МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут «Інститут державного управління»

До захисту

Завідувач кафедри публічної політики

_____Дзюндзюк В.Б.

ДЕРЖАВНА ПОЛІТИКА ДЕЗІНФОРМАЦІЇ ТА МАНІПУЛЯЦІЯМ У ЦИФРОВОМУ ПРОСТОРІ

Кваліфікаційна робота на здобуття освітнього ступеня «магістр»

281 Публічне управління та адміністрування

28 Публічне управління та адміністрування

Виконавець здобувач ІІ курсу групи ППГД-23 _____О.О. Бабенко

Науковий керівник

к.е.н, проф. _____ В.Ф. Золотарьов

Харків – 2024

ЗМІСТ

ВСТУП

Актуальність теми. В умовах сучасних геополітичних подій і військових конфліктів вивчення феномену дезінформації та маніпуляції набуває особливої важливості, оскільки вони становлять серйозну загрозу національним інтересам країн.

Сьогодні з розвитком інформаційного суспільства, використовуючи інноваційні комп'ютерні технології, системи, мережі та сучасні засоби зв'язку, особливої уваги вимагають технології інформаційного впливу на особистість у різних сферах життя. Інформаційне суспільство сучасності відзначається тим, що інформація стала ключовим елементом у житті кожної людини, а цифровий простір зайняв майже весь вільний час. У умовах війни особливо важливим стає питання маніпулятивного впливу на громадську свідомість, яка може
проявлятися через дезінформацію, провокації, залякування та інші деструктивні методи. Велика кількість інформаційного контенту, яку споживають люди в цифровому просторі, створює сприятливі умови для маніпулювання масовою свідомістю.

Маніпулятивні технології та використання дезінформаційної інформації в умовах збройної агресії проти України використовуються як базові технології реалізації стратегії інформаційної війни. Актуальність зазначеної проблеми дієвого використання інструментів для боротьби з поширенням неправдивої інформації та їх негативним впливом на суспільну думку обумовлена необхідністю захисту інформаційного простору від маніпуляцій і дезінформації.

В українській та світовій дослідницькій літературі проблеми маніпулювання та дезінформації активно досліджували такі учені, як: П. Барановська, В. Бондар, А. Блінкін, В. Брижко, І. Вільчинська, В. Галіпчак, С. Глобенко, О. Дзьобань, О.

Євсюкова, А. Колдомасов, К. Кузьменкова, І. Мудра, М. Моліна О. Півторак, В. Фурашев, та ін.

Актуальність теми дослідження зумовлена відсутністю достатнього теоретичного обґрунтування принципів формування державної політики в сфері боротьби з дезінформацією та маніпуляціями в цифровому просторі, а також недостатністю розроблених практичних рекомендацій щодо їх удосконалення в умовах цифровізації публічного управління. Таким чином, визначена потреба в ефективній боротьбі з дезінформацією маніпуляцією вимагає удосконалення напрямів державної політики в цій сфері.

Мета магістерського дослідження полягає у теоретичному обґрунтуванні засад вироблення державної політики у сфері

Для досягнення поставленої мети було сформульовано наступні *завдання*:

- з'ясувати основні дефініції понятійно-категорійного апарату у сфері протидії дезінформації та маніпуляціям;
- проаналізувати інституційно-правові засади державної політики у сфері захисту інформаційного простору України;
- оцінити сучасний стан громадської думки у сфері протидії дезінформації;
- систематизувати світовий досвід протидії інформаційним впливам;
- визначити основні напрями посилення безпеки в інформаційному просторі України.

Об'єктом дослідження є система заходів забезпечення національної безпеки в цифровому просторі в Україні.

Предметом дослідження є державна політика протидії дезінформації та маніпуляціям у цифровому просторі.

Методи дослідження. Для реалізації визначеної мети та поставлених завдань дослідження автором використано комплекс загальних та спеціальних 5
методів наукового пізнання, зокрема: метод узагальнення та систематизації теоретичних джерел і нормативно-правових документів – для здійснення аналізу

національних програм, законодавчих актів, стратегій при регулюванні процесів формування державної політики протидії дезінформації та маніпуляціям; порівняльний метод – вивчення громадської думки щодо процесів поширення дезінформації та застосування маніпулятивного впливу; загальнонауковий та спеціальний методи – розроблення ефективних напрямів удосконалення протидії дезінформації з урахуванням теоретичних, нормативно-правових, соціальних аспектів; метод порівняльно-правового аналізу – дослідження світового досвіду та можливостей його імплементації у державну практику; метод узагальнення – формування висновків і результатів дослідження.

Методологічною основою дослідження є наукові праці вітчизняних і зарубіжних учених. Нормативно-правовою базою дослідження є Конституція України, Закони України, укази Президента України, постанови Кабінету Міністрів України, інші нормативно-правові акти державних і публічноуправлінських інституцій, вітчизняні та міжнародні статистичні й аналітичні матеріали.

Практична значення отриманих результатів дослідження полягає в тому, що основні науково-теоретичні положення, висновки та практичні рекомендації даного дослідження можуть бути використані у діяльності центральних та місцевих органів державної виконавчої влади, а також органів місцевого самоврядування в питаннях оптимізації напрямів державної політики у сфері протидії дезінформації, при підготовці та викладанні навчальних дисциплін «Цифрові комунікації та зв’язки з громадськістю в публічному управлінні», «Інформаційні війни та цифрова культура».

РОЗДІЛ 1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

1.1 Категоріально-понятійний апарат дослідження

Суспільство сьогодні переживає інформаційний етап, а тип інформаційної культури, відповідно зумовлює стан суспільної свідомості. Науковими дослідниками відзначено на даний час величезну кількість різних проблемних «хвороб» суспільної свідомості. Однією з важливих проблем є маніпулювання інформацією у соціальному та культурному просторі всього суспільства. Саме через посилення ролі інформатизації суспільства маніпулювання свідомістю громадян через надання різного виду їм інформації набуло тотального характеру [16].

Цифрова трансформація сучасного світу змінює традиційні методи комунікації на впровадження сучасних комунікаційних засобів, а саме глобальних мереж.

Мережа Інтернету, електронне урядування та публічні електронні послуги, електронні закупівлі та ін. стали вже звичайними у використанні.

Науковці застосовуючи термін «простір», підкреслюють, що «цифровий простір» є більш широким поняттям, ніж Інтернет-мережа. Цей простір охоплює не лише веб-сайти або веб-сторінки, як частини веб-сайтів, файли та оцифровані об’єкти інтелектуальної власності, електронні документи, а й усі пристрої в яких не передбачено паперова форма документообігу, тобто «гаджети»: планшети,

комп’ютери, носії інформації, ноутбуки, телефони тощо [7].

Таким чином, цифровий простір штучно створений за допомогою цифрових технологій, який забезпечує його учасникам нескінченне число внутрішніх ступенів свободи. В свою чергу поняття «цифровий простір» порівняно зі звичайним простором є похідним, а складовим простору інформаційного, з функцією кіберпростору в частині переходу від інформаційного до цифрового суспільства» [26].

Більшість конфліктів виникають між людьми через неоднозначність в поняттях, відсутність переконливості доказів тощо.

Однак, під час спілкування може бути подана інформація, яка не відповідає правдивості, яка має характер неправильності, перекрученості інформації, в якій простежується спрямованість на маніпулювання думками та фактами, не аргументованість відомостей, формулювання фраз з декількома значеннями.

Вагомий внесок у дослідження поняття «інформація» зробив Йонезі Масуда – японський соціолог і футуролог. Інформаційний простір Масуда

визначає, як поле зі складовими частини, які пов'язані між собою мережами інформації та мають три основні ознаки:

– інформація без кордонів;

– складання інформації з елементів, які залежать від дій, орієнтованих на конкретну мету;

– інформація має ієрархічний, динамічний характер і організовується тими, хто має право її використовувати та створювати [59].

Відомий японський дослідник у сфері інформаційної безпеки Йошифумі Масуда, чітко формулює проблеми, які представлені в новому інформаційному суспільстві.

Однієї з основних загроз, яку підкреслює дослідник, є втручанням в інформаційні технології у внутрішній світ особистості та соціальної спільноти. Отже, на думку Й. Масуди вирішити проблем у сфері інформаційної безпеки можна через демократизацію феномену інформації, забезпечення захисту громадян державою, цілеспрямовану роботи щодо запобігання комп'ютерним злочинам [59].

Забруднення і переповнення інформаційних ресурсів, направлена агресія в них стосовно конкретного користувача – це сучасний інформаційний простір суспільства. Відповідно не санкціонованість втручання в інформаційний обмін особи непотрібної, несправжньої, непрофесійної інформації, яка є перешкодою в роботі, створюючи при цьому труднощі та сприяючи втраті інформації й порушенню ритму роботи є ознаками інформаційної агресії.

Тому, концепція інформаційної безпеки держави має розглядатися як комплексний процес, що включає не лише захист від зовнішніх і внутрішніх загроз,

але й створення відповідних умов для ефективного функціонування інформаційного простору в межах країни та включати ключові підходи такі, як: забезпечення реалізації конституційних прав і свобод громадян, громадських організацій та загалом суспільства з питань доступу до відкритих інформаційних ресурсів, свобода інформаційної взаємодії, отримання необхідної відповідної інформації та можливість користування нею задля забезпечення ефективного діяльності держави, спрямування на підтримку стабільності, законності та захисту основних цінностей і принципів, закладених у Конституції України, досягнення стабільності з соціальних і політичних питань, захист співробітництва в самій державі, а також на міжнародному рівні.

Отже, можна зазначити, що захист інформації – це система саме державних заходів, які спрямовані на забезпечення інформації що має бути цілісною, конфіденційною та доступною. В той же час, діяльність, завданнями якої є вирішення питань щодо запобігання втраті відповідної інформації, недопустимості несанкціонованому проникненню в ресурси інформаційні, захисту прав власників інформації тощо, також розкриває поняття «захист інформації».

О.В. Буньківська зазначає, що сьогодні сформувався новий інформаційний простір з зміненою комунікативною системою сучасного світу, який можна охарактеризувати особливостями глобальності, відсутністю реальних кордонів міжнаціонального характеру, доступністю і швидкістю комунікацій, режимом реального часу, відсутністю чітких видимих ієрархій, основ – мережевих принципів організацій, уявної анонімності за реальної прозорості, тобто з можливістю контролю будь-яких дій, інтеграцією різних видів інформації, а саме: аудіо, відео, друкованої тощо [10].

Науковці Національної академії наук визначають інформаційний простір як інформаційну інфраструктуру, яка включає в собі сукупність інформаційних ресурсів, технологій їх супроводу і використання, інформаційні та телекомунікаційні системи [17].

Саме трактування науковцем О. М. Солодкої, найбільшою мірою, на нашу думку, підходить до визначення сучасного інформаційного простору, який є середовищем здійснення суб’єктами відповідної діяльності з питань створення,

використання, збирання, одержання, поширення, зберігання, охорони та захисту інформації з поширенням на неї юрисдикції України, в тому числі з

функціонуванням державної інформаційної інфраструктури [52].

Всі засоби передачі інформації за формами і змістом, що надходить до реципієнта, мають прямий та прихований маніпулятивний вплив на психіку людей, а також на індивідуальну й суспільну психологію.

Таким чином, виникнення процесів інформаційної глобалізації у взаємозв'язку з позитивними надбаннями привели до процесів появи сучасних викликів і загрозливих питань, що стосуються безпеки самої людини, всього суспільства і держави, тобто до руйнації соціокультурних цінностей, а саме: створення інформаційної зброї, впровадження інформаційних операцій та воєн, посилення психологічного маніпулювання свідомістю людей та інформаційних впливів [5].

Не існує загальноприйнятого визначення терміну «дезінформація», а також єдиного підходу до його тлумачення. Цей термін визначає неправильний або недостовірний зміст, який заподіяв конкретну шкоду, незважаючи на мотиви, усвідомлення або поведінку та використовується Організацією Об'єднаних

Націй з питань освіти, науки і культури та Міжнародним союзом електрозв'язку.

Інформація, яка вводить об'єкт в оману стосовно правдивого стану певних справ, та створює спотворену реальність, розповсюджує навмисно, часткову або без свідомо неправдиву інформацію з метою досягнення комерційних, пропагандистських, військових цілей тощо визначає поняття «дезінформація» або «дезінформування» (французькою des – спотворення) [3].

Науковці Європи розділяють поняття «дезінформація», як інформацію неправдиву та навмисно створену з результатом заподіяння шкоди особі чи окремій соціальній групі, чи взагалі організації або країні від «помилкової інформації», що містить також неправдиву інформацію, але вона не створювалася для заподіяння шкоди. Визначають європейські науковці ще такий вид інформації, як «зловмисна інформація», яка ґрунтується на реальних подіях і використовується для заподіяння шкоди окремій особистості, організації чи державі взагалі [20].

Таким чином, для визначення поняття «дезінформація» в сучасних наукових дослідженнях та документах Європейського Союзу наразі

застосовуються різні термінології, які можуть стосуватися фейків, дезінформації, пропаганди, маніпулюванню інформацією, інформаційним розладам, гібридній війні. Головне потрібно означити, що дезінформація має спрямованість на маніпуляцію свідомістю людини.

У 2022 році Європейським Союзом був запроваджений Посилений кодекс практики щодо дезінформації, в якому поняття «дезінформація» розглядалося більш ширше, яке включало в собі власну умисну недостовірну інформацію, помилкову інформацію, а також іноземне втручання інформаційного характеру.

Крім цього, новим Кодексом було встановлено більш «жорсткіші» рамки та заходи, які спрямовувалися на підвищення дієвості боротьби з інформаційним впливом, а саме:

− введення обмежень на монетизацію контенту, який містить недостовірну інформацію та дані; запровадження інструментів для боротьби з рекламою, що поширює дезінформацію;

− запровадження заходів, орієнтованих на підвищення прозорості політичної реклами; забезпечення етичності онлайн-послуг, що включає посилення заходів для зменшення маніпуляцій в кіберпросторі, зокрема через використання штучного інтелекту та інших технологій;

− розширення функцій користувачів онлайн-платформ, зокрема надання доступу до інструментів для перевірки інформації та виявлення дезінформації та маніпуляцій;

− співпраця та розширення можливостей для науковців, зокрема в частині надання доступу до анонімізованих даних, для вивчення феномену дезінформації та інших маніпулятивних впливів;

− розширення можливостей та зміцнення співпраці з організаціями, що займаються фактчекінгом [61].

В свою чергу, поняття «маніпуляція», тобто з латинської мови перша частина поняття означає «руку», а друга – «наповнювати» [4]. В переносному значенні це визначає прихованість дій з людьми як з об’єктами або речами.

За визначенням Сучасного словника соціології, видавництва Нью-Йорку у 1969 році маніпуляція – при якій носій інформації застосовує свою владу, впливаючи на поведінку інших, без розкриття її особливостей [4].

Отже, поняття «маніпуляція» – це способи скритого управління, найчастіше задля брехні та отримання односторонньої вигоди. Узагальнюючи роботи авторитетних дослідників [20;4;13;34;50], то можна окреслити головні ознаки цього поняття:

– інформаційно-психологічна дія маніпулятора на свідомість, психіку однієї людини або всього колективу людей, без фізичного насильства, але може бути кроком до застосування насильства;

– прихована маніпуляція – приховування інформації є обов'язковою – факт який має залишитися без усвідомлення суб'єктом маніпуляції. Цей вид маніпуляції розрахований на повний успіх коли той, на кого направлена інформація, вірить їй та сприймає все за дійсність;

– маніпуляція – з вимогами майстерності. Такий вид маніпуляції розраховується на масовість (суспільна свідомість, політика) та забезпечується спеціальними фахівцями та спеціальними знаннями. Сьогодні вже існує ціла система підготовки професійних кадрів та відповідної літератури.

Основною метою маніпуляторів є створення різних вигаданих і правдивих фактів і подій, формування до себе чи певних осіб лояльного відношення, ідеалізація чогось, панічних настроїв та провокаційних напружених ситуацій серед населення, нав'язування відповідного погляду через викравлення реальних фактів, а також дискредитування чогось або когось [59].

Також науковці вважають, що такі поняття, як «брехня» та «обман» є базовими будь-якої дезінформації та маніпуляції та активно використовуються при використанні «блефу», «хитрості», «махінації».

Маніпулювання громадською думкою є одним із основних інструментів управління масами людей. Така маніпуляція прихована і спрямована на встановлення відповідного контролю над їх поведінкою, тим самим позбавляючи їх свободу вибору, змінюючи їх уявлення, особисті переконання та цілі в потрібному маніпулятору напрямку. За своєю суттю маніпуляція суспільною думкою нагадує

війну, організованою і підготовленою не великою групою проти великої маси населення, яка не готова до цієї війни.

