МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ІВАНОВА ЄЛИЗАВЕТА ІГОРІВНА

Допускається до захисту:
в.о. завідувача кафедри
міжнародних відносин і зовнішньої політики,
к.і.н., доцент І.В. Богінська
«_____» _____2021 р.

ІНФОРМАЦІЙНА АГРЕСІЯ РФ ЯК ФАКТОР ДЕСТАБІЛІЗАЦІЇ УКРАЇНИ

Спеціальність 291 Міжнародні відносини, суспільні комунікації та регіональні студії

Кваліфікаційна (бакалаврська) робота

Керівник:
Фротвейт М.М., доктор
політичних наук, доцент

Оцінка: _____ /_____ /_____
(бали/за шкалою ECTS/за національною шкалою)

Голова ЕК:_____
(підпис)

Вінниця – 2021

АНОТАЦІЯ

Іванова Є.І. Інформаційна агресія РФ як фактор дестабілізації України. Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії». Донецький національний університет імені Василя Стуса, Вінниця, 2021.

У кваліфікаційній (бакалаврській) роботі досліджено проблематику інформаційної агресії Російської Федерації по відношенню до України, фактор дестабілізації внутрішньополітичної ситуації внаслідок потужної інформаційно-пропагандистської кампанії. Показано сучасний стан інформаційного впливу, напруження відносин між акторами інформаційного суспільства на фоні пандемії COVID-19. Встановлено необхідність активних дій по запобіганню існуючих впливів, дій по відношенню до існуючих загроз, адже вірогідність появи нових, більш небезпечніших, зростає з кожним днем.

Ключові слова: інформаційна війна, інформація, вплив, втручання, дестабілізація, дезінформація, пропаганда, Україна, Росія, Крим, анексія, інформаційна експансія.

47 с., 15 джерел

ABSTRACT

Ivanova Y. I. Information aggression of the Russian Federation as a factor of destabilization of Ukraine. Specialty 291 "International Relations, Public Communications and Regional Studios". Vasil Stus Donetsk National University, Vinnytsia, 2021.

The qualification (bachelor's) work investigates the problematics of information aggression of the Russian Federation towards Ukraine, the factor of destabilization of the internal political situation because of a powerful information-propaganda campaign. Shows the current state of information influence, tension of relations between actors of information society on the background of the COVID-19 pandemic. Established the need for active measures to counteract the current

influences, actions in relation to the current threats, because the likelihood of new, more dangerous, is increasing every day.

Keywords: information warfare, information, influence, intrusion, destabilization, disinformation, propaganda, Ukraine, Russia, Crimea, annexation, information expansion.

ЗМІСТ

ВСТУП

Актуальність теми дослідження.

Сьогодні неможливо уявити світ без зручних інформаційних технологій, без постійного доступу до інформації. Наше суспільство на етапі розвитку, трансформації, переходу в повністю інформаційний простір, де зберігається інформація, яка охоплює майже усі сфери людської діяльності. Поява нових технологій призвела до значних позитивних трансформації, однак в той ж час з'явились нові, небезпечні, загрози безпеці як персональній так і національній.

В ході потужної інформаційно-пропагандистської кампанії Російської Федерації значною мірою постраждала Україна, яка на час першої інформаційної атаки була цілком неспроможна дати відсіч. Однак з часом потенціал зростав, які і можливість забезпечення власної інформаційної безпеки. Однак навіть з підготовленими нормативно-правовими документами Україна не може бути впевнена в виходу з під інформаційного впливу РФ.

Актуальність даного дослідження полягає в детальному розборі інформаційно-пропагандистської кампанії Російської Федерації щодо України на різних стадіях розвитку. Від передумов до наслідків інформаційного і фізичного втручання у справи незалежної держави, Визначення рекомендацій щодо подальшого розвитку інформаційної безпеки. Адже дуже важливо розуміти усі існуючі загрози, для створення системи захисту власних національних інтересів.

Об'єктом дослідження є інформаційна діяльність в умовах глобалізації

Предмет дослідження - втручання РФ в інформаційний простір України

Хронологічні рамки: нижня межа: 1991; верхня межа: 2021.

Географічні рамки. Україна – Російська Федерація; Сполучені Штати Америки – Європейський Союз.

