту, застосувала санкції щодо деяких фізичних і юридичних осіб. URL: <https://www.rnbo.gov.ua/ua/Diialnist/5085.html> (дата звернення: 05.12.2021).

78. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року Про Доктрину інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017. URL: <https://www.president.gov.ua/documents/472017-21374> (дата звернення: 05.12.2021).

79. Про рішення Ради національної безпеки і оборони України від 2021 року Про Стратегію інформаційної безпеки: проект Указу Президента України. URL: <https://mkip.gov.ua/files/pdf/45698712365.pdf> (дата звернення: 05.12.2021).