Одним із завдань цієї невеликої групи маніпуляторів є обов'язкове перешкоджання розкриттю методів маніпуляції, обмежуючи доступ загальних мас до застосованих технологій, використовуючи винагороди для своїх прихильників.

Необмежений доступ до використання соціальних мереж з отриманням в них своєчасної інформації зробили їх найбільш популярним засобом інформування. В свою чергу технічні можливості сучасних соціальних медіатехнологій мають вплив на формування новітніх напрямів продукування та

поширення у суспільстві інформації.

Розвиток інтернет-технологій зробили соціальні мережі активним місцем для поширення неправдивої інформації саме через велику кількість користувачів, доступність, анонімність при користуванні, популярність [6].

Таким чином, через неправдивість інформації, пропаганди тощо соціальні медіа вже здобули негативну популярність як платформи, що поширює Фейки, як неправдиві повідомлення, достовірність яких забезпечують свідчення, так званих, очевидців, сфабрикованих фото та відеоматеріалів [30].

Таким чином, фейкову інформацію можна розповсюджувати різними медіаформатами, включаючи текстові повідомлення, рекламу, підроблені фото-, відео- та аудіоматеріали, а також за допомогою активного використання ботів і тролів, які залучаються до обговорень під відповідними публікаціями в соціальних мережах чи на форумах.

Отже, до різновидів фейкової інформації можна віднести такі явища, як відкриту поширення плиток, дезінформацію, меми, маніпуляції, пропаганду,

«вірусний» контент, генерацію новин, а також синтезований медіаконтент тощо.

В свою чергу, українські дослідники поділяють фейки на різновиди за їх функціональним завданням: посіяти паніку; розпалити ворожнечу; заплутати за допомогою хибних думок, відволікти від правди; маніпулювання свідомістю;

рекламування когось або щось; плямування репутації; розважання [21].

Потрібно зазначити, що саме слово «фейк» використовується недавно і є новим, а новини з використанням фейків, тобто з ретельно сформульованих вигаданих історій з метою вигоди будь-якого характеру існували завжди. Незважаючи на цілеспрямованість чи спонтанність формування фейків, учать у їх поширенні бере велика кількість осіб, додаючи до не правдивої інформації свої нюанси, уточнюючи деталі, прикрашуючи емоційними подробицями тощо [60]. Тому в соціальних і політичних дискусіях особливо помітними сьогодні є виклики, що пов’язані саме з фейковими новинами.

Тому, на нашу думку, наразі варто звернути увагу на деякі загрозливі моменти для суспільства через використання фейків в наданні інформації, а саме: – присутність негативного впливу на всі аспекти суспільного устрою через велику чисельність новин-фейків в засобах масової інформації та соціальних мережах;

– перевантаження інформаційного простору неправдивими або спотвореними даними може викликати тривожні розлади організму у особи, а саме: посилений та постійний страх, тривога, нервозність, побоювання та стан занепокоєння

Достовірність відомостей цифрових, наприклад, засобів масової інформації сьогодні формують суспільну думку та можуть діяти для розпалювання відповідної ворожнечі та поширення панічних настроїв серед різних верств населення. Інформаційний цифровий простір сьогодення, зокрема Інтернет, став засобом інформаційного управління з виконаннями функцій обміну думками серед громадськості та отримання їм інформації.

1.2 Державна політика України щодо інституціоналізації суспільних відносин у сфері захисту інформаційного простору

Сьогодні значною мірою значущість інформації, а особливо цифрового простору, має тенденції до зростання. Для окремої людини наявність необхідної інформації, а також обізнаність в професійних, соціокультурних і політичних питаннях дають можливість ефективно орієнтуватися в навколишньому світі, робити обґрунтований вибір та приймати відповідні рішення.

Важливо, щоб така інформація відповідала низці характерних рис, зокрема: оперативності, актуальності, деталізованості, повноті, своєчасності, коректності, адекватності, доступності, зрозумілості, сучасності, точності, об’єктивності, новизні, узагальненості, цілеспрямованості, накопичувальності, повторюваності,

сегментованості, потенціалу до зростання і розвитку, циклічності, багаторазового використання, можливості відтворення на носіях різного характеру, здатності до кодування і декодування, стійкості, застосовності, незалежності від носія, збереження, безперервності, логічності, правдивості.

Один із факторів, що впливає на порушення відповідного стану

інформаційної безпеки людини – це забрудненість і перенасичення, в нашому випадку, цифрового простору.

Це відбувається завдяки втручанню рекламних повідомлень, сторонніх і шкідливих даних, програм у процесах обміну інформацією та взаємодії. Таким чином відбувається руйнація цього процесу та створюється загроза для особистих інформаційних даних користувача, створюючи деструктивні умови для його діяльності.

Тому виникає необхідність у формуванні організаційно-правових засад забезпечення інформаційної безпеки від дезінформації та маніпулятивних впливів на цифровий простір.

Отже, інформаційна безпека країни ґрунтується на створенні певних умов для дієвого функціонування інформаційного простору та, в тому числі, відповідної інфраструктури, які відповідно до чинного законодавства, Конституції України, а також напрацьованими практиками соціального характеру мають забезпечувати реалізацію питань, що визначають конституційні права і свободи суспільства, доступність до відкритих інформаційних ресурсів громадських організацій та громадян, тримання необхідної інформації та її використання для забезпечення дієвої роботи держави, збереження

конституційного державного ладу, устрою та територіальної цілісності країни, суверенітету держави, забезпечення соціальної та політичної стабільності, всілякого захисту інформаційних інтересів і потреб держави, що забезпечує діяльность державних структур, спрямованих на забезпечення законності, миру та

правопорядку, взаємодії з громадянським суспільством, рівноправного і вигідного співробітництва на внутрішньому і міжнародному рівнях, що сприяє гармонійному і динамічному розвитку держави.

Одним із ключових напрямків діяльності для забезпечення належного рівня інформаційної безпеки країни є захист будь-якої інформації, що визначається цілою системою державних заходів, які спрямовані на цілісність та конфіденційність інформації, а також забезпеченість її доступності.

Разом з тим, захист інформації – це відповідна діяльність, яка орієнтована на запобігання втраті даних, несанкціонованому доступі до інформаційних ресурсів та неналежному використанні інформації, включаючи незаконне використання авторських прав та прав власників даної інформації

Правові заходи, державні акти та відповідно до них спеціальні дії є саме засобами захисту, які спрямовані на захист інформації, на проведення різного характеру державних інформаційно-технічних експертиз тощо.

Отже в Україні створено низку інституцій за для захисту інформаційного простору.

В нашій державі Рада національної безпеки і оборони України відповідно до Закону України є координаційним органом, який займається питаннями безпеки і оборони національної спрямування при Президентові України та здійснює контроль за діяльністю органів публічної влади у галузі національної безпеки та оборони під час воєнного чи надзвичайного стану, а також у випадках виникнення кризових ситуацій, що становлять загрозу національній безпеці України [43].

У 2021 році урядом України створюється, як робочий орган Ради національної безпеки і оборони України, Центр протидії дезінформації за для протидії поточним та наявним загрозам національній безпеці, а також інтересам України в інформаційному просторі, забезпечення цифрової інформаційної безпеки держави, ефективної боротьби з пропагандою, дезінформаційними атаками та кампаніями, а також запобігання маніпуляції [44].

Основні завданнями Центру протидії дезінформації визначені в положенні про нього, затверджене окремим указом Президента України [32]:

– проведення аналізу та моніторингу подій і явищ в інформаційному просторі держави та самого інформаційної безпеки;

– проведення ідентифікації, досліджень реальних та потенційних загроз відповідної сфери, певних дестабілізуючих факторів, роботи щодо прогнозування та якісного оцінювання їх наслідків;

– формування основних принципів, координація дій органів державної влади, зміцнення можливостей відповідальних органів в інформаційній сфері, забезпечення інформаційної безпеки країни, розвиток національної інфраструктури;

– розробка методології щодо питань протидії застосування маніпуляцій, поширення неправдивої інформації та фейків, поліпшення ситуації підвищення рівня медіаграмотності взагалі суспільства.

Так, практичне втілення діяльності зазначено Центру відображено в розробленому Посібнику з протидії дезінформації, в якому наводяться відповідні техніки інформаційного впливу зі сторони держави-агресора, які стосуються :

– соціально-когнітивного хакінгу – процес активного впливу відповідного суб'єкта на деякі ділянки мозку індивіда, застосовуючи підсвідомі стимули, для отримання бажаних поведінкових проявів (застосовуючи приховану рекламу, ефекти сторони-переможця тощо) [24];

– використання фальшивих особистостей – використання клонами особистості для обману інших людей, для розголошення особистої інформації (підроблення, фейкові медіа, самозванці та шахраї, підставні особи);

– зловмисного використання технологій – ботів, віртуалів, діпфейків, фішингів;

– дезінформації – фальсифікації, маніпуляції, місапропріації, сатири та пародії;

– маніпулювання риторикою – використання дій, які спрямовуються проти конкретних особистостей, підміни тез, риторичних технік, в яких учасник, наприклад, дебатів намагається придушити не точною, брехливою інформацією опонента з надмірною кількістю аргументів тощо [50].

На наш погляд, сьогодні особливістю визначаються сучасні інструменти інформаційних впливів, маніпулятивних заходів, дезінформування, кампаній (табл. 1.1.)

Враховуючи триваючу війну на території нашої країни, необхідно розуміти, наскільки світовий інформаційний простір насічений проросійськими наративами.

У 2023 році Центром протидії дезінформації були оприлюднені основні проросійські думки, в основі яких знаходяться маніпулювання свідомістю, нав'язування свої вигідних тверджень стосовно того, як приклад, що НАТО спровокувало Російську Федерацію до нападу на території України, процес надання Україні відповідної зброї призводить до певної ескалації конфлікту з боку НАТО; Росія воює не з Україною, а з НАТО тощо.

Інформаційний простір сьогодні демонструєте високу агресивність щодо конкретного користувача, проявляючись у не санкціонованості втручання в інформаційний обмін та взаємодії особи невірною, фальшивою, неякісною

інформацією, яка, в свою чергу, створює перешкоди у роботі, труднощі та сприяє певним чином втраті інформації, а також порушує робочий ритм.

Таблиця 1.1 – Інструменти інформаційних впливів, дезінформування та маніпулювання [54]

Заговорювання	*Ефект первинності*
використання в пропаганді, за для зниження актуальності та викликання негативної реакції до будь-якої події	неправдива інформація має бути донесена до аудиторії раніше, ніж правда
Буденна розповідь	*Удар на випередження*
привчання аудиторії до неправдивої інформації, що пов'язана з вчиненням насильства, вбивства, терористичних актів, обстрілів, тобто застосування ефекту «звикання» до насильства	випереджаючий вкид брехні, за для виклику зустрічної реакції для подальшого використання у вигідному для себе контексті
Хибна аналогія	*Констатація факту*

зіставлення певних властивостей і відносин, які не мають взаємозв'язка реального	подання в медіа ресурси бажаної інформації як такої, що не можу підлягати сумніву
Обхід з флангу	*Ефект ореолу*
дозована передача правдивих відомостей, яку можна перевірити, з легким додаванням пропагандистської інформації	зводиться до двох основних тверджень: «поруч – значить разом», «якщо людина ефективна в одній галузі, то і в інший буде такою ж»
Керований коментар	*Створення проблеми*
повідомлення, направлене на скерування думок у потрібному напрямку	підвищення значимості через підбір інформації, одних подій та, в той же час, її зменшення щодо інших
Відволікання уваги	*Переконання*
Зменшення фокусу уваги одного об'єкта для збільшення значимості іншого; відволікання зайнятої важливою діяльністю людини стороннім подразником	вплив на психічний стан людини через апелювання до її критичного мислення з метою нав'язати думку
Спіраль мовчання	*Зараження / «стадний» інстинкт*
маніпулювання процесом опитування суспільної думки шляхом підбору відповідних коментарів, з метою переконання населення у підтримці більшістю	Передача емоційного стану від однієї людини до іншої на рівні несвідомості
Дублювання акаунтів	*Підміна понять*
копіювання інформаційного вмісту справжніх акаунтів користувачів, для створення облікових з подальшим використанням для шахрайства, маніпулювання, поширення дезінформації тощо	представлення перед аудиторією об'єкта або явища таким, яким він не є за допомогою підміненого вислову для вкорінювання в суспільство як єдиного вірного

На прикладі небезпечних наративів російської пропаганди, що потрапляють в інформаційний простір деяких країн, що межують з Україною на заході (Молдова, Польща, Угорщина) можна зазначити, що кожен такий наратив має глибоке підґрунтя до маніпулювання свідомістю громадян відповідних країн та нав'язування їм своєї потрібної пропаганди (рис. 1.1).

Рисунок 1.1 – Наративи російської пропаганди, які були застосовані в країнах Заходу під час повномасштабного вторгнення на територію України

Центр протидії дезінформації пропонує узагальнений алгоритм відповідної реакції на інформаційні загрози в яку закладено наступні кроки:

– оцінювання (аналіз певної ситуації, фактчекінг, повне дослідження);

– інформування (надання офіційних заяв, миттєве інформування зацікавлених сторін);

– відстоювання (викриття, доступність інформації, поширення); – захист (блокування інформації, направлення скарг) [33].

Міністерство культури та стратегічних комунікацій України в частині формування та реалізації державної політики в інформаційній сфері відповідає за питання інформаційного суверенітету та інформаційної безпеки нашої країни, розробляє заходи щодо запобігання інформаційному впливу внутрішнього і зовнішнього характеру, захищаючи тим самим інтереси держави, зміцнюючи національну безпеку і відновлюючи територіальну цілісність України [15].

Так, для розбудови національної стійкості, запровадження заходів протидії інформаційним загрозам, ефективної боротьби з дезінформацією, фейкам,

запобігання маніпулятивної інформації тощо при Міністерстві культури та інформаційної політики України у 2021 році було створено Центр стратегічних комунікацій та інформаційної безпеки [55], діяльністю, якого визначено наступне:

– дослідження інформаційного середовища, моніторинг дезінформаційних повідомлень у цифровому просторі;

– посилення захисту від дезінформації та інформаційних атак зі сторони країни-агресора, гібридних загроз;

– реалізація спеціалізованих інформаційних програм для підвищення рівня медіаграмотності громадян;

– зміцнення потенціалу стратегічних комунікацій для національного користувача та міжнародної спільноти.

За ініціативи Центру стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та Міністерство культури та стратегічних комунікацій України у співпраці з деякими центральними органами виконавчої влади (Державна служба України з надзвичайних ситуацій, Міністерство оборони України та ін.) та громадськими організаціями було проведено роботу з розроблення рекомендацій щодо поводження в інформаційному просторі за умов воєнного часу, в яких зазначаються основні тези, щодо мети поширювачів дезінформації, поширення інформації із сумнівних джерел, деморалізування України, поширення інформації про переміщення українських військ, обстрілів мирного населення українськими військовими, поширення чуток про військовополітичне керівництво країни, інформації про втрати під час воєнних дій, поширення наклепів країною-агресором через свої офіційні чи підконтрольні їй канали, дія при виламуванні сторінки публічних органів [53].

Окрім Центру протидії дезінформації та Центру стратегічних комунікацій та інформаційної безпеки в Україні створені інші центри з діяльністю у сфері кіберзахисту. Такими центрами є:

– Рада національної безпеки і оборони України – Національний координаційний центр кібербезпеки – забезпечення координації та контролю за діяльністю суб'єктів сектору безпеки і оборони України [41];

– Державна служба спеціального зв'язку та захисту інформації України – Державний центр кіберзахисту – питання аудиту безпеки, стану відповідних об'єктів критичної інформаційної інфраструктури тощо [14];

Сьогодні інформаційний простір, в тому числі і цифровий, має такі ключові функції.

– інтегруючу – об'єднання в єдиному просторово-комунікативному та соціокультурному середовищі різних суб'єктів та видів людської діяльності;

– комунікативну – створення особливого середовища транскордонних, інтерактивних та мобільних комунікацій різних суб'єктів відповідної діяльності;

– актуалізуючу – здійснення актуалізації інтересів різних відповідних суб'єктів діяльності через реалізацію ними інформаційної політики;

– геополітичну – формування власних ресурсів та зміна значущості традиційних ресурсів;

– соціальну – трансформування складу суспільства, змінюючи характер та зміст соціальних та політичних (суспільних) відносин політичній, культурній, науковій, релігійній та інших сферах.