Історіографічний огляд. Вивчаючи фактор російського втручання во внутрішні справи України можна впевнено сказати, що вона є достатньо популярною у дослідників різних сфер діяльності, адже вплив відбувається

майже на усі сфери життєдіяльності. Доречним буде розподілити їх за напрямками дослідження:

1. Вивченням теоретико-концептуальними засадами займались наступні дослідники: Радутний О.Е. [32], Савінова Н.А. [37]. В своїх дослідженнях науковці вивчають інформаційну агресію як з різних сторін. Вони здебільшого пишуть про фактор використання і засоби протидії агресії.
2. Витоками та факторами інформаційної агресії займались наступні дослідники. Про інформаційну агресію, як фактор дестабілізації, можливість впливати на внутрішні справи інших держав писали і досліджували: Магда Є. [16], Цуканова О.В. [41], Сасин Г.В. [38]. Витоками конфронтації займались Лисенко С.О.[22], Маклюєн М. [19], Магда Є. [16], Цуканова О.В.[41]. Про фактор впливу писали Герасимчук С., Шелест Г.[4].
3. Питанням протидії зовнішнім інформаційним чинникам займались науковці зі всього світу. Щодо реакції України на зовнішню інформаційну агресію писали: Манойло А. [20], Біловус Л. [1], Кирильчук Є.О. [13]. Проблематику інформаційного простору була проаналізована і досліджена такими дослідниками як: Сасин Г. [2738 Герасимчук С., Шелест Г. [4], Кирильчук Є.О. [13], Собків Я. [39], Онищенко О.С. [22], Пилипчук В.Г. [23].

Мета: дослідити фактор дестабілізації внутрішньої політики України через інформаційно-пропагандистське втручання РФ.

Відповідно до мети, сформовані наступні завдання:

1. Визначити поняття інформаційної агресії, з’ясувати розбіжність українських і зарубіжних науковців;
2. Проаналізувати літературу та джерела з напрямки теми; дослідити нормативно-правове забезпечення інформаційної безпеки;

3. Окреслити інформаційну агресію як фактор дестабілізації державної структури;
4. Проаналізувати підготовку та початок інформаційно-пропагандистської кампанії Російської Федерації по відношенню до України;
5. Конкретизувати вплив політки Кремля на внутрішню політику України;
6. Проаналізувати реакцію і засоби протидії інформаційній компанії з боку постраждалої держави;
7. Розглянути міжнародні приклади протидії інформаційній агресії;
8. З'ясувати проблематику інформаційного простору.

Характеристика джерел. В бакалаврської роботі були використані наступні джерела:

Законодавчі документи:

1. Конституція України : Закон України від 08.06.1996 р. № 254к/96-ВР / Відомості Верховної Ради України. 1996. № 30. Ст. 141. [14].
2. Закон України «Про інформацію» від 02 жовтня 1992 р. Відомості Верховної Ради України (ВВР). – 1992. – № 48. – С. 650 [11].

Нормативно-правові документи:

1. Про Стратегію сталого розвитку «Україна – 2020» : Указ Президента України від 12.01.2015 р. № 5/2015 [31]
2. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : Указ Президента України від 26.05.2015 р. № 287/2015 [27]
3. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 р. № 96/2016 [28]
4. Про Заяву Верховної Ради України «Про відсіч збройній агресії Російської Федерації та подолання її наслідків : Постанова Верховної

Ради України від 21.04.2015 р. № 337-VIII / Відомості Верховної Ради України. 2015. № 22. Ст. 153 [25]

5. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Указ Президента України від 01.05.2014 № 449/2014 [29]
6. Резолюція Генеральної Асамблеї ОООН про територіальну цілісність України від 27 березня 2014 р. № 68/262 [36]
7. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. №47/2017 [30]
8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-19 [26]

Міжнародні стратегії

1. The Cybersecurity Strategy [50]
2. Cybersecurity Legislation 2020 [44]
3. European Union’s new cybersecurity strategy [45]

Засоби масової інформації

1. Freedom House опасается, что в Украине может усилиться цензура в интернете [46].

Методи дослідження.

