ТЕОРІЯ ТА ІСТОРІЯ ДЕРЖАВИ І ПРАВА

УДК 344.77(477)
DOI https://doi.org/10.32782/39221495

Атаманова Н. В.,
кандидат юридичних наук, доцент,
доцент кафедри державно-правових дисциплін
Міжнародного гуманітарного університету

ЗАСОБИ ПРОТИСТОЯННЯ ІНФОРМАЦІЙНИМ ФЕЙКАМ У СУЧАСНІЙ ДЕРЖАВІ

MEANS OF COMBATING INFORMATION FAKES IN THE MODERN STATE

У статті йдеться про сутність і поняття терміну «фейк». Фейк визначили як різновид інформаційної зброї точкової спрямованості. Виявили, що з розвитком мережі Інтернет та соціальних мереж, аудиторія яких обчислюється десятками тисяч, а часом і мільйонами, поширення «фейкових» новин перетворюється на епідемію. Доведено, що із введенням в оману, фейки можуть призначатися для інформаційно-психологічного впливу на цільову аудиторію або пропаганди певних поглядів в інтересах надання впливу на когнітивні здібності (сприйняття, мислення, свідомість та пам'ять), емоційний стан, переконання, позицію і, в результаті на діяльність об'єктів впливу. До основних способів введення в оману чи дезінформування віднесли такі об'єкти впливу: повідомлення або передача свідомо неправдивої інформації; повідомлення чи передача необхідним чином зміненої (спотвореної) правдивої інформації; маніпулювання правдивою інформацією під час її безпосереднього повідомлення чи передачі. Визначено різновиди і шляхи поширення фейкових новин та їх вплив на сучасну державу. Середовищем поширення фейків є соціальні медіа та засоби масової інформації. Дізнались, що незалежно від виду фейку його застосування являє собою комплекс заходів організаційного та технічного характеру щодо створення (підготовки, виробництва) та поширення хибної інформації в соціальних медіа та ЗМІ на користь введення користувачів – об'єктів впливу – в оману. Дійшли висновку, що найпотужніша зброя проти фейків – це критичне мислення та фактчекінг, тобто здійснення перевірки фактів. Важливо визначити першоджерело інформації, це може бути державний орган, відео з камер спостереження, дослідження чи конкретний речник. Виявили, що існують професійні фактчекери, які спеціалізуються на перевірці достовірності інформації. Досліджено засоби протистояння фейкам органами держави. Дізнались, що для боротьби з фейками почали застосовувати технологію блокчейн – ланцюжок зв'язаних блоків даних, збудованих за певними правилами. Така технологія визначатиме, хто, коли, як і де створив контент, а також чи він піддавався змінам і де був опублікований.

***Ключові слова**: фейк, фейкові матеріали, інформаційні фейки, інформаційна війна, протидія фейкам.*

The article deals with the essence and concept of the term "fake". A fake was defined as a type of point-directed information weapon. It was discovered that with the development of the Internet and social networks, the audience of which is calculated by tens of thousands, and sometimes even millions, the spread of "fake" news turns into an epidemic. It has been proven that with misleading information, fakes can be intended for informational and psychological influence on the target audience or propaganda of certain views in the interests of influencing cognitive abilities (perception, thinking, consciousness and memory), emotional state, beliefs, position and, as a result, on the activity of objects of influence. The main methods of misleading or misinforming included the following objects of influence: notification or transmission of deliberately false information; communication or transmission of the necessary changed (distorted) true information; manipulation of true information during its direct communication or transmission. The types and ways of spreading fake news and their impact on the modern state are determined. The environment for the spread of fakes is social media and mass media. We learned that regardless of the type of fake, its use is a set of measures of an organizational and technical nature related to the creation (preparation, production) and dissemination of false information in social media and mass media for the benefit of misleading users – objects of influence. They came to the conclusion that the most powerful weapon against fakes is critical thinking and fact-checking, that is, checking facts. It is important to identify the original source of the information, whether it is a government agency, surveillance video, research, or a specific spokesperson. We discovered that there are professional fact-checkers who specialize in checking the reliability of information. The means of countering fakes by the state bodies have been studied. We learned that blockchain technology – a chain of linked data blocks built according to certain rules – was used to combat fakes. Such technology will determine who, when, how and where the content was created, as well as whether it was modified and where it was published.