РОЗДІЛ 2 СУЧАСНИЙ СТАН ОЦІНЮВАННЯ РІВНЯ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА МАНІПУЛЯЦІЯМ В УКРАЇНИ

2.1 Правові засади протидії дезінформації в Україні

У контексті швидкого розвитку інформаційних технологій, цифрового простору та зростання обсягів різної інформації, яка поширюється серед населення країни, в той же час, неправдива інформація та фейки стають серйозною загрозою для національної безпеки, демократичних інститутів та громадського здоров'я. Особливо гостро постає проблема несумісності законодавчих актів в Україні, оскільки існує нагальна потреба в питаннях комплексного підходу до національної нормативно-правової системи, яка б могла забезпечити ефективне регулювання різносторонніх аспектів правових відносин і проблем, пов'язаних з дезінформацією та маніпуляцією.

Відсутність чітких визначень понять «дезінформація», «фейкові новини» та «маніпуляція», насамперед, призводить до невизначеності в правовій сфері та в діяльності органів публічної влади з функціями контролю.

Така ситуація веде ускладнення, а в деяких випадках до відсутності належної координації між інституціями, що, навпаки, приводить до дублювання повноважень у боротьбі з дезінформаційними впливами.

На наявність високого рівня неправдивої інформації пливають відповідні чинники, а саме: низький рівень медіаграмотності та критичного мислення серед громадян, недостатня їх обізнаність; відсутність належного фінансування використання сучасних цифрових технологій; наявність етичних та правових аспектів, які впливають на дезінформацію та захист свободи слова, приватність. Тому, можна зазначити, що з огляду на вказану проблематику, все ж таки виникаю питання щодо удосконалення процесу формування інституційних та нормативно-правових засад протидії маніпулюванню та неправдивій інформації, які б, свою чергу мають бути націлені на створення належного цифрового

простору та покращення безпеки українського суспільства.

Інституційно-правові основи боротьби з неправдивою інформацією повинні включати законодавчі, організаційні та стратегічні заходи, які будуть спрямовані на захист інформаційного середовища держави. В основі таких засад складають наступні компоненти:

1. Система законодавства, що охоплює:

1.1. Нормативно-правові акти, що регулюють реалізацію національної інформаційної політики, діяльність медіа, права на доступ до відповідної інформації та встановлюють відповідальність за поширення фейків та дезінформації.

1.2. Законодавча база, яка надає гарантії щодо захисту прав споживачів, зокрема норм, які захищають громадян країни від неправдивої, наприклад, реклами та інформації.

1.3. Антидискримінаційне законодавство, яке спрямовується на захист від фейків та неправдивої інформації, що, в свою чергу,

призводить до дискримінації певних соціальних верств населення.

2. Органи контролю та нагляду:

2.1. Національні ради з питань телебачення і радіомовлення – здійснення контролю щодо забезпечення відповідності стандарту інформаційного мовлення. 3. Антимонопольні органи – контроль питань не допустимості монополізації медійного простору та пропаганди.

4. Державні стратегії та програми протидії неправдивій інформації – спрямованість на підвищення серед населення країни медіаграмотності забезпечення координації зусиль різних відповідних організацій та установ.

5. Інформаційні кампанії – направленість на покращення обізнаності громадян про ризики неправдивої інформації та її наслідки.

6. Міжнародні організації – співучасть у ініціативах глобального та регіонального рівнів, які орієнтовані на боротьбу з фейками, маніпулюваннями та дезінформацією тощо.

7. Моніторинг та реагування – розробка відповідних системи моніторингу дезінформації, яка забезпечує технологію штучного інтелекту визначення новинфейків.

8. Навчання та освіта – створення освітніх програм, спрямованих на підвищення медіаграмотності учнів, студентів та слухачів.

Отже різноманітність компонентів інституційно-правових засад боротьби з фейками та неправдивою інформацією залежить саме від особливостей

розвитку конкретної держави та її існуючої правової системи.

Захист суверенітету країни, територіальної цілісності та забезпечення національної безпеки взагалі є основними пріоритетами для будь-якої держави, зокрема й для України, що підтверджується статею 17 Конституції України [23]. Саме ці аспекти фундаментом. Саме ці принципи є основою для забезпечення інших прав і свобод громадян, а також для соціально-економічного розвитку країни.

Закон України «Про національну безпеку України» визначає державну політику, яка спрямована на забезпечення також кібербезпеки та інформаційної безбеки України [42].

Стратегія національної безпеки України конкретизує відповідні напрями [45], в частині критичних проблем інформаційної сфери, зміцнення інструментів національної сили через використання інформаційно-психологічних та кіберзасобів, а також вплив інформаційної «зброї.

Інформаційна безпека направлена на захист інформаційного, в тому числі цифрового, простору країни від впливу зовні, фейків, неправдивої інформації та інших загроз, які можуть завдати шкоди суспільству та загалом державі. Для забезпечення всіх аспектів національної безпеки передбачаються спільні зусилля держави та громадян, а також розробка ефективних стратегій та політик у відповідних сферах.

Унормування загальних положень в питаннях забезпечення інформаційної безпеки України, конкретизуючи актуальні виклики та загрози у вказаній сфері простежується у Стратегії інформаційної безпеки [47].

У Стратегії визначені ключові напрямки та принципи забезпечення інформаційної України, створюючи правові, стратегічні та організаційні основи для зазначеної діяльності у цій сфері.

Розгляд різноманітних глобальних викликів та загроз у Стратегії, пов’язані з інформаційною безпекою країни. Сьогодні сучасна реальність визначається загрозою демократичного розвитку через зростання кількості дезінформаційних проблем, що організовуються відповідно авторитарними урядами та радикальними угрупованнями. Особливу увагу приділено інформаційній політиці Російської Федерації, яка впливає відповідним чином на демократичні інституції та, в свою чергу, поглиблює протиріччя в державах демократичного устрою через проведення спеціальних інформаційних операцій та гібридної війни.

Під час пандемії COVID-19 простежується підвищення ролі соціальних мереж у цифровому просторі сучасності. Саме розвиток цифрових технологій на загрозу щодо права на приватність та появу недоліків у гарантуванні відповідної безпеки персональних даних. Також, в даному документі приділяється увага саме недостатності рівня медіаграмотності населення, що в свою чергу, вказує на наявність у населення некритичного сприйняття інформації. Таким чином, можна зазначити, що через зростання доступності інформації з недостатністю медіаграмотністі поширюється дезінформація та маніпуляції, що, в свою чергу, позначається негативно на стабільності демократичних держав.

У розділі Стратегії, що стосується національних викликів та загроз, розглядаються інформаційні відповідні виклики та загрози України національного рівня, а саме застосування різних методів інформаційного впливу за для підриву національної безпеки; ліквідація української національної державності та ідентичності, застосовуючи дестабілізацію в цілому суспільстві.

Саме такий інформаційний вплив сьогодні чинить Російська Федерація як держава-агресор проти України. Тимчасово окуповані території нашої країни потерпають від інформаційного домінування через придушення свободи слова, контролю над засобами масової інформації, повного блокування доступу до

інформаційних джерел, які є незалежними, а також створення альтернативної – неправдивої інформації для маніпулювання та нав’язування потрібної інформації.

Наявність недосконалої системи реагування та слабко розвинутої інформаційної інфраструктури в Україні вказує на обмежену здатність ефективно протистояти дезінформаційним кампаніям, що певним чином впливають на загрозу національної безпеки та інтереси України.

Також у цьому розділі акцентується увага на важливості розвитку стратегічних підходів та національних ініціатив для боротьби з інформаційними загрозами та викликами, зокрема на необхідності підготовки та зміцнення саме інформаційної обізнаності та стійкості громадян держави.

У затвердженій відповідним указом Президента України Стратегії кібербезпеки України [46], яка ґрунтується на положеннях Закону України «Про основні засади забезпечення кібербезпеки України» [43], розглядаються актуальні питання забезпечення кібербезпеки через призму пріоритетів національної безпеки країни, визначаються ролі кіберпростору та інформаційних технологій сучасності та акцентується увага на ризиках, що пов’язані з їхнім використанням, підкреслюються значення захисту від сучасних кіберзагроз, а також значення питань, що стосуються захисту відповідних об’єктів інформаційної інфраструктури критичного значення та інших об’єктів від кібератак.

Зазначений документ підкреслює, що Російська Федерація є одним із головних джерел кіберзагроз та гібридної війни проти нашої країни, що, в свою чергу, створює потребу у перегляді стратегії та тактики боротьби з кіберзагрозами та розвідувально-підривною діяльності в кіберпросторі. Питання важливості співпраці всіх відповідних суб’єктів, що опікуються напрямами забезпечення кібербезпеки, для забезпечення безпеки в цифровому просторі також визначені у Стратегії кібербезпеки України.

Особливої уваги, на нашу думку, заслуговує Концепція забезпечення національної системи стійкості [48], що формує уявлення та підходи країни до розробки та впровадження відповідної державної системи, яка охоплює різні

аспекти управління загрозами та кризовими ситуаціями, які можуть виникати в сучасних умовах, в тому числі гібридного характеру.

У документі передбачено чіткий розподіл повноважень і відповідальності між органами управління, а також забезпечення співпраці на всіх виключно рівнях управління, що є основними для ефективного реагування на різноманітні загрози та ситуацій кризового характеру.

Ключовими складовими елементами ефективної національної системи стійкості є ретельно продуманий підхід до таких питань як загрози, оцінка ризиків та розробка планів дій, їх систематичності. А для вирішення завдань, що

стоять перед національною системою, необхідно забезпечити всі сфери життєдіяльності суспільства і держави, зокрема економічні, кібернетичні, енергетичні, екологічні, інформаційні, продовольчі, а також питання охорони здоров'я, культури і освіти [18].

Отже, в Україні існує ряд нормативно-правових актів, які визначають обмеження та заборони на розповсюдження певної категорії інформації

Так в Законі України «Про медіа» встановлюються обмеження на

поширення аудіо інформаційних медіа-сервісів на замовлення та послуги провайдерів аудіо послуг інформаційного характеру з держави-агресора [40].

Саме реагування на виклики зовнішній агресії було метою прийняття цього відносно нового закону. Відповідно до зазначеного закону та на основі поданих звернень до Міністерства культури та інформаційної політики України Радою національної безпеки і оборони України, Службою безпеки України, Національною радою України з питань телебачення і радіомовлення було створено відповідний Перелік осіб, які визначені такими, що створюють загрозу національній безпеці України [31].

Очікуваним було внесення змін та доповнень і до інших нормативно-правових актів стосовно протидії фейкам, пропаганді, дезінфомації, маніпулюванням тощо, а саме:

– Закон України «Про кінематографію» – заборона розповсюдження та демонстрування фільмів з популяризацією органів держави-агресора або радянських органів державної безпеки [39];

– Закон України «Про видавничу справу» – заборонна поширення продукції ідентичної тематики та передбачення дозвільного режиму на ввезення продукції видавничого характеру із території держави-агресора [36].

Відповідно до Конституції України, Законів України «Про медіа» та «Про інформацію» [23; 40; 38] під забороненою цензурою в Україні потрібно використовувати будь-яку вигоду, яка спрямована до засобів масової інформації, журналістів, засновників (співзасновників) засобів масової інформації, керівників, видавців, розповсюджувачів, узгоджувати інформацію перед її поширенням, а також будь-яка заборона чи перешкода в інших формах на тиражування або розповсюдження інформації. Однак, потрібно зазначити, що відповідна заборона не має права поширюватися, якщо інформація попередньо узгоджена на підставі закону на випадки, коли попереднє узгодження інформації здійснюється на підставі закону [7].

Таким чином, можна зазначити, що держава має певні механізми впливу як на осіб, що поширюють дезінформацію, фейки тощо, так і на саму неправдиву (спотворену), брехню інформацію. Однак, з огляду на масштаби та швидкість її поширення, залучені ресурси є наразі недостатніми

Але відсутність законодавчих змін та потужної організаційної роботи приводять до продовження споживання активно громадянами нашої країни іноземного контенту, в тому числі й країни-агресора.

Так, у 2023 році центром Разумкова було проведено опитування українських громадян щодо їх ставлення до бойкотування культури російського контенту (рис. 2.1). Отже, за результатами опитування масово ідею бойкоту підтримало лише близько 40 відсотків, майже 15 відсотків реципієнтів згодні підтримувати проведення заходів із росіянами, але якщо останні засуджують дії своїх президента та уряду та ще 15 відсотків українців взагалі приймати участь у подіях, в яких представлені громадяни країни-агресора [27].

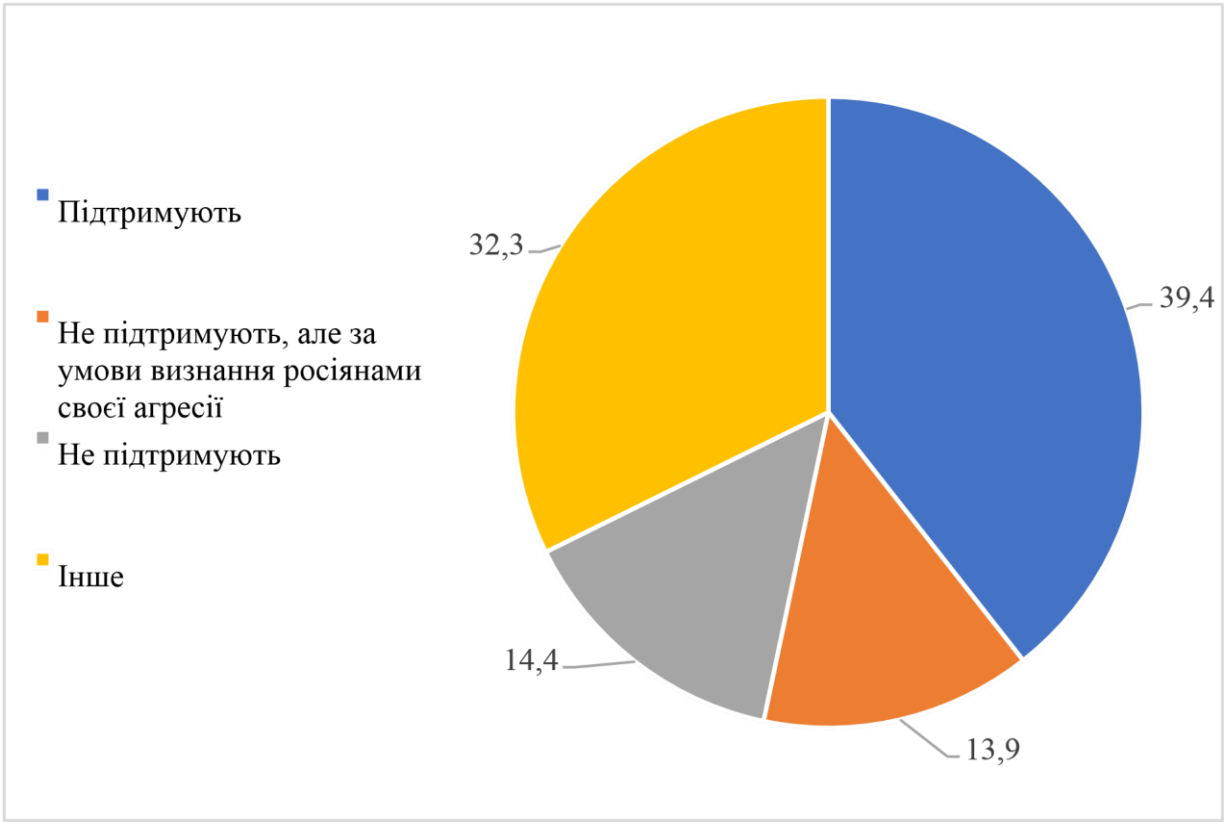

Рисунок 2.1 – Результати опитування центром Разумкова ставлення українців до бойкоту культури російського контенту [27]

Окрім органів публічної влади, відчувається, на нашу думку, необхідність у більшої активності діяльності саме громадських організацій, які зареєстровані відповідно до вимог Закону України «Про громадські об'єднання» [40], та приймають участь у діяльності з питань, що стосуються підвищення достовірності відповідної інформації за рахунок певних освітніх кампаній інформації та підвищення медіа грамотності громадян країни. Саме кампанії з зазначених напрямів діяльності особливо в цифрових сферах наразі стають

актуальною стратегією боротьби з неправдивою інформацією.

Уряд країни має всіляко забезпечувати прозорість процесу чітких механізмів щодо ідентифікації та реагування на фейки, дезінформацію, пропаганду, особливо, якщо вона від країни-агресора.