Для написання бакалаврської роботи був використаний системний підхід, який сприяє поступовому розв’язанню і вивченню головної мети дослідження. Дослідження здійснювалось за допомогою наступних методів:

1. Загальнонауковий
   - описовий, при дослідженні певних явищ, процесів
   - системний – для з’ясування інформаційної системи в цілому, її складових

2. Метод контент-аналізу – допоміг дослідити причинно-наслідкові зв'язки між інформаційною агресією РФ та дестабілізацією внутрішньої політики України за допомогою якісного контент-аналізу в російського, російського англомовного, українського медіапростору.
3. Івент-аналіз – на основі реальних прикладів, історичних подій було сформовано більш детальне розуміння ситуації, окреслені приклади інформаційного втручання, системне дезінформування в засобах масової інформації.
4. Метод дедукції, за допомогою якого був сформований логічний висновок засобом від загального до окремого.

Теоретичне значення одержаних результатів – полягає в критичному аналізі вже досліджених аспектів, виявлення нових загроз і обставин в інформаційній сфері через пандемію COVID-19. Поява нових засобів трансляції інформаційного впливу, нові методи передачі потрібної інформації до кінцевого отримувача.

Структура кваліфікаційної (бакалаврської) роботи. Робота складається з титульного аркушу, анотації, змісту, вступу, трьох розділів: в першому розділу – 2 підпункти, в другому і третьому по 3 підпункти, висновків, списку використаних джерел та літератури. Загальний обсяг кваліфікаційної (бакалаврської) роботи становить 47 сторінок.

РОЗДІЛ 1. ТЕОРЕТИКО-КОНЦЕПТУАЛЬНІ ЗАСАДИ І ДЖЕРЕЛЬНА БАЗА ДОСЛІДЖЕННЯ

1.1. Поняття інформаційної агресії вітчизняних і зарубіжних науковців

Інформація, як ресурс, була ще за довго до появи новітніх засобів комунікації, таких як Інтернет. Ще у стародавні часи, правителі відправляли дипломатичні каравани для отримання інформації, відсилали таємних агентів для підривної діяльності з середини. Колись Вінстон Черчилль сказав: «Хто володіє інформацією, той володіє світом». Крилатим вираз став майже одразу і з кожним наступним роком набуває ще більшої актуальності. Інформаційна сфера на сьогодні охоплює весь світ, усі сфери людської життєдіяльності. Вільний доступ до інформації – одне із основних прав людини в сучасному світі, таке ж як доступ до води і чистого повітря. Фактично сьогодні світ переступив межу певної залежності від інформації. Інформаційне суспільство – це історична фаза еволюційного розвитку цивілізації, де інформація і знання є головними продуктами виробництва.

Незважаючи на стрімкий розвиток суспільства в інформаційному плані, психологічно до новітніх інформаційних викликів готові були не усі. Таким чином, інформацію доволі швидко почали використовувати як новий інструмент маніпуляції, впливу чи злочинності використовуючи новітні технології. Однак, втім використовувати інформацію як зброю почали ще за довго до появи сучасних технологій. Звично, раніше, в стародавні часи, це стосувалось більш політичних інтриг на дипломатичному рівні. На сьогоднішній день інформаційний вплив поширюються на всі сфери діяльності і суспільні шари. Відносно дешевий, а в деяких випадках безкоштовний, доступ до інформації створює ситуацію, коли фільтр споживання і захисту інформації не є стійким механізмом з налагодженою структурою. Фактично, це означає швидкий, маже без бар'єрний інформаційний вплив чи виклик, а також повноцінну інформаційну агресію. В такому випадку, держава, організація чи фізична особа стають об'єктом

інформаційного впливу чи агресії. А відсутність механізмів регулювання створюють загрозу захисту суверенітету не лише в інформаційному, а й звичайному сенсі.

Радутний О. Е. писав, що «інформаційна агресія є різновидом інформаційного протиборства (суперництва в інформаційній сфері щодо впливу на соціально значущі відносини та/або встановлення контролю над джерелами стратегічних ресурсів), яке, у свою чергу, є різновидом будь-якого протиборства, і полягає у посяганні на свідомість та світосприйняття людини» [33].

Передумовами інформаційної агресії як інструменту виступають бурхливий розвиток технологій, швидкий поток інформації, від цього прискорення процесів подання та зникнення відомостей, невміння розпізнати інформацію за різними ознакам. Наприклад розпізнати недостовірну подачу чи упередженість, а також відсутність навичок у пошуку альтернативних джерел і застосування критичного мислення. Свій наслідок також залишило необізнаність користувачів інформаційних ресурсів. Для суспільства, де довгий час прогрес і в інформаційному плані був під повним контролем влади, люди були не підготовленні для стрімкої віртуалізації життя, появу нової інформаційної культуру. Таким чином, це створило умову зручного маніпулювання і контролю за допомогою новітніх технологій [32].