***Key words:** fake, fake materials, informational fakes, information war, countering fakes.*

Вступ. В сучасній державі інформаційні фейки за ступенем ефективності застосовуються для досягнення військових, економічних і політичних цілей. Фейкову інформацію використовують, щоб підвищити медіатрафік, сформувати громадську думку, дискредитувати конкурента чи публічну людину. Саме фейки стали потужним інструментом впливу і набули нової сили в цифрову еру. Характерно, що кількість хибних новин значно зростає під час політичних кампаній, воєнних конфліктів та кризових ситуацій. Звичайно відстежити кожну фіктивну новину неможливо. Більше того, хибні публікації виглядають досить реалістичними. Вони містять багато правдивих деталей, фіктивні посилання на джерела та коментарі публічних людей. Ще одна вразливість закладена в людській природі – людям властиво довіряти вигаданим історіям, якщо вони збігаються з їхнім світоглядом. До того ж, аудиторія має великий інтерес до гарячих чуток та пікантних подробиць. Захиститись і протистояти хибній інформації вкрай складно без інноваційних технологій, які допоможуть людині ідентифікувати фейковий контент.

Аналіз останніх досліджень і публікацій. Дослідженням фейків як одного із інструментів негативного впливу на суспільство і країну зокрема займались такі фахівці як В.М. Вовк, Д. Ю. Золотухін, В. Гладких, Р. Ф. Черниш тощо. Проте дане питання є швидкорозвиваючим елементом і потребує постійного вивчення.

Метою статті є аналіз засобів протистояння інформаційним фейкам у сучасній державі.

При дослівному перекладі з англійської «fake» означає підробка, обман або фальшивка. У першу чергу, він розглядається як інтернет-термін, який вживається стосовно підробленої новини, інформаційного повідомлення або іншого контенту користувача (user-generated content), спеціально підготовленого для поширення в соціальних медіа та електронних ЗМІ помилкової інформації під виглядом достовірної та розрахованої на введення в оману об'єктів впливу. Цей термін вживається і фахівцями інших країн у рамках військової дезінформації (military deception) – діяльності з цілеспрямованого введення в оману ймовірного чи реального супротивника шляхом «надання» йому свідомо хибної або необхідним чином зміненої правдивої інформації, а також шляхом маніпулювання нею в ході безпосереднього повідомлення (передачі) [8]. Мета військової дезінформації полягає у спонуканні противника до бездіяльності або виконання дій, що сприяють успішному виконанню завдань своїми військами (силами). Саме так РФ ще з 2014 р. з розв'язанням конфлікту на Донбасі, анексією Криму, а з 24 лютого 2022 р. в зв'язку з повномасштабним військовим вторгненням на території України розпочала активну інформаційну операцію з розповсюдженням фейків.

Фейк можна охарактеризувати як різновид інформаційної зброї точкової спрямованості. З розвитком мережі Інтернет та соціальних мереж, аудиторія яких обчислюється десятками тисяч, а часом і мільйонами, поширення «фейкових» новин перетворюється на епідемію.

Поняття «fake» стало основою появи наступних термінологічних словосполучень: фейкові матеріали (fake materials), зокрема документи (fake documents); фейкові тексти (fake texts), включаючи історії (fake narratives) та оповідання (fake stories); фейкові повідомлення (fake announcements) та заяви (fake allegations); фейкові новини (fake news); фото- (fake photo), відео- (fake video) та аудіо- (fake audio) фейк; фейкові сторінки (fake page) та обліковий запис (fake account).