Так, відповідно законодавства в Україні передбачається цивільно-правова, кримінальна та адміністративна відповідальність за поширювання дезінформації, що викликає панічний настрій у населення або порушення громадського порядку, та

тягне за собою, відповідно, накладення штрафу у розмірі від 10 до 15 неоподатковуваних мінімумів доходів або призначення виправних робіт строком до одного місяця [22]. В той же час кримінальне законодавство орієнтується не на оцінку факту достовірності самої інформації, а більшою мірою направлений на визначення ступеня загрози, яку відповідна інформація несе відбиток для суспільство [25].

Тому при виборі законних та ефективних способів боротьби з дезінформацією необхідно в першу чергу орієнтуватися відповідними принципами. Напрацювання з актуального питання були розроблені під егідою Європейської Комісії, які є ефективними не тільки в країнах Європейського Союзу, але й виступають орієнтирами для формулювання та впровадження інформаційної політики в Україні [2].

2.2 Ефективність національної політики протидії дезінформації: аналіз громадської думки

На даний час інформаційний цифровий простір нашої країни максимально перенасичений різноманітними інформаційними ресурсами, забрудненнями та переповнений недостовірною, а часто й просто фейками. Саме несанкціоновані втручання у внутрішні цифрові ресурси користувачів проводять до нав’язування їм шкідливої, зовсім непотрібної, взагалі незатребуваної інформації.

Саме негативний характер цифрового інформаційного простору щодо кожної людини створює умови для відповідного порушення її власної інформаційної безпеки.

У всьому світі, як й в Україні останніми роками найпопулярнішим джерелом інформації є цифровий простір, а точніше Інтернет.

Згідно з опитуванням, більше 60 відсотків реципієнтів отримують всю інформацію з соціальних мереж і майже 50 відсотків з новинних сайтів. Відсутність в соціальних мережах редакційного контролю, свобода різних публікацій для будь-якого користувача, а також швидке створювання та поширення інформації на безкоштовній основі приводить до легкого розповсюдження дезінформації. Через те,

що кожен може створити контент, легко поширити вірусний вміст, який, в свою чергу, поширюється на багатьох сайтах, сьогодні соціальні цифрові мережі набирають величезної популярності

[29].

Таким чином, через переповнення інформації в Інтернеті, стало вкрай важливо для користувачів соціальних мереж розрізняти джерела, з приводу довіри до них.

До 2014 року наша країна не приділяла належної уваги рівню загрози в цифровому інформаційному просторі, тобто, не визнавала або не бажала визнавати рівень негативного інформаційного впливу сусідньої країни. Через вільний доступ в Україні телеканалів сусідньої країни українська аудиторія знаходилася в полі постійної уваги пропагандистів, російських контенту, політтехнологів. Окупація Криму та частин Луганської та Донецької областей у 2014 році почало змінювати ситуацію тому, що ігнорування зазначеної проблеми стало вже зовсім неможливим. Так Україна починає застосовувати всілякі інструменти задля протидії маніпулюванням, фейкам, дезінформації тощо з боку Росії.

Повномасштабне вторгнення Російської Федерації на територію нашої країни призвело до активізації суспільства України в інформаційному цифровому полі. Так, більше 60 відсотків українців почали отримувати новини через телеграм-канали саме після 24 лютого 2022 року, тоді як до цього часу лише 36 відсотків ознайомлювалися з новинами через телеграм-канали.

Дане опитування проводилося Київським міжнародним інститутом соціології на замовлення громадської організації «Український інститут медіа та комунікації» у 2023 році.

При проведенні дослідження, визначено, що більше 80 відсотків громадян України обізнані про існування дезінформації. Ще 73 відсотки вважали, що вміють і можуть її розпізнавати. І тільки менше 10 відсотків реципієнтів зуміли взагалі правильно виявити всі фальшиві новини.

Майже всі опитувані учасники дослідження погодилися, що країна-агресор стала поширювати більше фейків та неправдивої інформації проти України після початку повномасштабного російського вторгнення на територію нашої країни

(рис. 2.2).

Також потрібно зазначити, що різниці між мешканцями різних регіонів у відповідях не виявилося. Так, майже 85 відсотків реципієнтів західної України погоджуються з зазначеним твердженням, східна Україна – 80,4 відсотки, центральна Україна – 86 відсотків, південна Україна – 82 відсотки. Практично не простежується різниця між міським та сільським населенням, відповідно 85 відсотки та 81 відсоток. Майже такий же розподіл відсотку визначення відповідей серед опитуваних по гендерному розподілу, чоловіків трохи більше
погоджується з цим твердженням (чоловіки – 87 відсотків, жінки – 81 відсоток).

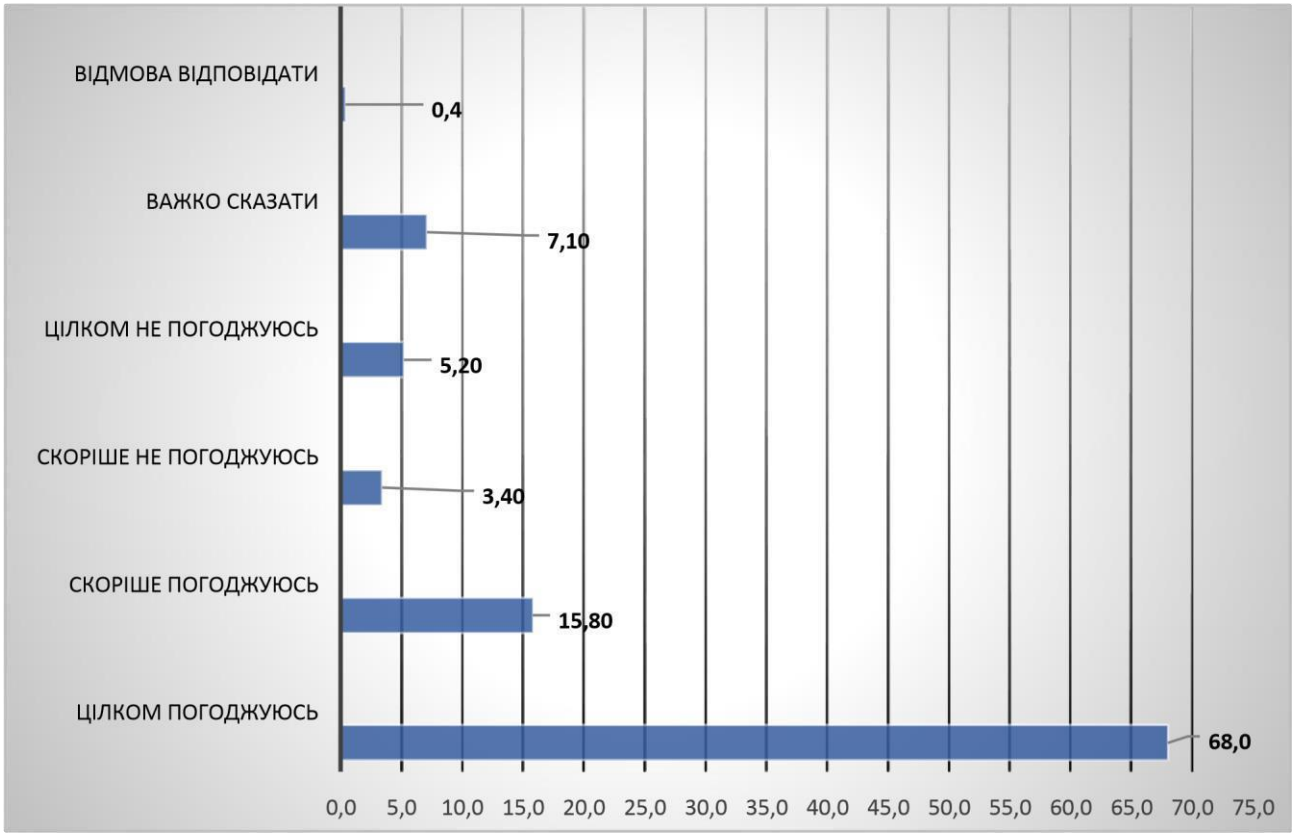

Рисунок 2.2 – Оцінка учасників опитування щодо збільшення поширення Росією дезінформації проти України після 24 лютого 2022 р. у % [11]

Наступним питанням учасникам дослідження було запропоновано визначити ефективність протидії України російській дезінформації. Громадяни загалом дали високу оцінку ефективності протидії неправдивій інформації. Так, майже 35 відсотків респондентів вважають, що держава з цього питання діяла ефективно,

майже 50 відсотків опитаних означили часткову ефективність. Але більше 7 відсотків українців вважають протидію дезінформації зовсім неефективною (рис. 2.3).

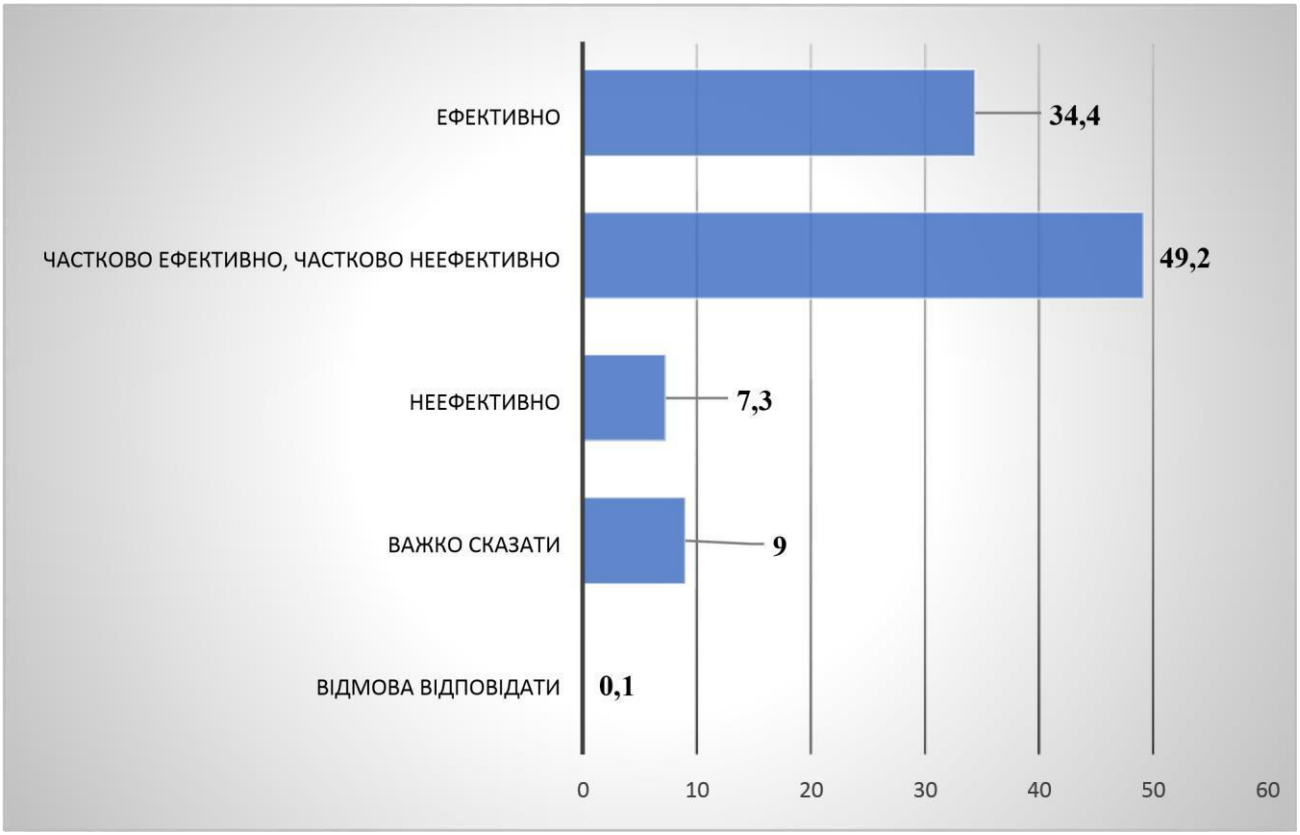

Рисунок 2.3 – Показники ефективності протидії дезінформації у % [11]

У регіональному контексті, як і в першому випадку, відслідковується різниця незначна: західні регіони оцінюють протидію неправдивій інформації ефективною – 32,3 відсотки, майже 52 відсотки – як частково ефективну або частково неефективну; східні регіони – відповідно 36,7 та 43,3 відсотків, центральні регіони – 35,8 та майже 49 відсотків, південні регіони – 33,6 та 50,8 відсотків. Так само, в гендерному розрізі майже однаково оцінюють ефективність із зазначеного питання чоловіки та жінки, а саме: ефективна протидія дезінформації – чоловіки – 36,4 відсотки, жінки – майже 33 відсотки. Серед

опитаних 50 відсотків чоловіків та 48,5 відсотків жінок вважають, що протидія є частково ефективною, частково неефективною.

Наступним питанням учасникам опитування було запропоновано визначити хто більше сприяв протидії дезінформації країни-агресора після повномасштабного вторгнення 24 лютого 2022 року та потрібно було обрати три варіанта. Таким чином, 42,8 відсотки респондентів визначили Президента України таким, що найбільше сприяв протидії фейкам та неправдивій інформації. З 35 відсотками на другому місці опинилися військові. Третє місце серед тих хто сприяв протидії дезінформації, посів марафон «Єдині новини» – 29 відсотків. В той же час лише в 13,8 відсотків оцінили зусилля інших засобів масової інформації. Вклад в протидію неправдивій інформації волонтерами оцінили респонденти в 25 відсотків (рис. 2.4).

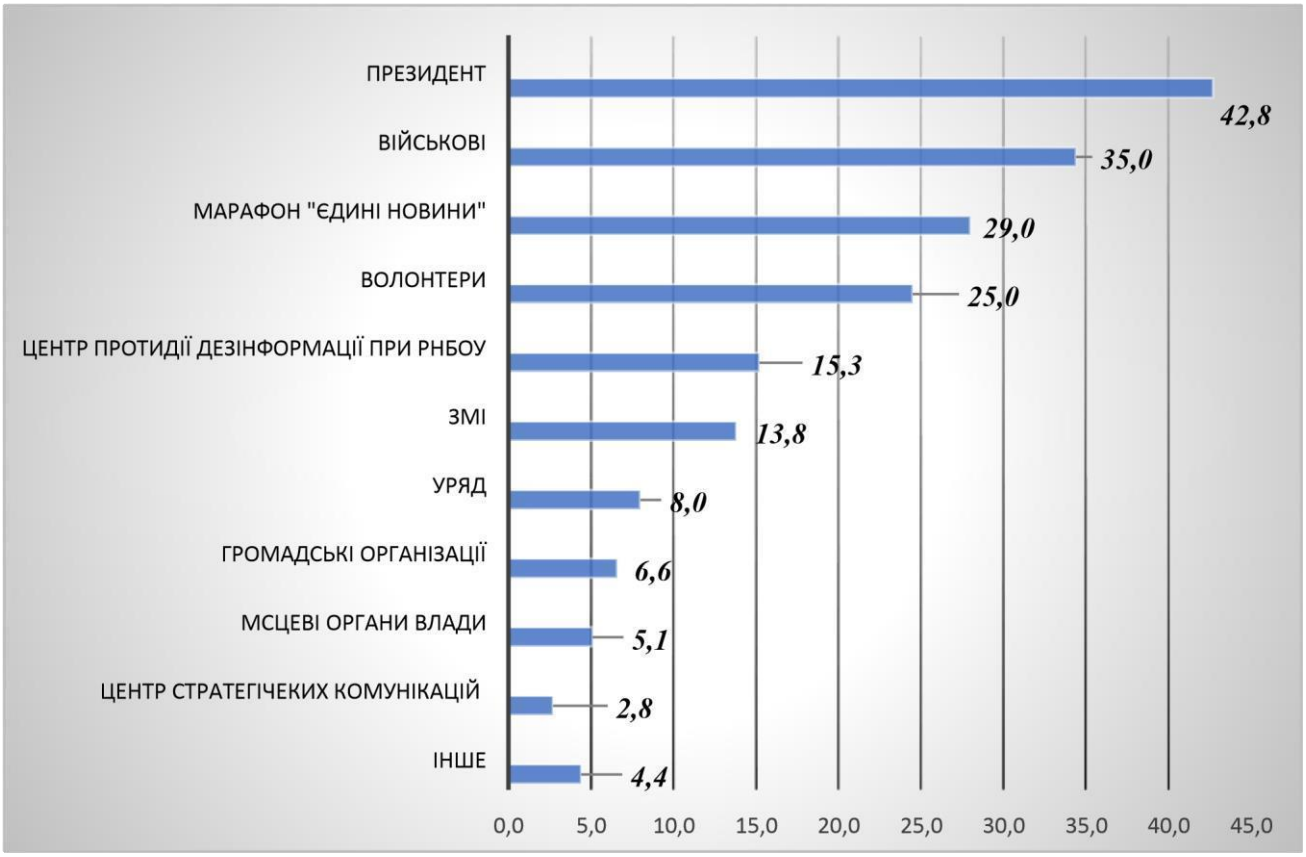

Рисунок 2.4 – Показники визначення тих, хто більше сприяв протидії дезінформації країни-агресора після повномасштабного вторгнення 24 лютого 2022 року у % [11]

Позитивно оцінили (15,3 відсотки) роботу в цьому напрямку Центру протидії дезінформації при Раді національної безпеки і оборони України на відміну від роботи Центру стратегічних комунікацій при Міністерстві культури і стратегічної комунікації (2,8 відсотки). Така різниця у відсотках серед опитаних може бути через не розуміння громадян України у функціональній різниці між обома Центрами.