Якщо ми будемо розглядати додаткові чинники, які сприяють, чи можуть сприяти інформаційній агресії, то тут можна виділити наступні:

- Засоби масової комунікації та їхнє подання інформації виключно агресивного контексту з той чи іншої теми. Тут, можна навести приклад сучасних ЗМІ Російської Федерації, де подається агресивна новинна політика по відношенню до Сполучених Штатів Америки, України і низки інших держав і організації;
- З цього, перенасиченість населення політичними шоу-програмами, які здебільшого заангажовані і пов’язані більше з елементами театру, ніж зі справжньою аналітикою.

- Останнім часом, з популяризацією соціальних мереж, можна помітити тенденцію на штучну популяризацію той, чи іншої думки в мережах Інтернету. Як приклад, це використання популярних соціальних мережах «Тік-ток», «Твиттер» та інші. Замовники покупають у відомих блогерів їх час мовлення, для трансляції необхідних думок через їх відомий персональний бренд. Політична реклама у відомих особистостей Інтернету використовується максимально активно останні декілька років [37].

Звичайно, інформаційне агресія проявляється не тільки на політичному рівні, в використанні засобів масової комунікації, дезінформації, спотворенню історичних та інших фактів, формуванні суспільної думки або поглядів, а також на більш глибинних рівнях державного управліннях, що є максимально небезпечним і створюю загрозу національної безпеці.

Фактично, інформаційна агресія, це незаконні дії однієї сторони в інформаційному просторі по відношенню до іншої сторони, чи ряду сторін, які спрямовані на нанесення конкретного удару цілі, чи області її діяльності шляхом різного масштабу застосування сили. Однак, масштабну інформаційну агресію можна порівняти з грою у шахи, де кожен крок має різну силу і наслідки, але в результаті буде або Шах або Мат.

Відповідно до чинників інформаційної агресії, її можна класифікувати за певними ознаками:

1.) Інформаційна агресія, має складніший механізм, ніж наприклад кібератака, де я фактично винний і жертва. Таким чином, це не дозволяє використовувати самі небезпечні види інформаційної зброї, що, втім, не дозволяє надійно контролювати реальний розмір впливу;
2.) Обмеження простору дії, об’єктів інформаційної інфраструктури та соціальних груп, які найбільш потрапляють під вплив. Фактично, агресія зачіпає не весь інформаційний простір «жертви» -держави, або організації, а діє лише на його частину. Однак, звичайно, що вплив лише на одну із державних структур здатен нанести значної шкоди;

3.) Обмеження за метою і часом. Від точкових локальних, приватних до глобальних цілей. Зазвичай, агресія припиняється після завершення агресором поставленої мети, однак в деяких випадках це може перетворитись на постійний, затяжний, характер інформаційної агресії по відношенню до другої сторони;

В інформаційній сфері агресія переростає у війну, тільки у тому випадку, коли одна із сторін конфлікту починає ширше застосовувати проти супротивників тяжку інформаційну зброю. В свою чергу, інформаційна війна – найвища ступень інформаційного протиборства, яка спрямована за допомогою поступового, точкового впливу розв'язувати суспільно-політичні, ідеологічні, національні, територіальні та інші конфлікти між державами, народами, націями, класами й соціальними групами.

Літератури, яка стверджує, що інформація – це зброя, досить багато і визначити її не складно. Автори зазвичай говорять про свої переконання, що електрон – це саме високоточна керована зброя, а інформація – мета і одночасно зброя. Цілком можливо, що солдати будуть керувати комп'ютерами, а ніж звичною зброєю. Вже сьогодні жодна армія світу не може забезпечувати безпеку без необхідного обладнання. Фактично, скоро, держави, а деякі і вже, зможуть вести війну лише за допомогою комп'ютерної миші, клавіатури і комп'ютерного вірусу. Найпотужнішою зброєю є не бомба чи ядерна ракета, а безкінечна кількість електронних одиниць та нулів.