Серед всього найпоширенішими і найвпливовішими є фейкові новини, які з'явилися за кордоном у 2017 році, коли цей термін було внесено до тлумачного словника англійської мови Collins English Dictionary з визначенням «неправдива, найчастіше сенсаційна інформація, що розповсюджується під виглядом повідомлень новин». В 2018 році Оксфордський університет вніс його до свого словника: «фейкові новини – це хибна інформація, яка передається або публікується під виглядом новин з метою обману або з політичних міркувань». Крім того, серед зарубіжних фахівців у галузі інформаційних операцій використовується класифікація фейків за якістю їхньої підготовки. Так, вони поділяються на низькоякісні (cheapfakes) та високоякісні (deepfakes) [7]. На сьогодні у США та інших країнах відбувається уніфікування понятійно-категоріального апарату в аналізованої сфері.

Загалом фейк незалежно від його виду необхідно вважати інструментом введення в оману

(дезінформування) об'єктів впливу (цільові аудиторії). І середовищем поширення фейків є соціальні медіа та засоби масової інформації (ЗМІ). При цьому до соціальних медіа віднесено: соціальні мережі і месенджери, блоги та блог-платформи, інтернет-портали спільного використання контенту та інші цифрові майданчики щодо обміну інформацією між користувачами, а до ЗМІ – телебачення, радіо, газетні та журнальні видання.

Таким чином, слід виділити такі основні способи введення в оману (дезінформування) об'єктів впливу – цільової аудиторії:

– повідомлення або передача свідомо неправдивої інформації;

– повідомлення чи передача необхідним чином зміненої (спотвореної) правдивої інформації;

– маніпулювання правдивою інформацією під час її безпосереднього повідомлення чи передачі.

В даному випадку фейки спрямовані на дестабілізацію ситуації в країні, поширення панічних настроїв, а опосередковано, знову ж таки, призводять людей до висновків про неефективність держави та провокують думки про доцільність зміни державної влади чи конституційного ладу.

Одночасно із введенням в оману, фейки можуть призначатися для інформаційно-психологічного впливу на цільову аудиторію або пропаганди певних поглядів в інтересах надання впливу на когнітивні здібності (сприйняття, мислення, свідомість та пам'ять), емоційний стан, переконання, позицію і, в результаті на діяльність об'єктів впливу. Самі явища пропаганди, дезінформації описав Е. Тоффлер в праці «Війна та антивійна» [8]. Адже поширення інформаційних фейків в сучасній війні є закономірним продуктом економіки так званої Третьої хвилі за Е. Тоффлер, що ґрунтується на знанні у широкому значенні слова, що містить інформацію, символи, зображення, дані, культуру, систему цінностей й ідеологію [8].

Останнім часом користувачі воліють дізнаватися новини в мережі Інтернет, соціальних мереж та різних месенджерів. Такі новини поширюються від людини до людини, з однієї соціальної мережі до іншої, а їх правдивість рідко цікавить читачів і сприймається «на віру». Специфіка «фейкових» новин визначається її спрямованістю на певні, конкретні групи людей та впровадження конкретних психологічних установок, маніпуляції громадською думкою та настроєм. Потенційна небезпека такої зброї полягає у дестабілізації політичного становища держави та створення негативного іміджу країни.

З огляду на це немає нічого дивного в тому, що повномасштабна агресія РФ проти України, також включає і великий пласт інформаційної війни, яка щодень набирає обертів.

Насамперед це поширення фейків, з допомогою яких відбувається маніпулювання громадською думкою, свідомістю людей, створення спотвореної картини подій. За оцінками кіберфахівців, приблизно 70% деструктивних матеріалів про Україну просуваються саме з інформаційного простору РФ, зокрема російських соцмереж.