Під час опитування привернуло увагу той факт, що майже 50 відсотків жінок проти 36,4 відсотки чоловіків вважають, що саме зусилля Президента України найбільше приділяли уваги протидії фейкам та дезінформації. Така ж сама суттєва різниці простежується у віковому розрізі, а саме:

– висока оцінка зусиллям Президента України надана людьми віці до 30 років, тобто молодшого віку (53,7 відсотки);

– низька оцінка зусиллям Президента України надана людьми у старшій віковій групі (особливо старше сімдесяти) – 36,4 відсотки. Ця вікова категорія опитаних віддавали перевагу телемарафону «Єдині новини» – майже 30 відсотків.

Також ціллю опитування було з’ясувати, що могло б допомогти українцям ефективніше розпізнавати дезінформацію. Так майже 40 відсотків опитаних вважають, що це має бути від органів публічної влади, а 22,5 відсотки – від національних засобів масової інформації, в той же час, 14 відсотків надію покладають на інформацію від блогерів.

Однак певне занепокоєння викликає втрата бажання людей до навчання. Тільки 5 відсотків опитаних респондентів вважають, що тренінги, онлайн-курси

тощо могли б допомогти їм ефективніше розпізнавати інформацію стосовно фейків, дезінформації та ін.

Ця цифра дещо вища серед молодшої та середньої вікових груп (майже 7 відсотків), а серед людей старше 70 років жоден респондент не обрав зазначену опцію.

Світ сьогодні постійно стикається з проблемою дезінформації, фейків, маніпулювання, що створюються за допомогою штучного інтелекту. Все це несе серйозні ризики в питання підриву довіри до надійних джерел інформації, маніпулювання громадською думкою та суспільними настроями, а також втручання у вибори.

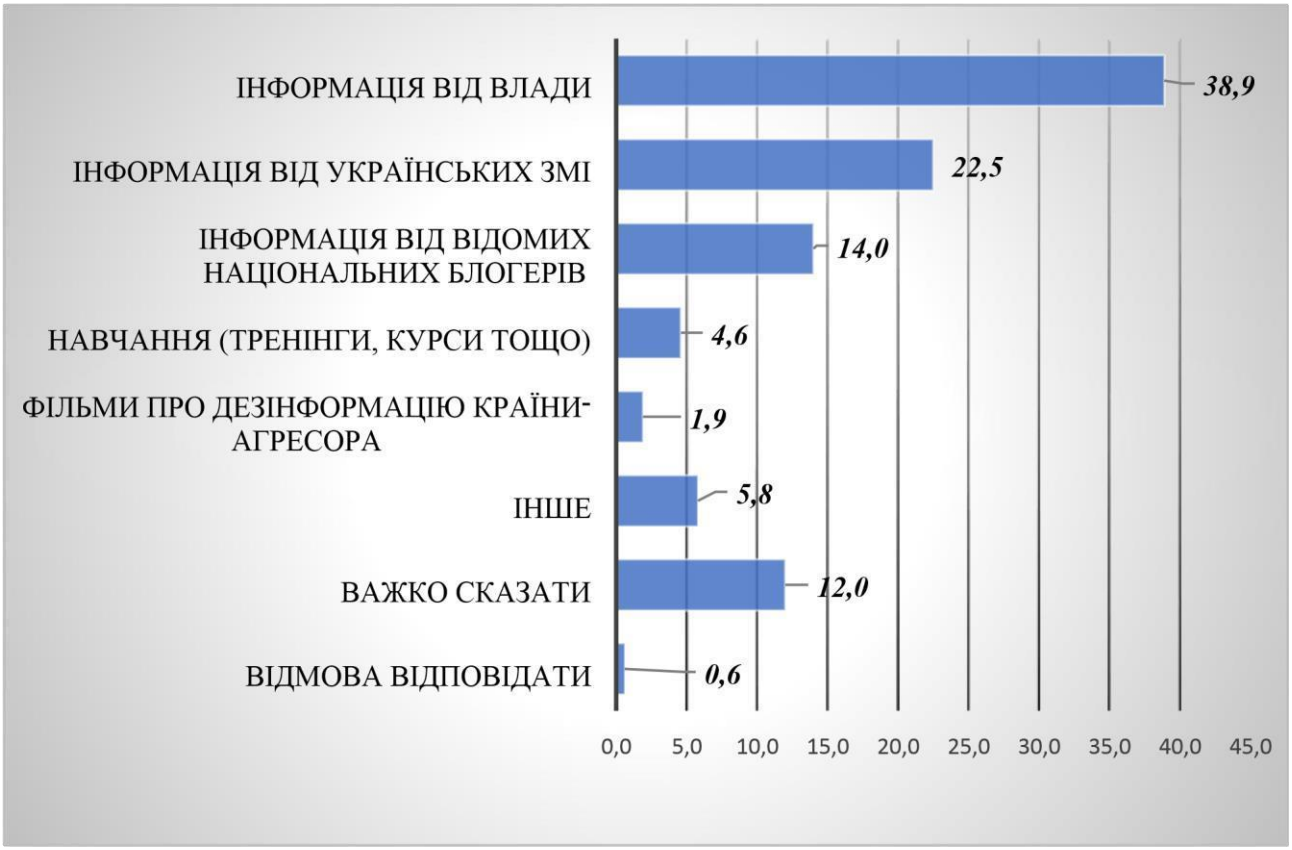

Рисунок 2.5 – Показники впливу допомоги в питаннях розпізнання дезінформацію після 24 лютого 2022 року у % [11]

Розвиток штучного інтелекту може стати інструментом для добра або зла. Його використання певним чином залежить лише від людей. За допомогою штучного інтелекту сьогодні фейки генеруються за декілька хвилин, а реальність і вигадка можуть настільки переплетені, що різницю між ними можна взагалі не помітити.

Під час опитування була поставлена мета щодо з'ясування усвідомлення українців всіх ризиків, які несе штучний інтелект. Отже, більше 60 відсотків респондентів вважають на створення дезінформації та на допомогу боротися з нею штучний інтелект впливає однаково. Таких людей більше, які проживають у місті (65,2%), ніж у селі (55%). Також молодь визначає однаковість впливу штучного інтелекту, ніж люди старшої вікової групи (рис. 2.6).

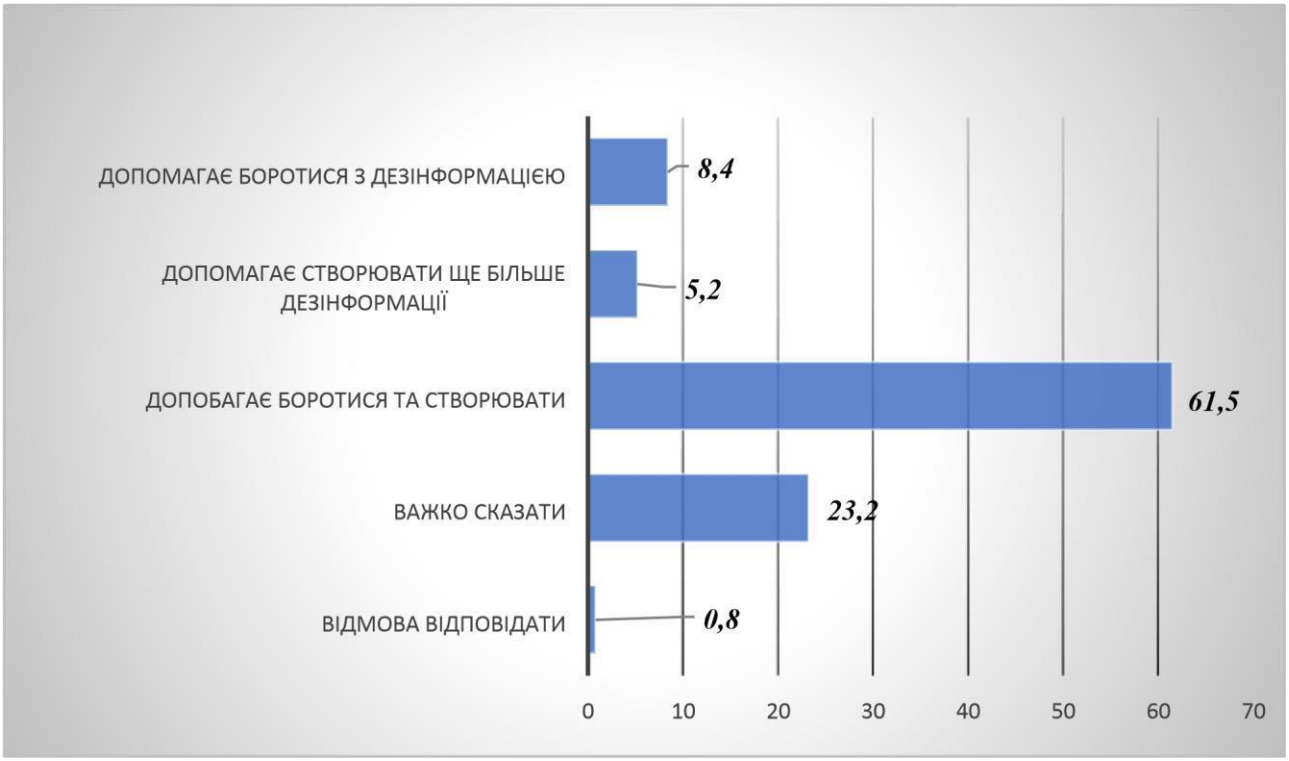

Рисунок 2.5 – Показники ступеня допомоги боротьби з дезінформацією за допомогою штучного інтелекту у % [11]

Зростаюча роль штучного інтелекту в сьогоденні, особливо в частині генерації контенту вимагає від суспільства обережності щодо ризику фейків та неправдивої інформації. Створення переконливих текстових, аудіо та візуальних матеріалів вже вводять в оману навіть самих досвідчених споживачів контенту.

Дані результати опитування суспільної думки дають лише загальне виявлення про те, як громадськість, яке є основною цільовою аудиторією заходів контрпропаганди та протидії неправдивій інформації, дає оцінку ефективності різним стейкхолдерам.

РОЗДІЛ 3 ШЛЯХИ УДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА МАНІПУЛЯЦІЯМ

3.1 Світовий досвід протидії дезінформації та маніпуляціям у країнах розвиненої демократії

Інформаційна діяльність й захист інформаційного простору будь-якої країни сьогодні, особливо в умовах загрози чи виникнення надзвичайних будьяких кризових явищ набуває актуальності. Недооцінюючи чи нехтуючи захистом інформаційного простору може призвести до непоправних втрат, які стосуються ресурсів, іміджів, репутації тощо.

Світові держави через важливість і складність зазначених питань, знаходяться в постійному процесі розробки дієвих інструментів й вживання ефективних заходів щодо захисту національного інформаційного простору. Так, запровадження захисту інформаційного простору Європейського Союзу ґрунтується на наступному:

– забезпечення максимальної прозорості щодо походження,

генерування, поширення інформації тощо, з метою надання можливості самим громадянам розуміти відповідний контент і виявляти можливі спроби маніпулювання чи дезінформування;

– підтримка різноманітність інформації, задля приймання громадянами обґрунтованих рішень на основі критичного аналізу;

– сприяння достовірності інформації через представлення доказів її надійності;

– запровадження інклюзивності, комплексності рішень [9].

Отже пропонуємо розглянути нормативно-правову організацію протидії дезінформації у таких державах, як політично-економічний союз Бенелюкс (Бельгія, Нідерланди та Люксюмбург), США, а також Центральної, Західної та

Північної частин Європи. Майже всі держави, які будемо аналізувати є членами Європейського Союзу. У зв’язку з цим, поширення дезінформації, забезпечується та контролюється не тільки національним законодавством, державних і недержавних ініціатив, а й певними нормами й інституціями Європейського Союзу.

Саме заходами координації комунікацій і протидії поширенню дезінформації через медіа соціального направлення з 2015 року Європейський Союз добивається змін поведінки саме соціальних медіа.

Уряд Люксембурги гарантує свободу слова та преси на законодавчому рівні. В країні не має прямого регулювання протидію дезінформації з боку державних органів і законодавства. Регулювання питань дезінформації здійснюється завдяки міжнародному координуванню, за допомогою Ресурсного центру економічного співробітництва та розвитку . Цілі діяльності цього центру стосуються розвитку спільних заходів, спрямованих на підвищення інформаційної грамотності та протидії дезінформації. Програма Bee Secure, метою якої є навчання дітей, молоді та їх батьків, вчителів тощо безпековому та відповідальному використанню цифрових технологій [35]. Крім освітніх компонентів зазначена платформа має також зворотній зв’язок при виявленні фейків, дезінформації тощо. Зазначена програма працює за чотирьома напрямками, а саме:

– підвищення обізнаності і інформації серед громадян;
– орієнтація та поради
– повідомлення про незаконний контент; – контроль.

З 2017 року в Люксембурзі запроваджена, за ініціативою місцевої неурядової організації, платформа respekt.lu, яка має фінансування від держави та приватних донорів. Основними завданнями зазначеної організації та

платформи є питання запобігання та протидії екстремізму насильства,

радикалізму у суспільстві, підтримки осіб, що стали їх жертвами. Крім того їх діяльність направлена на розробки програм з питань боротьби з дезінформацією, освітні заходи, відеоуроки тощо.

Боротьба з дезінформацією урядом Нідерландів відбувається через розроблені та впроваджені стратегії та освітні заходи. Однією з таких стратегій є загальнодержавна стратегія з питань ефективної боротьби з дезінформацією [57].

Метою цієї стратегії є зниження впливу дезінформації та інформування суспільства щодо питань національної безпеки, громадського здоров'я, а також соціально-економічної стабільності.

Також урядом Нідерландів, а точніше міністерством внутрішніх справ і королівських відносин, було розроблено посібник із протидії дезінформації для посадовців публічного управління, керівників закладів і установ з юридичними ініціативами та практичними порадами [58].

Розроблений урядом Нідерландів у 2021 році Кодекс що стосується прозорості політичної реклами в мережах інтернету для запобігання поширенню оманливої відповідної інформації під час проведення виборів. Потрібно зазначити, що кодекс направлений на добровільність та відкритість є для всіх, без виключень політичних партій та онлайн-платфор. Кодексом визначені відповідні вимоги для виборчої кампанії з питань прозорості відправника, ціни й охоплення реклами для

того, щоб політичні партії та кандидати уникали публікацій оманливих повідомлень і відмовлялися від іноземного фінансування.

Конституція Бельгії є основою в питаннях протидії поширення дезінформації. В головному Законі визначаються обмеження на свободу слова для боротьби з поширенням мови ворожнечі за статевими, расовими чи політичними ознаками. Сенатом Бельгії у 2022 році було розроблено 53 рекомендації, які стосувалися створення онлайн-контенту, розробки процедур з питань запобігання дезінформації та забезпечення повної прозорості політичної реклами.

Країни Центральної та Західної Європи найбільшу увагу приділяють вирішанню питань фейкових новин і наклепу, використовуючи механізми, які саморегулюють медіа, а вони, в свою чергу, займаються регуляцією і питаннями правильності та достовірності наданої інформації.

Закон про свободу преси у Франції прийнятий ще у 1981 році спрямований на захист свободи преси та боротьбу з неправдивою інформацією, який встановлює правові обмеження для медіаінформувань за наклепи і расистські заяви. Для осіб, які словесним чи візуальним способом в громадських місцях чи в засобах медіа. зробили такі заклики законом визначено штраф більше сорока тисяч євро або взагалі позбавлення строком на 1 рік. З часом уряд Франції розширив норми цього Закону в частині поширення дезінформації , встановивши штраф у сорок п’ять тисяч євро. Людська гідність, громадський порядок, права інших людей або національна безпека захищені у країні Законом про довіру до цифрової економіки.

З 2018 року У Франції діє Закон з питань маніпулювання інформації, який встановлює відповідальність для онлайн-платформи та надає інструменти для швидкого реагування на дезінформацію під час виборчих кампаній. В таких випадках суд має розглянути заяву позивача з питань неправдивої інформації протягом 48 годин з прийняттям рішення щодо її видалення [1].

Французький державний регуляторний орган для комунікацій аудіовізуальних і цифрових проводить роботу з питань захисту аудіовізуальних творів, веде боротьбу з піратством і запроваджує легальне споживання контенту, а також веде контроль за засобами боротьби з неправдивою інформацією, фейками та презирством в мережі Інтернет. Зазначений орган є гарантом дотримання норм

щодо захисту неповнолітніх, проведення виборчих заходів, реклами та відображення різноманітності суспільства. Також державний регуляторний орган виконує має контролюючи функції, які спрямовані на забезпечення безпеки, також розвитку цифрового простору.

Відсутність у Німеччині окремого закону, присвяченого боротьбі з неправдивою інформацією, заміщує закон що стосується удосконалення правозастосування в соціальних мережах. Таким чином, адміністратори платформ, відповідно до зазначеного закону, мають право на видалення з соціальних мереж різноманітних видів фейкової або незаконної інформації, наприклад, образів, зловмисних пліток, наклепів, публічного підбурювання до злочину, розпалювань

ненависті тощо. Цей Закон був прийнятий після став постійних зволікань Facebook з видалення публікацій, що мали порушення відповідно до стандартів соціальних мереж.

За розпалювання ненависті, поширення дезінформації, антисемітських висловлювань кримінальний кодекс Німеччини передбачає покарання до двох років тюрми або призначення штрафу.

Закон про медіа Австрії визначає обов'язки журналістів і захист свободи відповідно медіа, а також регулює випадки, за наклеп і висміювання яких можуть бути оштрафовані. Дотримання етичного кодексу якісними медіа та журналістськими асоціаціями є ключовими вимогами кодексу.

У 2022 році користувач твіттеру Іспанії отримав вирок, перший в історії країни, у вигляді п'ятнадцяти місяців ув'язнення та штрафу за неправдиве

звинувачення неповнолітнього іноземця.

Такі країни північної Європи, як Норвегія, Швеція, Данія та Фінляндія мають ефективну систему протидії неправдивій інформації. Завдяки високому рівню свободи слова та прозорості журналісти працюють в цих країнах незалежно та професійно, а населення зазначених країн володіють високим рівнем освіти та інформаційної грамотності.

Відповідно до нормативно-правових актів Фінляндії, якими встановлюються заходи протидії поширенню дезінформації, неправдива інформація з медіа та вебсайтів підлягає видаленню тільки за рішенням суду.

Свобода слова Швеції захищена Конституцією, а визначення меж свободи та санкцій за поширення фейків регулюються кримінальним кодексом країни. Крім Конституції та кримінального кодексу в частині протидії поширення неправдивої інформації діють закони проти наклепу, сприяння міжнаціональних ворожнеч, агітацій тощо. З 2022 року уряд Швеції утворив агентство психологічного захисту з повноваженнями виявлення та боротьби з дезінформацією, яка не стосується медіа. В той же час зазначене агентство має заборонену на стеження за громадянами країни, з фокусуванням на громадян та підприємства інших держав.

Робоча група при департаменті, який опікується питаннями мистецтва, туризму, гельської мови, культури, медіа та спорту Ірландії з 2023 року займається розробкою державної стратегії протидії неправдивій інформації. Основні напрямки національної стратегії включають координацію зусиль для боротьби з організованими кампаніями, які направленні на маніпуляції в Інтернеті, забезпечення прозорості в політиках модерації контенту, підтримку інновацій у перевірці фактів та досліджень фейків, стимулювання ініціатив з медіаграмотності.

З 2022 року Законом виборчої реформи розпочалася боротьба з дезінформацією в мережі Інтернету під час виборів і референдумів. Відповідно до закону власники медіаплатформ мають в повній мірі, сприяти виборчій комісії Республіки Ірландія, в частині розкриття інформації про фейки, маніпуляції та неавтентичну поведінку.

Під час пандемії COVID-19 урядом Великої Британії був створений Відділ із протидії дезінформації для моніторингу загальнодоступної інформації та спростування дезінформаційних повідомлень. З 2023 року діяльність цього відділу забезпечується Актом з онлайн-безпеки. Відповідно до Акту перед онлайнплатформами стає зобов’язання приймати заходи для запобігання поширенню незаконного або шкідливого контентів. Не виконання обов’язків може привести до накладання штрафу на суму до вісімнадцяти мільйонів фунтів стерлінгів або десяти відсотків від їхнього річного обороту. Також зазначений Акт з онлайнбезпеки дає право на блокування доступу до певних вебсайтів.

Якщо аналізувати систему нормативно-правового регулювання США сфери забезпечення інформаційної безпеки можна зазначити, що вона є складною та розгалуженою. Питання забезпечення безпеки інформації в основному регулюються федеральними законами країни. Саме Закон про інформаційну безпеку є першим законодавчим актом США фундаментального значення у сфері регулювання інформаційної безпеки [25], який визначив базові вимоги для забезпечення інформаційної безпеки федеральних інформаційних систем і став правовою основою

для створення цієї системи. На операторів всіх федеральних інформаційних систем країни покладалися зобов’язання щодо розробок власних планів забезпечення інформаційної безпеки.

Національна консультативна рада з інфраструктури, яка була створена у 2000 році разом зі схваленням щодо формувань спеціальних відомчих центрів з питань інформаційної безпеки, були наділені повноваженнями виявляти відповідні вторгнення та сповіщати, в свою чергу, державні, приватні та інші будь-які організації про можливі загрози інформаційній безпеці.

У 2002 році в США створюються Комітет та Міністерство внутрішньої безпеки, в свою чергу, у складі Міністерства утворюються декілька Управлінь, підрозділи Центр екстреного реагування, який займався на комп’ютерними інцидентами, але завданнями всіх відомств було саме зниження ризику для інформаційної інфраструктури США.

Окремі органи, що здійснюють нормативно-правове регулювання зазначеної сфери в США, в свою чергу, наділені повноваженнями щодо надання обов’язків до виконання нормативно-правових актів.

В той же час, зміцненням безпеки критичної інформаційної інфраструктури США, розташованої за межами країни, а також для сприяння обміну досвідом і кращими практиками, опікується Державний департамент разом з Міністерством національної безпеки та іншими федеральними органами, залучаючи до цього процесу іноземні уряди та міжнародні організації.

Таким чином, відповідне рекордна кількість різноманітних органів та нормативно-правових актів є певним чином особливістю американської моделі в питаннях регулювання сфери інформаційної безпеки, що ускладнює реалізацію такого підходу, наприклад, в Україні.

Можемо зробити висновок, що організаційна структура системи інформаційної безпеки США демонструє, на нашу думку, нерозривність взаємозв’язку між безпекою національного та воєнного напрямку та інформаційною,

адже регулюючими установами є Міністерство оборони та Міністерство внутрішньої безпеки.

Національний інститут стандартів та технологій є відповідальним за виконання нормативно-правових вимог в галузі забезпечення інформаційної безпеки та розробки відповідних стандартів, а також посібників, з проведенням наукових досліджень з питань виявлення загроз у сфері інформаційної безпеки, оцінювання їх масштабу, здійснення доцільних заходів щодо захисту, що використовуються в інформаційних системах державної та приватної форм власності.

Отже, можна зазначити, підходи зарубіжних країн в питаннях протидії дезінформації та взагалі інформаційної безпеки істотно різняться, а саме: - США – пріоритетність на забезпечення саме технічного захисту інформації, тобто на захист від зломів, хакерських атак тощо, в свою чергу, а питання ворожої дії, які направлені на критичну інформаційну інфраструктуру розглядаються в країні через призму інформаційної війни;

– США та країни Європи – однаковість у питанні захисту персональних даних, приватних відомостей, інтелектуальної власності. В країнах Європи система захисту персональних даних можна вважати, на нашу думку, більш підконтрольною;

- різні підходи до встановлення вимог щодо безпеки критичної інформаційної інфраструктури характеризуються розгалуженою структурою відомств у США з делегуванням у рамках ризик-орієнтованого підходу нагляду за виконанням вимог законодавства.

3.2 Напрями удосконалення рівня безпеки інформаційного простору України

Для сучасного світу характерним стають процеси все більшої взаємозалежності та взаємовпливу між країнами, що зумовлено самим розвитком світового співіснування на основі інформаційного суспільства та

глобальних цифрових комунікативних й інформаційних мереж.

Інформаційно-комунікаційний простір, створений за допомогою останніх, відіграє все більш важливу роль в організації суспільного, політичного та економічного життя кожної держави і, в той же, розвиток означених технологій продукує появу нових безпекових викликів і загроз, особливо посилених умовами виникнення міжнародних конфліктів чи воєнного протистояння, чому яскравим підтвердженням є сьогоднішня ситуація з безпекою національного інформаційного простору нашої країни в умовах прямої воєнної агресії сусідньої країни. Оскільки сучасний світовий інформаційний простір зумовлюється характером невід'ємних зв'язків між технологічним, соціальним та політичним спектром життя держави і суспільства, то здатен створити численні можливості для ефективної комунікації, якісної освіти, результативної комерції та різноманітних розваг і, водночас, спроможний на відкриття нових векторів розвитку потенційних загроз, зокрема, небезпечних викликів у сфері кібербезпеки та інформаційних війн, особливо в результаті реального чи потенційного міждержавного конфлікту, коли крім безпосередніх бойових дій, кібератаки та інформаційна війна стають дієвими інструментами і впливовими факторами гібридної воєнної стратегії. Мета вказаних дій полягає у підриві рівня довіри до національних інститутів, здійснення дестабілізації внутрішньої ситуації в середині країни, а також здійснення тиску на міжнародну спільноту в цілому. За таких обставин країна-агресор починає використовувати широкий спектр методів поширення дезінформації, маніпуляцій та фальсифікацій для коригування суспільними думками через соціальні медіа, а також задля підтримки антидержавних елементів та різного роду проксі всередині країни [8].

Поширення викривленої чи явно недостовірної інформації, нажаль, є суттєвим викликом для подальшого цивілізаційного розвитку сучасного інформаційного суспільства, оскільки дана тенденція сьогодні виступає вагомим фактором впливу на формування громадської думки, важелем корегування процесів прийняття політичних чи управлінських рішень. Крім того, дезінформація використовується як

раціональний спосіб ведення сучасних воєн, що отримали назву гібридних форм ведення війни. Україною на високому міжнародному рівні задекларовано прагнення розвиватись як демократична держава зі свободою слова, доступністю до джерел інформації, плюралізмом позицій, думок, суджень та правом вільного їх вислову, проте, зазначене вступає у протиріччя із обмеженнями, зумовленими наслідками воєнного часу, затребуваними самим розвитком історичних умов воєнного конфлікту, а тому потребують, з одного боку, здійснення збалансованого підходу до забезпечення високого рівня національної безпеки, з іншого – забезпечення дотримання основних демократичних цінностей в суспільстві, інформаційної відкритості та свободи.

Масштабним ресурсом поширення усього комплексу глобальних, національних, регіональних і локальних новин для їх споживачів в світовому масштабі віднині стали різні соціальні медіа, у першу чергу, розповсюджений га просторах інтернету тип віртуальних соціальних мереж, оскільки, недосконалість сучасної системи верифікації фактів, викладених у публікаціях з даних джерел, майже нерегульовані процеси в середині мережі інтернет перетворюють соціальні мережі на сприятливий ґрунт для масового поширення неперевіреного чи завідомо неправдивого інформаційного контенту. Ба більше, соціальними мережами забезпечено не тільки існування осередків розповсюдження фейкових новин, різного роду дезінформації та агресивної пропаганди, а й прискорення темпів і збільшення масштабів поширення означених негативних явищ. Сфабриковані і спотворені відносно правди новини суттєво впливають на розвиток суспільства, оскільки явно маніпулятивний і викривлений інформаційний контент легший у створенні та важчий у виявленні, а головні актори здійснення спланованої штучної дезінформації намагаються постійно змінювати тактику і стратегію подальшої діяльності у даному сегменті.

У сучасному світі значною кількістю держав використовуються пропаганда і дезінформація для збереження і зміцнення власних антидемократичних політичних режимів і посилення впливу на інші держави, їх управлінську систему та їх

населення та, нажаль, доводиться констатувати, що кількість останніх має тенденції до постійного зростання, що і актуалізує нагальні потреби розробки відповідних стратегій і технологій надійного захисту інформаційного й державного суверенітету країн [51].

В умовах повномасштабної збройної агресії, національний інформаційний простір знаходиться під перманентною загрозою втручання ззовні, викликами прагнень країни-агресора до інформаційної дестабілізації українського суспільства, внаслідок чого означена проблема актуалізує потребу своєчасного реагування та дієвої протидії негативним наслідкам гібридного тиску, здатних гарантувати збереження української державності, сприяти відсічі ворогові на всіх напрямках протистояння, в тому числі і на інформаційному фронті. Маніпуляція наявними фактами, спотворення змісту інформації, цілеспрямоване поширення дезінформації, фальсифікація сутності наслідків подій і явищ, поширення мови ворожнечі, застосування різних форм і напрямів здійснення кібератак на стратегічно важливі об’єкти інфраструктури і національної безпеки продукують виникнення серйозних проблем у сфері національної безпеки країни, посилених тим, що чинні на сьогодні та наявні в цивілізованому світі механізми протидії даним викликам не завжди є результативними в умовах нових методів здійснення кібератак, поширення дезінформації та її руйнівного впливу на суспільну свідомість, на рівень стабільності в державі й суспільстві.

Актуальність та важливість означеної проблеми сьогодення породжує затребувану часом і обставинами воєнного протистояння зовнішній агресії необхідність розроблення і пошуку відповідних ступеню загрози та дієвих за кінцевими результатами механізмів захисту від кібератак, протидії дезінформації, фальсифікаціям, викривленням та відвертій брехні, вироблення ефективної національної стратегії протидії комплексу ворожої дезінформації та маніпуляціям, а також визначення дієвих форм співпраці між різними стратами українського суспільства для всебічного протистояння іншим деструктивним тенденціям в інформаційному просторі України [28].

Дезінформація та маніпулятивні технології визнаються значною загрозою українському суспільству і у відносно мирний час, і, особливо, у час війни, оскільки не мають однієї і єдиної першопричини виникнення та поширення, а тому відсутні загальні й однолінійні механізмі запобігання і методи вирішення посталих внаслідок означеної небезпеки проблем. Врахування різних аспектів і причиннонаслідкових зв'язків допомагатиме розкриттю та розумінню механізмів, що застосовуються задля поширення дезінформації, що, в першу чергу, дозволить стимулювати розвиток ефективних стратегій боротьби із цим явищем. Враховуючи означені виклики, протидія дезінформації та маніпуляціям в інформаційному просторі набуває рис необхідної і затребуваної діяльності для збереження гармонії в суспільстві, зовнішньої, внутрішньої соціальної та політичної стабільності.

Визнання ступеню усієї небезпеки, що породжується агресивною політикою поширення дезінформації та маніпулятивного впливу, на вищому законодавчому рівні нашої держави ще у довоєнний час були зроблені перші суттєві кроки у напрямку нормативного забезпечення публічної діяльності з реалізації окремих аспектів державної політики протидії означеним інформаційним викликам, зокрема, це стосується оновлення Стратегії національної безпеки України [45] та інших нормативних документів, зокрема Стратегії забезпечення державної безпеки [49], Стратегії інформаційної безпеки [30], положеннями і нормами яких врегульовуються питання інформаційної безпеки нашої держави, що посилює ефективність боротьби з дезінформацією і маніпуляціями як стратегічно важливою формою діяльності держави та її інституцій, інституту громадянського суспільства для зміцнення міжнародного іміджу та міжнародної репутації Української держави, а також сприяння подальшому розвитку позитивних для неї міжнародних відносин.

У внутрішньому житті, посилення дієвості національних механізмів виявлення та протидії дезінформації і маніпулятивним викривленням в національному інформаційному просторі є важливою необхідністю для стабілізації функціонування держави як на рівні внутрішнього розвитку, так і на міжнародній арені.