Механізм впливу фейками ґрунтується на споживчому інтересі. Практично кожна особа проводить значну частину свого часу в так званому інформаційно-комунікаційному просторі – одному із головних інформаційних середовищ. Поведінка у ній корелює не із об'єктивною інформацією про явища і події, що відбуваються у сфері його інтересів, а з комунікативною інформацією, що містить підготовлену (тобто чужу) думку. Як зазначають фахівці, застосування фейків дозволяє «проникнути» в уже існуюче або сконструювати нове інформаційне середовище, пов'язане з певним об'єктом впливу (управління), щодо якого це середовище розглядається [2].

Значний сплеск активності агітаторів, тролета ботоферм в інфополі відбувається за активізації внутрішніх політичних подій в Україні, напередодні колишніх радянських, сучасних українських чи релігійних свят. Найчастіше такі фейки мають ознаки посягання на територіальну цілісність та недоторканність України, дії, спрямовані на насильницьку зміну конституційного ладу чи захоплення державної влади, а також створення терористичних груп.

В умовах демократії інформація відіграє таку ж роль, як насильство в умовах репресивних режимів відзначає політичний експерт В. Гладких. Адже на тлі достатньої кількості прикладів, коли вміло використовуючи інформацію, можна впливати на поведінку людей

не гірше, ніж використовуючи насильство чи загрозу його застосування. Більше того, за допомогою інформації можна впливати на поведінку значно більшої кількості людей, аніж за допомогою безпосередньо фізичного насильства, і коштує це значно дешевше, бо зміст репресивного апарату – недешеве задоволення. А головне, на відміну від насильства, ніхто не сперечатиметься про легітимність використання таких інструментів [3]. Саме це стосується розповсюдження фейків.

Для введення в оману цільової аудиторії буває достатньо поодиноких фейків. Для маніпулювання емоційним станом, надання істотного впливу на когнітивні здібності, переконання, позицію, і в кінцевому рахунку діяльність цільової аудиторії необхідна сукупність фейків та їх регулярне «тиражування» в ході так званих інформаційних кампаній. Усе це дозволяє сформувати потрібну інформаційну реальність. Для гарантованого переконання користувачів у «затребуваності» фейкового контенту та авторитеті його творців можуть бути використані різні способи. Наприклад, у соціальних медіа може здійснюватися симуляція активності цільової аудиторії шляхом купівлі на спеціальних біржах та сервісах лайків, передплат, репостів, коментарів та інших показників залучення користувачів. З цією ж метою може створюватися мережа адміністрованих фейкових облікових записів. Для виключення підриву довіри до інформації розповсюдження та створення «затребуваності» фейкового контенту здійснюється під зовнішнім управлінням [6, с.111]. Зокрема це дозволяє уникнути зайвої «агресивності» або нав'язливості в його доведенні до користувачів.

Те саме стосується й ефективності використання інформації для досягнення цілей у зовнішньополітичній діяльності. Причому, порівняно з військовими діями використання інформації як зброї дешевше, безпечніше, а іноді й набагато ефективніше. Варто погодитися, що використовуючи військову силу, РФ навряд чи змогла б втрутитися у перебіг американських виборів.

Незалежно від виду фейку його застосування являє собою комплекс заходів організаційного та технічного характеру щодо створення (підготовки, виробництва) та поширення хибної інформації в соціальних медіа та ЗМІ на користь введення користувачів – об'єктів впливу – в оману.

Усвідомлення цього факту призвело до розробки та широкого використання методів, сукупність яких отримали назву «інформаційних та психологічних воєн». Після стрімкого розвитку засобів масової комунікації та інформаційних технологій «інформаційно-психологічні війни» стали самодостатніми. Причому їх почали застосовувати не лише у міждержавних відносинах, а й у внутрішньомережевій політичній боротьбі та бізнесі.

Найпотужніша зброя проти фейків – це критичне мислення та фактчекінг (перевірка фактів). Коли ж новина викликає бурхливі емоції чи в свою чергу шокує, то це перша ознака засумніватись. Важливо визначити першоджерело інформації, це може бути державний орган, відео з камер спостереження, дослідження чи конкретний речник. Якщо подібних заяв ніде немає, мабуть, що матеріал фейковий. Уважно варто поставитись і до новин із посиланнями на приховані джерела, без згадки про конкретну особу чи організацію. Закон дозволяє журналістам не розкривати ім'я інформатора з професійних переконань чи безпеки. Але на практиці це швидше виняток із правил при висвітленні резонансних справ авторитетними ЗМІ. Саме тому варто перевіряти унікальність домену сайту, адже популярні медіа дуже часто копіюють, додаючи до веб-адреси зайві символи, наприклад, Fox-news24.com, Bloomberg.ma або Washingtonpost.com.co. Водночас слід звертати увагу на репутацію самого ресурсу [3]. Зазвичай ЗМІ, які розповсюджують фейки, дуже швидко втрачають довіру аудиторії.

Існують професійні фактчекери, які спеціалізуються на перевірці достовірності інформації. Але покладатися виключно на людський ресурс – це дуже повільний процес, адже програма зможе опрацювати більше контенту за менші терміни. Для боротьби з фейками вже почали застосовувати технологію блокчейн – ланцюжок зв'язаних блоків даних, збудованих за певними правилами. Технологія визначатиме, хто, коли, як і де створив контент, а також чи він піддавався змінам і де був опублікований. Видання The New York Times вже запустило пілотний проект із використанням блокчейн,

спочатку система ідентифікуватиме виключно фейкові фото [7].

Фейкова інформація у соціальних мережах поширюється вшестеро швидше, ніж правдива. Саме тут варто згадати про боти, але американські дослідники однією з головних причин назвали саме репости реальних людей. При цьому охоплення хибних історій, в середньому, на 35% вищі за реальні. Секрет у тому, що фейкові новини за своєю природою сенсаційніші, а їхній емоційний градус спонукає користувачів зробити репост без перевірки інформації. Без сумнівів, ботів і далі продовжують використовувати для розкручування фейкових новин, вони впливають на громадську думку, дискредитують погляди, зміщують акценти, атакують в інтернеті конкурентів. Приміром, лише для тиску на учасників конкурсу «Євробачення 2018» із метою змусити їх відмовитись від поїздки до Ізраїлю використали 232 фіктивні облікові записи в Twitter. Вони змогли охопити аудиторію у 10 мільйонів користувачів [3]. Ще одне завдання ботів – надати публікації чи ресурсу кількісну підтримку у вигляді лайків, репостів та коментарів, щоб усе менше людей змогли поставити інформацію під сумнів. Тут працює концепція «спіралі мовчання», коли людина з меншою ймовірністю висловить протилежну думку, якщо вона перебуває в меншості. Крім роботів, для виконання аналогічної роботи сьогодні наймають і реальних людей, задум яких набагато складніше викрити, оскільки вони діють унікально.

Інформаційні фейки емоційно забарвлені і мають так звані «емоційні гачки», які спрацьовують через деякий час стверджує В.М. Вовк. І щодо стратегічного рівня, то він насамперед залежить від державної політики і діяльності всіх державних інституцій, й зокрема їх здатності до оперативної і довгострокової роботи стосовно протидії фейкам [1, с. 83].

Тому варто виділити кілька напрямів діяльності держави у протидії фейкам.

1. Задля забезпечення поширення достовірної інформації і протидії фейкам ще на початку повномасштабної війни РФ в Україні було утворено офіційні телеграм-канали голів облдержадміністрацій для висвітлення лише достовірної та актуальної інформації. Оскільки виправдання постфактум та відповідно спростування фейкової інформації, навпаки, у деякої частини населення тільки утверджують переконаність в непорядності органів влади, а також спонукають до конспірологічних пошуків, переконаності ц «достовірності» раніше одержаної інформації.