З часу початку збройної агресії сусідньої держави, форми, методи та стратегії ворожих кібератак на український інформаційний простір зазнали відчутних змін у напрямі більшої виваженості підготовки, більшого рівня розрахування, більшого ступеню тонкощів реалізації та багатоаспектного характеру. Замість використання прямих атак на конкретно визначені цілі, сьогодні як найчастіше застосовуються методи та технології соціальної інженерії або наміри цілеспрямованого обману суспільства, окремих його складових чи індивідів задля отримання прямого доступу до різного виду конфіденційності тієї чи іншої інформації.

Поширеними і показовими тенденціями, вкоріненими у чинну практику втручання у сферу національного кіберпростору, стали прагнення змін фокусу задіяних пошкоджень – від ініціації звичайних перебоїв в роботі інформаційних систем до сприяння значному витоку важливої інформації, що може бути використана для організації міжнародного чи внутрішнього політичного та, навіть, військового тиску чи шантажу.

Спостерігається останнім часом зростання питомої ваги тактик, що передбачають підготовку і організацію довготривалих кампаній у напрямі дестабілізації або руйнування мережевих комунікацій віддаленого характеру, використовуючи вірусні технології та програми.

Основними серед означених загроз для інформаційної безпеки нашої держави стали кібератаки, націлені на пошкодження критичної інфраструктури, на сферу діяльності державних інституцій та організація масових кампаній дезінформації, пропаганди та маніпуляцій суспільною думкою, що мають за мету підрив довіру до національних державних інститутів та суспільства в цілому.

Негативний вплив дезінформації, пропаганди та маніпуляцій на українське суспільство, окремих громадян та на інформаційний простір, як і саме явище дезінформації, маніпуляції та пропаганди, за увесь час військової агресії перетворились на потужні інструменти і важелі деструктивного впливу в руках країни-агресора, оскільки активно використовуються задля маніпуляцій

громадською думкою, підриву рівня довіри до національного уряду, створення і підтримки ознак суспільного напруження та суспільного розколу.

Соціальні мережі та соціальні медіа формують собою основне поле для зазначених атак, проте не менш активно вони також проводяться через традиційні мас-медіа та інші сучасні канали суспільної комунікації, більше того, сучасні інформаційно-комунікаційні технології, розвиток штучного інтелекту, електронне діловодство, зберігання та обмін персональними даними, сприяють появі абсолютно нових можливостей для кібератак, протистояти яким стає дедалі важче, захиститись від яких стає надто складно і технологічно, і ментально.

Водночас, прогрес новітніх технологій, в свою чергу, продукує винайдення нових дієвих інструментів для такого потрібного і затребуваного часом захисту та автоматизованого виявлення небезпечних загроз, створення сучасних захищених новітніми можливостями систем.

З метою забезпечення надійності функціонування єдиного інформаційного простору України, необхідним виявляється дотримання алгоритму сформульованих і закріплених злагоджених дій як на рівні владних інститутів держави, так і на рівні приватного сектору та громадського компоненту здійснення відповідної державної політики.

Даний алгоритм кроків і заходів задля збільшення ефективності забезпечення інформаційного простору держави надійним захистом і можливістю протистояти дезінформації, маніпуляціям та ворожій пропаганді, на наш погляд, має включати:

1. Розробку та запровадження нової стратегії забезпечення кібербезпеки, якою має бути охоплено різнобічні аспекти виявлення, захисту, протидії кібератакам, спрямованих, першочергово, на захист національної системи об’єктів критичної інфраструктури, державно-владних, публічноуправлінських та самоврядних інституцій, а також інтересів приватних осіб. що повинна мати гнучкість для адаптування до швидко змінюваних тактик і стратегій противника.

2. Модернізацію національної системи інформаційного навчання і освіти, оскільки сучасні інформаційно-комунікаційні технології мають тенденцію до

постійного розвитку, а тому відповідне і постійне спеціалізоване навчання, освіта та підвищення професійної кваліфікації у зазначеній сфері є вкрай затребуваними та необхідними задля посилення ступеню національної інформаційної безпеки.

3. Сприяння процесам посилення міжнародної співпраці України у сфері інформаційних технологій та кібербезпеки, що дозволить вчасно скористатися передовим міжнародним досвідом і надійною підтримкою країнпартнерів у протидії кібератакам. Означений процес співробітництва необхідно включатиме обмін затребуваною інформацією про існуючі чи потенційні загрози, запозичення кращих світових технологій та елементів світових практик протидії гібридним викликам і загрозам, тісну і плідну співпрацю в розкритті і розслідуванні злочинів у кіберпросторі тощо.

4. Посилення боротьби з дезінформацією, маніпуляціями та пропагандою, що може містити необхідність розробки технологій по ідентифікації та контролю поширення дезінформації, запровадження освітніх програм для населення щодо виявлення та обробки дезінформації.

5. Додаткові інвестиції в забезпечення інновацій та технологій, якими має бути забезпечено дієву допомогу у політиці захисту від кібератак, що потребує крім державних, додаткових інвестиційних проектів для її ефективного впровадження, впровадження заходів активного стимулювання інновацій в цій галузі шляхом державного фінансування, здійснення заходів державноприватного партнерства, міжнародної співпраці та залучення різного роду додаткових інвестицій. Основними методами боротьби з ворожою пропагандою та дезінформацією в Україні слід визнати запровадження комплексного підходу до формування і впровадження означених заходів, оскільки лише в такому разі забезпечується сукупність та злагодженість дій, а їх результати будуть досягати високого й якісного рівня.

До комплексу зазначених заходів слід нагально включити організовану діяльність та політику державного регулювання і забезпечення:

1. Прозорості діяльності і процесів в соціальних медіа, відкритих і цивілізованих методів моніторингу наявної в них інформації, що визначатимуть, яка інформація і з яких джерел доходить безпосередньо до користувачів.

2. Здійснення державної регуляції і політики необхідних санкцій, що включатиме прийняття відповідних законів та норм державної регуляції, якими будуть встановлені види моральної та юридичної відповідальності за поширення в мережах відвертої дезінформації чи агресивної пропаганди.

3. Політики постійного підвищення рівня громадської обізнаності через проведення публічних і загальнодоступних кампаній з інформування

громадськості розуміння того, як, хто і, головне, чому поширює дезінформацію.

4. Продовження тісної співпраці з міжнародними партнерами України у сфері боротьби з дезінформацією на міжнародному рівні, здійснення міжнародного обміну кращими світовими практиками та досвідом координації спільних дій.

Слід наголосити на тому, що сучасні підходи, застосовані Україною у напрямі протидії кібератакам та іншим видам загроз, послуговуються досвідом і напрацюваннями сучасних західних практик, а на національному рівні знайшли власну універсальність і свою унікальність. Станом на сьогодні в Україні спільно із іншими країнами світу активно працюють над розробкою стратегій подальшої протидії кібератакам з боку країни-агресора, що включають в себе кілька

складових і ключових напрямів,

І нарешті, важливою складової успішної протидії ворожій дезінформації, маніпуляціям і агресивній пропаганді має стати національне українське законодавство та нормативно-правова база здійснення такого виду діяльності, адаптоване до новітніх викликів, здане унормувати діяльність з протидії загрозам на основі світових технологічних стандартів, що постають в результаті

цивілізаційного прогресу й якісних трансформацій у тактиці та стратегії ведення інформаційних війн, враховуючи темпи розвитку сучасних технологій та

змінний характер політичної ситуації, необхідність перегляду й оновлення концепцій забезпечення національної інформаційної безпеки.

Підводячи підсумок маємо зазначити на тому, що адаптація означених стратегій щодо здійснення ефективної національної безпекової політики та захисту інформаційного простору України на сучасному етапі державотворення потребує подальшого розроблення, актуалізації, розвитку та удосконалення.

Після початку повномасштабного вторгнення в Україну військ країниагресора чинна концепція безпеки національного інформаційного простору багато в чому залежить від діяльності державних публічно-владних установ та інформаційних інститутів, всебічної підтримки з боку країн-партнерів та міжнародного співробітництва у сфері міжнародної інформаційної безпеки, спільного захисту та збереження національних суверенітету та державності.

ВИСНОВКИ

У магістерській роботі здійснено узагальнення актуального завдання, що полягає у теоретичному обґрунтуванні засад вироблення державної політики у сфері протидії дезінформації та маніпуляціям та визначення напрямів щодо їх вдосконалення в умовах цифровізації. Отриманим в процесі дослідження результатами підтверджуються досягнення поставленої мети й вирішення завдань, сформульовані наступні висновки і практичні рекомендації.

1. *Уточнено* понятійно-категорійний апарат у сфері протидії дезінформації та маніпуляціям в цифровому просторі, зокрема з'ясовано, що термін «цифровий простір» є більш широким поняттям, ніж Інтернет-мережа, який охоплює не лише веб-сайти або веб-сторінки, як частини веб-сайтів, файли та оцифровані об'єкти інтелектуальної власності, електронні документи, а й усі пристрої в яких не передбачено паперова форма документообігу, тобто «гаджети»: планшети, комп'ютери, носії інформації, ноутбуки, телефони тощо. Таким чином, цифровий простір штучно створений за допомогою цифрових технологій, який забезпечує його учасникам нескінченне число внутрішніх ступенів свободи.

З'ясовано, що поняття «дезінформація» може бути інформацією неправдивою та навмисно спотвореною з результатом заподіяння шкоди особі або окремій соціальній групі, чи взагалі організації або країні та «помилковою інформацією», що містить також неправдиву інформацію, але без мети заподіяння шкоди. Таким чином, для визначення поняття «дезінформація» в сучасних наукових дослідженнях та документах Європейського Союзу наразі застосовуються різні термінології, які можуть стосуватися фейків, дезінформації, пропаганди, маніпулювання інформацією, інформаційним розладам, гібридній війні. Дезінформація має спрямованість на маніпуляцію свідомістю людини.

В свою чергу, поняття «маніпуляція» – це спосіб скритого управління, найчастіше задля брехні та отримання односторонньої вигоди. *Окреслено* головні ознаки цього поняття:

– інформаційно-психологічна дія маніпулятора на свідомість, психіку однієї людини або всього колективу людей, без фізичного насильства, але може бути кроком до застосування насильства;

– прихована маніпуляція – вид маніпуляції розрахований на повний успіх коли той, на кого направлена інформація, вірить їй та сприймає все за дійсність;

– маніпуляція з вимогами майстерності – вид маніпуляції розраховується на масовість (суспільна свідомість, політика) та забезпечується спеціальними фахівцями та спеціальними знаннями.

Також *з'ясовано,* що такі поняття, як «фейк», «брехня», та «обман» є базовими будь-якої дезінформації та маніпуляції та активно використовуються.

2. *Наголошено*, що формування інститутів для захисту інформаційного простору держави є складним і багатогранним процесом, який потребує всебічного підходу до його організації з боку як держави, так і суспільства. *Визначено*, що сучасний інформаційний простір має кілька ключових характеристик, а саме: по-перше – постійне розширення, з охопленням різних сфер людської життєдіяльності, які впливають на повсякденне життя та соціальні відносини; по-друге – відображання в інформаційному просторі соціальної реальності, тобто створення своїх цифрових аналогів, що спотворюють та підміняють традиційну реальність; по-третє – здатність простору генерувати наслідки негативного характеру для інформаційної безпеки особи, з застосуванням підвищеного інформаційного тиску, маніпулювання думкою громадськості.

Для забезпечення дієвого функціонування цифрового простору важливо гарантувати інформаційну безпеку країни, що передбачає створення умов для безперебійної роботи інформаційної інфраструктури, вжиття заходів щодо захисту

інформації від несанкціонованого доступу, незаконного поширення, а також боротьбу з дезінформацією та маніпуляціями.

Визначено, що ефективно протидіяти дезінформаційним впливам, особливо сьогодні під час російської агресії можливо лише при наявності чітко сформованих інституційно-правових засаду у сфері протидії дезінформації та маніпуляціям, прояви яких в Україні, набувають системного характеру.

Здобутками цього напряму можна вважати:

- діяльність регуляторних органів – функціонування державних установ, які несуть відповідальність за контроль та протидію дезінформації (Національна рада з питань телебачення і радіомовлення, Центр протидії дезінформації, Центр стратегічних комунікацій та інформаційної безпеки тощо);

- система законодавства – розроблення низки нормативно-правових актів, що відносяться до сфери інформаційної безпеки та протидії дезінформації; – співпраця з міжнародними організаціями – активна співпраця з міжнародними партнерами для обміну досвідом у визначеній боротьбі;

- освітня діяльність – реалізація програм, підвищення обізнаності громадян з окреслених питань та інструментів їх подолання, тощо.

Але потрібно зазначити, що наразі в Україні досі відсутнє на законодавчому рівні поняття «дезінформації», що в свою чергу, впливає на формування інституційно-правових засад відповідно протидії цьому явищу. В Законі України «Про інформацію» визначається тільки достовірність і повнота інформації, а в Законі України «Про медіа» зобов’язує журналістів і творців надавати об’єктивну і достовірну інформацію та перевіряти її.

Визначено, що ефективність інституційно-правових засад протидії дезінформації та маніпуляціям в цифровому просторі, залежить від таких чинників, як: проведення оцінки реальної ефективності діючих правових норм; адаптації до нових викликів, що включає швидкий розвиток технологій, наприклад таких, як соціальні мережі та штучний інтелект; використання світового досвіду у протидії

дезінформації та маніпуляціям; створення партнерства між державними органами, медіа та неурядовими організаціями для розробки комплексних рішень; розроблення освітніх програм для підвищення медіаграмотності серед населення країни; запровадження системи моніторингу ефективності національних заходів у боротьбі з дезінформацією та створення механізмів оцінки їх результативності.

3. Сьогодні інформаційна сфера має вирішальне значення не тільки в умовах стабільності, а й під час загрози надзвичайних ситуацій або в періоди криз. Під час повномасштабного вторгнення Російської Федерації на території нашої держави знову було продемонстровано важливість точної, достовірної та своєчасної інформації для підтримки громадського порядку та безпеки в умовах кризових ситуацій.

Досліджено процес формування та розвитку сучасної політики зарубіжних країн (розвинутих країн Європи та США) в сфері боротьби з дезінформацією показало зміну напрямів і підходів до розв'язання цієї проблеми. *Наголошено,* якщо на початку активної діяльності країн Європи в питаннях боротьби з дезінформацією та маніпулятивними впливами заходи щодо їх подолання були максимально лояльними та зосередженими на стратегічних комунікаціях і просвітницькій діяльності, фактично не допускаючи введення обмежень на поширення недостовірної інформації та блокування контенту й ресурсів, то сьогодні політика реагування змінена, про що свідчать, зокрема, положення Посиленого кодексу практики щодо дезінформації.

Окреслено, основні кроки діяльності урядів зарубіжних країн у сфері протидії дезінформації, які при більш детальному вивчені можуть бути імплементовані у відповідну практику України, і визначаються: у розвитку інструментів для виявлення та реагування на деструктивні інформаційні впливи, ефективній комунікації та координації відповідних дій, спільному вирішенні проблем, підвищенні медіаграмотності громадян країни (забезпечення стійкості

населення до дезінформації), підтримці та сприянні діяльності незалежних медіа та громадських ініціатив, саморегуляції онлайн-простору та встановленні правил поширення інформації в кіберпросторі

4. *Наголошено*, що на даний час інформаційний цифровий простір нашої країни максимально перенасичений різноманітними інформаційними ресурсами, забрудненнями та переповнений недостовірною, а часто й просто фейками. Саме несанкціоновані втручання у внутрішні цифрові ресурси користувачів призводять до нав'язування їм шкідливої, зовсім непотрібної, взагалі незатребуваної інформації. У всьому світі, як й в Україні останніми роками найпопулярнішим джерелом інформації є цифровий простір, а точніше

Інтернет.

Зазначено, що до 2014 року наша країна не приділяла належної уваги рівню загрози в цифровому інформаційному просторі, тобто, не визнавала або не бажала визнавати рівень негативного інформаційного впливу сусідньої країни. Через вільний доступ в Україні телеканалів сусідньої країни українська аудиторія знаходилася в полі постійної уваги пропагандистів, російського контенту, політтехнологів. Отже, *з'ясовано,* що повномасштабне вторгнення Російської Федерації на територію нашої країни призвело до активізації суспільства України в інформаційному цифровому полі. Так, більше 60 відсотків українців почали отримувати новини через телеграм-канали саме після 24 лютого 2022 року, тоді як до цього часу лише 36 відсотків ознайомлювалися з новинами через телеграмканали. Майже всі 85 % громадян усіх регіонів України вважають, що країнаагресор стала поширювати більше фейків та неправдивої інформації. 35 % громадян дали високу оцінку ефективності протидії неправдивій інформації, ще 50% означили часткову ефективність.