Так, Facebook, у свою чергу, вже розробляє інструменти для виявлення дезінформації та використовує машинне навчання для перевірки фото та відеоматеріалів. Спочатку алгоритми визначають вірусні та підозрілі пости, використовуючи аналіз метаданих, геометок та інших відомостей. Далі матеріали відправляють на перевірку професійним фактчекерам [3]. Якщо виявлено фейк, його розповсюдження зупиняють, а користувачі повідомляють про сумнівний контент. Одночасно з цим накопичується база навчальних даних для нейромережі, яка все краще справлятиметься зі своєю роботою і без людського втручання.

2. Поширення інформації ЗМІ. Так, досить актуальним стереотипом в сприйнятті інформації є довіра великої кількості людей до інформації, що поширюють ЗМІ. Приміром, така сліпа довіра до повідомлень ЗМІ призвела до того, що населення РФ вірить федеральним каналам більше, ніж своїм рідним, які живуть в Україні. Саме тому нагальною є розробка на законодавчому рівні елементів юридичного механізму протистояння фейкам і фейковим новинам, що можуть загрожувати національній безпеці країни і її громадян.

Якщо більшість ЗМІ дорожить репутацією і дотримується закону, то в соціальних мережах слід бути більш пильними. Щоб розпізнати повідомлення фейку, перевірити інформацію недостатньо. Слід також встановити автентифікацію облікового запису автора, дату створення сторінки, наявність друзів та проаналізувати контент.

3. На сучасному етапі мають існувати спеціальні органи держави або наділення додатковими повноваженнями й функціями вже наявні органи, що забезпечують боротьбу із інформаційними фейками. Так, в Україні на сьогодні функціонує Центр протидії дезінформації при РНБО, що виявляє фейки РФ як в національному, так і в міжнародному вимірі (прикладом цього є звіт від 27 жовтня 2022 року «Аналіз наративів пропагандистської публічної дипло-

матії РФ в країнах «Великої сімки») [4]. Водночас, у вересні 2022 року Центр протидії дезінформації подав ініціативу створити міжнародний хаб із протидії інформаційним загрозам в міжнародній площині [5].

Також в сучасній державі часто використовується DeepFake, яка модифікує відео та фото, змінюючи частини тіла, рухи та навіть мовлення часто досить популярної людини. І при створенні таких роликів, один аудіовізуальний контент накладають на інший. І якщо з появою технології в 2017 році такі фейки використовували для розваг, зараз це небезпечний інструмент у руках шахраїв. Наприклад, у березні 2022 р. директора британської енергетичної компанії пограбували на 220 тисяч євро, причому його руками. Він самостійно відправив всю суму угорській компанії за дорученням керівника, який особисто підтвердив завдання із відеозв'язку [4]. Ось тільки з жертвою в режимі реального часу тоді зв'язався шахрай, підробивши особу, міміку та голос під реального керівника компанії.

Головна загроза DeepFake – це знецінення фактів та доказів. Якщо зараз можна сподіватись на достовірність цих категорій, то в майбутньому всі опубліковані фото та відео потрібно ставити під сумнів. Адже їх могла згенерувати нейромережа [6, с. 111]. Звісно, подібні технології сприяють розвитку інформаційної війни. Якщо уявити, що DeepFake стане загальнодоступним, він буде затребуваним інструментом впливу на суспільство. Все, що потрібно – запрограмувати нейромережу на створення необхідного сценарію з будь-якою людиною на планеті. А соціальні мережі оперативно розповсюджуватимуть фейкові матеріали.