Визначено, що допомогу у розпізнаванні дезінформації 40 % українців сподівалися отримати від органів влади, а 22,5 відсотків – від національних

засобів масової інформації, і тільки 14 % надію покладають на інформацію від блогерів. Однак, певне занепокоєння викликає втрата бажання людей до навчання. Тільки 5 % громадян вважають, що тренінги, онлайн-курси тощо могли б допомогти їм ефективніше розпізнавати інформацію стосовно фейків, дезінформації та ін.

5. *Визначено основні напрями* посилення безпеки в інформаційному просторі України та визначено основні шляхи їх удосконалення. *Визначено*, що здійснення протидії ворожій дезінформації затребує комплексу підходів до поєднання сучасних технологій, національних і міжнародних заходів, ініціатив та тісного співробітництва, оскільки саме на світовому рівні сконцентровані наявні ресурси, ефективні практики та унікальний міжнародний досвід протидії дезінформації, маніпуляціям та агресивній ворожій пропаганді, вироблено перевірену часом систему заходів посилення стійкості національного інформаційного простору до негативних викликів і наслідків зовнішнього втручання. *Наголошено* на тому, що для нашої країни неперервний потік дезінформації в умовах повномасштабної війни залишається серйозною загрозою, оскільки саме остання набула ознак і перетворилась на важливий інструмент деструктивного впливу країни-агресора.

Доведено, що ефективна протидія кібератакам, боротьба з пропагандою, маніпуляціями та дезінформацією, а також співпраця на міжнародному рівні є важливими інструментами в цій боротьбі та мають і надалі включати в себе, зокрема: розробку та запровадження узгоджених на міжнародному рівні національних стратегій посилення рівня кібербезпеки, що містять низку основоположних напрямів потенційного розвитку даної сфери співробітництва; взаємодопомогу у розробці останніх, на основі запровадження інновацій, новітніх технологій у сфері кібербезпеки; підвищення дієвості спільних заходів з кібероборони, що, на основі вже розроблених і впроваджених технологій,

включає в себе зміцнення інфраструктури кіберпростору та інтенсифікацію спеціальної підготовки кадрів у сфері інформаційної безпеки; продовження міжнародної співпраці і співробітництва з країнами-членами Північно-Атлантичного Альянсу та Європейського Союзу, зважаючи на закріплений конституційно євроатлантичний вектор розвитку нашої держави, а також з рядом інших країн, що стикаються сьогодні із аналогічними викликами та загрозами з боку агресора.

Наголошено, що спільні зусилля і надалі включатимуть в себе необхідність обміну інформацією, затребувану рівнем загрози координацію спільних дій та організацію спільних навчань, проведення законодавчих реформ, внесення законодавчих змін, що на нормативно-правовому рівні, на законних підставах дозволяють здійснювати виявлення, розслідування та юридичне покарання протизаконних дій у світовому інформаційному просторі. Означені підходи до організації міжнародної співпраці, створюють сучасну, дієву та результативну міжнародну систему протидії кіберзагрозам та іншим безпековим викликам, що стали сьогодні загальносвітовою тенденцією, оскільки лише спільною та плідною діяльністю усіх зацікавлених сторін можливе досягнення спільного завдання – дієва та результативна протидія посталим загрозам, які є реальністю сьогодення в інформаційному просторі Української держави та поза її межами.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Барановська П., Півторак О., Колдомасов А. Аналізуємо, яку інфраструктуру для боротьби з дезінформацією створили у Західній Європі. 2024. . URL: https://ms.detector.media/propaganda-ta-vplivi/post/36288/20240928yak-vlashtovana-protydiya-dezinformatsii-na-zakhodi-tapivnochi-ievropyatakozhna-brytanskykh-ostrovakh/ (дата звернення: 12.09.2024).

2. Бондар В. Т. Особливості інформаційної політики Євросоюзу з протидії онлайн дезінформації: досвід для України. Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування, 2023. Вип. 9. С. 1–5.

3. Брижко В.М. Філософія права: юридична онтологія у сфері інформаційного права. *Інформація і право.* № 3(6)/2012. С. 14-21.

4. Брижко В.М., Дзьобань О.П. Дезінформація як фактор маніпулювання свідомістю *Інформація і право.* № 2(45). 2023. URL : http://il.ippi.org.ua/article/view/282318 (дата звернення : 15.09.2024).

5. Брижко В.М., Фурашев В.М. Інформаційне право та інформаційне законодавство. 2-ге вид., доп. Харків: Видавництво «Право», 2021. 288 с. С. 10-20.

6. Вільчинська І. Ю. Неправдива інформація як засіб маніпулятивної взаємодії. Інформаційна освіта та професійно-комунікативні технології XXI століття : матер. XII Міжнар. наук.-практ. конф. Одеса, 2021. С. 105–108.

7. Вінник О. Нормативно-правове регулювання відносин у сфері цифрової економіки. Зовнішня торгівля: економіка, фінанси, право. 2018. № 2. С. 124–135. URL: http://nbuv.gov.ua/UJRN/uazt_2018_2_15 (дата звернення : 15.09.2024).

8. Галіпчак В. Д. Безпека інформаційного простору України в умовах російської агресії на сучасному етапі: основні завдання та виклики. *Регіональні студії*. 2023. № 34. С. 81–85.

9. Глобенко С. В. Європейський концепт протидії дезінформаційним проявам у державному інформаційному просторі. Актуальні проблеми управління інформаційною безпекою держави : зб. матеріалів XIV Всеукр. наук.практ. конф. (30 берез. 2023, м. Київ) / НА СБУ ; Ін-т модернізації змісту освіти МОН України. Київ, 2023. С. 451–453.

10. Глобенко С. В. Стратегії та пріоритети держави щодо захисту 158 інформаційного простору в умовах надзвичайних ситуацій. Актуальні питання сучасної стратегії розвитку України: виклики, пріоритети та прогнози : зб. наук. праць за матеріалами III наук.-практ. онлайн-конф. студ., аспір. і молодих вчених (25 листоп. 2022, м. Київ) / ВМУРоЛ «Україна», Ін-т права та сусп. відносин, каф. міжнар. відносин та політ. консалтингу. Київ, 2022. С. 37–38.

11. Горбик Р., Дуцик Д., Шалайський С. Ефективність протидії російській дезінформації в Україні в умовах повномасштабної війни. Аналітичний звіт. ГО «Український інститут медіа та комунікації», 2023. 66 с. URL : https://law.chnu.edu.ua/dezinformatsiia-yak-rozpiznaty-ta-borotysia/ (дата звернення : 16.07.2024).

12. Гороховський О.М. Фактчек як тренд розслідувань: можливості та перспективи. Дніпро: Ліра, 2017. 133 с.

13. Грачов Г., Мірошник І. Маніпулювання особистістю: організація, способи й технології інформаційно-психологічного впливу. URL: //www.gumer.info.bibliotek_Buks.Psihol.Grach.intro.php (дата звернення : 15.09.2024).

14. Державний центр кіберзахисту Державної служби спеціального зв’язку та захисту інформації України. URL : https://scpc.gov.ua/uk (дата звернення: 20.09.2024).

15. Деякі питання діяльності Міністерства культури та інформаційної політики : постанова Кабінету Міністрів України від 16.10.2019 № 885 Дата оновлення : 24.09.2024. URL: https://zakon.rada.gov.ua/laws/show/885-2019%D0%BF#Text (дата звернення: 04.10.2024).

16. Дзьобань О.П. Маніпулятивний характер інформаційного середовища сучасного суспільства. *Інформація і право.* № 3 (12). 2014. С. 3-12.

17. Дзюба Т. М. Обґрунтування концептуальних положень інформаційної безпеки України. Наука і оборона. 2021. № 3. С. 41–46.

18. Дяковський О., Габрелян А. Основні засади та принципи протидії дезінформації. Юридичний вісник. № 4. 2024. URL : http://yurvisnyk.in.ua/v4_2024/6.pdf (дата звернення : 16.10.2024).

19. Євсюкова О. В., Кузьменкова К.С. Формування інституційноправових засад протидії дезінформації в України. *Наукові перспективи*: журнал. 2024. № 10(52) 2024. URL : http://perspectives.pp.ua/index.php/np/issue/view/290/389 (дата звернення : 26.09.2024).

20. Звоздецька О. Дезінформація як загроза національній безпеці Європейського Союзу: проблеми та підходи. *Історико-політичні проблеми сучасного світу*. 2021. Т. 43. С. 30-39.

21. Кіца М. О. Фейкова інформація в українських соціальних медіа: поняття, види, вплив на аудиторію. URL: http://nz.uad.lviv.ua/static/media/1 – 52/36.pdf (дата звернення: 25.09.2024).

22. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 р. № 8073-X. Дата оновлення : 25.10.2024. URL : https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення : 30.10.2024).

23. Конституція України від 28.06.1996 р. № 254к/96-ВР. Відомості Верховної Ради України (ВВР), 1996. № 30. Ст. 141.

24. Костючков С. К. Нейрокогнітивний хакінг як інструмент активізації кіберконфліктного простору в умовах глобалізованого світу. *Актуальні*

проблеми філософії та соціології. Політологія. 2022. URL : http://apfs.nuoua.od.ua/archive/38_2022/10.pdf (дата звернення : 16.09.2024).

25. Кримінальний кодекс України від 05.04.2001 р. № 2341-III. Дата оновлення : 21.11.2024. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення : 30.11.2024).

26. Куйбіда В.С., Карпенко О.В., Наместнік В.В. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. Вісник НАДУ при

Президентові України (Серія «Державне управління»). 2018, № 1, С. 5-10. URL: http://academy.gov.ua/infpol/pages/dop/2/files/974f8478-cfe8-4d31-

971bd5116efff458.pdf?fbclid=IwAR2N7BfJ4wqtZLIw1IGX60L6tLJd9FYi4yvHy S Dn2fT-_7-gYwofaqzcEw (дата звернення : 15.09.2024).

27. Культура бойкоту: скільки українців підтримують бойкотування р та російського контенту. VisitUkrain today. URL: https://visitukraine.today/ uk/blog/1971/boycott-culture-how-manyukrainianssupportboycottingrussiansandrussian-content (дата звернення: 07.09.2024).

28. Литвин Н. А., Ярош А. О. Вплив дезінформації на національну безпеку України в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2024. № 2. URL: file:///C:/Users/%D0%92%D0%B5%D1%80%

D0%BD%D1%8B%D0%B9%20%D1%81%D0%BE%D1%80%D0%B0%D1%82 %

D0%BD%D0%B8%D0%BA/Downloads/3.3%20%D0%9F%D0%9E%D0%A1% D0

%9C%D0%9E%D0%A2%D0%A0%D0%95%D0%A2%D0%AC.pdf (дата звернення: 19.11.24)

29. Миронюк О**.** Дезінформація: як розпізнати та боротися. 2023. URL :

https://law.chnu.edu.ua/dezinformatsiia-yak-rozpiznaty-ta-borotysia/ (дата звернення : 16.10.2024).

30. Мудра І. Поняття «фейк» та його види у ЗМІ. URL: http://old.journ.lnu.edu.ua/vypusk7/n15/tv15 – 25.pdf (дата звернення: 05.09.2024).

31. Перелік осіб, які створюють загрозу національній безпеці: офіційний сайт Ради національної безпеки і оборони України. 2024. URL: https://www.rnbo.gov.ua/ua/Diialnist/5903.html (дата звернення: 07.10.2024).

32. Питання Центру протидії дезінформації : указ Президента України від 07.05.2021 № 187/2021. Офіційний вісник України. 2021. № 39. С. 33.

33. Посібник з протидії дезінформації / РНБО України, Центр протидії дезінформації. Київ, 2023. 60 с.

34. Почепцов Г. Інформаційні війни. Київ: «Ваклер». 2000. 574 с.

35. Презентація та місія BEE SECURE. URL: https://stopline.bee-secure.lu/ (дата звернення: 12.09.2024).

36. Про видавничу справу: Закон України від 05.06.1997 р. 318/97. Дата оновлення : 15.11.2024. URL : https://zakon.rada.gov.ua/laws/show/318/97%D0%B2%D1%80#Text (дата звернення : 17.11.2024).

37. Про громадські об’єднання: Закон України від 22.03.2012 р. № 4572VI. Дата оновлення : 03.09.2024. URL : https://zakon.rada.gov.ua/laws/show/457217#Text (дата звернення : 17.10.2024).

38. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення : 15.11.2024. URL : https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення : 17.11.2024).

39. Про кінематографію: Закон України від 13.01.1998 р. № 9/98-ВР. Дата оновлення : 15.11.2024. URL : https://zakon.rada.gov.ua/laws/show/9/98%D0%B2%D1%80#Text (дата звернення : 16.11.2024).

40. Про медіа: Закон України від 13.12.2022 р. № 2849-IX. Дата оновлення : 11.02.2024. URL : https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення : 25.10.2024).

41. Про Національний координаційний центр кібербезпеки : указ Президента України від 07.06.2016 № 242/2016 URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення: 20.09.2024).

42. Про національну безпеку України : закон України від 21.06.2018 № 2469-VIII. Дата оновлення : 09.08.2024. URL: https://zakon.rada.gov.ua/go/2469-19 (дата звернення: 10.09.2024).

43. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 № 183/98-ВР. Дата оновлення : 29.07.2024. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text (дата звернення: 19.09.2024).

44. 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 № 106/2021. Офіційний вісник України. 2021.

№ 25. С. 53.

45. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : указ Президента України від 14.09.2020 № 392/2020. Офіційний вісник України. 2020.

№ 75. С. 127.

46. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : указ Президента

України від 26.08.2021 № 447/2021. Офіційний вісник України. 2021. № 70. С. 42.

47. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : указ Президента

України від 28.12.2021 № 685/2021. Офіційний вісник України. 2022. № 3. С. 22.

48. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості» : указ Президента України від 27.09.2021 № 479/2021. Офіційний вісник України. 2021. № 79. С. 31.

49. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» : Указ

Президента України від 16.02.2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/main/56/2022.#Text (дата звернення: 19.11.24).

50. Розробник ChatGPT закликав Конгрес США регулювати штучний інтелект. URL: https://www.rbc.ua/rus/news/rozrobnik-chatgptzaklikavkongresssharegulyuvati-1684276164.html (дата звернення : 15.09.2024).

51. Російські дезінформаційні кампанії в Європі. Національний інститут стратегічних досліджень. 2024. URL: https://niss.gov.ua/doslidzhennya/ mizhnarodni-vidnosyny/rosiyski-dezinformatsiyni-kampaniyi-v-yevropi (дата звернення: 19.11.24)

52. Солодка О. М. Інформаційний простір держави як сфера реалізації інформаційного суверенітету. Інформація і право. 2020. № 4 (35). С. 39–46.

53. У разі надзвичайної ситуації або війни / Центр стратегічних комунікацій та інформаційної безпеки МКІП. Київ, 2021. 28 с.

54. Центр протидії дезінформації. URL : https://cpd.gov.ua/ (дата звернення: 19.09.2024).

55. Центр стратегічних комунікацій та інформаційної безпеки. URL : https://spravdi.gov.ua/ (дата звернення: 20.09.2024).

56. Blinken A. J. Building A More Resilient Information Environment : speech. 2024. 18th of March / U.S. Department of State. URL : https://www.state.gov/building-a-more-resilient-information-environment/ (дата звернення : 25.09.2024).

57. Government-wide strategy for effectively tackling disinformation : 23 December 2022. URL:

https://www.government.nl/documents/parliamentarydocuments/2022/12/23/gover nm ent-wide-strategy-for-effectively-tacklingdisinformation (дата звернення:

12.09.2024).

58. Handreiking omgaan met desinformatie. 2022. .

URL:

https://www.rijksoverheid.nl/documenten/publicaties/2022/02/09/handreikingomga an

-met-desinformatie (дата звернення: 12.09.2024).

59. Masuda Y. The Information Society as Post-Industrial Society. Piscataway, New Jersey: Transaction Publishers, 1980. 178 p.

60. Molina M. D., Sundar S. S., Le T., Lee D. «Fake News» Is Not Simply False Information: A Concept Explication and Taxonomy of Online Content. URL: https://journals.sagepub.com/doi/pdf/10.1177/ 0002764219878224 (дата звернення: 12.09.2024).

61. Strengthened Code of Practice on Disinformation. European Commission. https://digitalstrategy.ec.europa.eu/en/library/2022strengthenedcodepracticedisinformation (дата звернення: 25.09.2024).