Наразі протидіють DeepFake, адже це складає національну небезпеку держави. Вже зараз нейромережі навчають як визначати правдивість згенерованого контенту. Потрібно визнати, що дана тема нескінченна: з удосконаленням технологій розпізнавання фейків розвиватимуться технології з їхнього створення. Раніше американські дослідники виявили, що на фейкових роликах спікери зазвичай не моргають, оскільки нейромережа рідко використовує фото людей із заплющеними очима. Але цей дефект алгоритмів DeepFake вже виправили. Фіктивне відео поганої якості набагато легше розпізнати. Насамперед, рекомендую відстежувати синхронність рухів губ та аудіоряду. Якщо вони не збігаються, швидше за все контент не оригінальний. Також варто звернути увагу на дрібні деталі, такі як пасма волосся, зуби та прикраси, їх все ще складно натурально підробити. Для боротьби із більш «глибокими фейками» вже оголосили масштабний Deepfake Detection Challenge. В конкурсі беруть участь дослідні групи, які опрацьовують алгоритми виявлення неправдивої інформації. Автори найкращих алгоритмів отримають гранти на загальну суму $10 мільйонів [7]. Боротися з дезінформацією варто кожному з членів суспільства, інформуючи соціальні мережі та браузери про сумнівний контент.

Цілком очевидно, що Служба безпеки України, яка, реалізуючи весь комплекс заходів щодо забезпечення інформаційної та кібербезпеки держави, протидіє кібертероризму, кібершпигунству, блокує хакерські атаки, спростовує фейки тощо, все одно самостійно не може повністю вирішити проблему протидії «гібридній агресії », яка продовжує активно проводитися РФ в інформаційному та кіберпросторі.

Висновки. Отже, для більш ефективної протидії необхідно не лише реформувати СБУ з урахуванням нових викликів, а й переосмислити принципи та підходи до регулювання роботи ЗМІ, особливо цифрових. А головне, треба переорієнтувати систему освіти на розвиток критичного мислення та формування навичок безпечної поведінки в океані інформації. Саме тому одним із нагальних питань, що стоять перед сучасним суспільством й потребує нагального розв'язання, є питання протистояння інформаційним фейкам та зменшення їх негативного впливу на цільового адресата для забезпечення національної безпеки. Окремі кроки з протидії фейкам передбачають: особиста відповідальність кожного з членів суспільства; медіаграмотність населення, законодавче регулювання; утворення спеціальних державних органів, центрів з протидії дезінформації; сформована комунікація державних органів з населенням тощо. Таким чином, дійшли висновку, що основною метою розповсюдження інформаційних фейків є контроль над інформаційним простором з метою формування певної громадської думки або настрою.

ЛІТЕРАТУРА:

1. Вовк В.М. Фейки як загроза національній безпеці в умовах гібридної війни. *Філософські та методологічні проблеми права*. 2022. № 2 (24). С. 80–84.

2. Золотухін Д. Ю. Біла книга спеціальних інформаційних операцій проти України 2014-2018. К., 2018. 384 с.

3. Гладких В. Теорія брехні та практика маніпуляцій: як РФ вкидає фейки в український інфопростір. *Слово і діло*. URL: 2020. https://ru.slovoidilo.ua/2020/09/15/kolonka/valentin-gladkix/politika/teoriya-lzhi-i-praktika-manipulyacij-kak-rf-vbrasyvaet-fejki-ukrainskoe-infoprostranstvo (дата звернення: 10.07.2023)

4. Центр протидії дезінформації при РНБО. URL: https://cpd.gov.ua/category/reports/# (дата звернення: 10.07.2023)

5. ЦПД при РНБО України ініціює створення міжнародного хабу з протидії інформаційним загрозам. *Рада національної безпеки і оборони України*: сайт. URL: https://www.rnbo.gov.ua/ua/Diialnist/5708.html. (дата звернення: 10.07.2023)

6. Черниш Р. Ф. Фейк як один із інструментів негативного впливу на національну безпеку України в умовах ведення гібридної війни. *Часопис Київського університету права.* 2019. № 2. С. 109–114.

7. Dice Mark The True Story of Fake News: How Mainstream Media Manipulates Millions. *The Resistance Manifesto*. 2017.

8. Toffler A. H. War and antiwar. URL: https://ia801301.us.archive.org/6/items/WarAndAntiWar-Toffler/War-AndAnti-War_-_Toffler.pdf. (дата звернення: 10.07.2023)