1.2. Нормативно-правове забезпечення інформаційної безпеки

Виникнення нових соціальних явищ, пов'язаних з інформацією обумовлюють розвиток нормативно-правового забезпечення інформаційної безпеки. Збільшується увага законодавців до регулювання відносно нової галузі суспільних відносин. Кожного дня інформація збільшує своє значення в абсолютно різних сферах людської діяльності. Обробка та передача інформації, розвиток новітніх технологій призводять до суттєвих змін в економічній, політичній, соціальній та інших сфера людської життєдіяльності.

Фактор інформаційного суспільства, на зміну індустріального суспільства вже є незворотнім і відповідним до реальності.

В реаліях нового інформаційного світу найважливішим є необхідність створення робочої моделі, системи, забезпечення прав і свобод людини на вільне отримання, поширення та використання інформації. По-перше для того, щоб забезпечити умови демократичного розвитку, по-друге – запобігти формуванню самостійного, неконтрольованого інформаційного суспільства [19, с. 2]. Необхідність забезпечення права – його відповідність на виклики і загрози інформаційного суспільства, особливо, якщо брати до уваги збільшення інтересу забезпечення інформаційної безпеки, що здебільшого зумовлено інформаційною агресією, яку проводять по відношенню до України з боку Російської Федерації. В даному випадку, слід відзначити посилення ролі права в нових реаліях.

В сукупності усі фактори зумовили виникнення не аби якого наукового інтересу до проблематики правового забезпечення інформаційної безпеки, її систематизації на законодавчому рівні, забезпечення прав і свобод громадян, інтересів юридичних осіб, суспільства та держави. Необхідність норм, які регулюють відносини пов’язані із забезпеченням інформаційної безпеки в єдиній системи національного права.

Ю. Є. Максименко у своєму дослідженні «Теоретико-правові засади забезпечення інформаційної безпеки України» пише, що галузь правового забезпечення інформаційної безпеки – частина системи інформаційного права. Правове забезпечення інформаційної безпеки є самостійним нормативним утворенням, яке складається з системи норм інформаційного права. Нормативно-правове регулювання інформаційної безпеки можна сприяти як форму владного правового впливу на суспільні відносини. В свою чергу, це здійснюється державою з метою упорядкування та забезпечення. [20, с.118] Однак, з іншого погляду інформаційна безпека є невід’ємною властивістю її об’єктів і правове регулювання має розглядатись як складова забезпечення.

Функції забезпечення, в свою чергу, необхідно закріпити в основному законі держави.

Стаття 17 Конституції України говорить: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [14].

Світова інформаційна революція, глобалізація інформаційних процесів, відповідно поява нових загрозливих чинників створили новий імператив – інформаційну безпеку. На сьогодні – одна із ключових сфер права та адміністративного регулювання. Фактично, вплив сучасних реалій на забезпечення інформаційної безпеки формує нову систему конституційних засад. В той час як систематизація норм має відповідати конституційним засадам, без додаткових перепон та складних процедур [15, с. 160].

Найважливішим фактором оптимізації державного управління має бути управління інформаційною сферою. Включаючи формування та поширення різних видів інформаційних впливів, регулювання інформаційних потоків та ресурсів; розвиток необхідної інфраструктури та ринку інформаційно-комунікаційної сфери послуг і технологій.

Якщо розглядати забезпечення інформаційної безпеки з точки зору державної політики, то вона має базуватись на наукових і методологічних розробках. Також, необхідна чітка систематизація об’єднана в єдину концепцію. Концепція має бути представлена як сукупність національних цілей, інтересів, цінностей. Розроблені та реалізовані державною владою стратегії та тактики для регуляції процесів інформаційної взаємодії в усіх сферах діяльності суспільства та держави; технологічне забезпечення взаємодії.

Державна політика забезпечення інформаційної безпеки України повинна мати чітко виокремлену мету, наприклад: формування відкритого інформаційного суспільства. Відкрите інформаційне суспільство – новий простір держави, інтеграція в світовий інформаційний простір. Звичайно

світову інтеграції необхідно проводити з урахуванням національних особливостей, національних інтересів для забезпечення інформаційної безпеки як на внутрішньодержавному, так і на світовому, міжнародному, рівні. Ефективна реалізація політики має ряд умов, одна із необхідніших – розробка організаційних і технологічних заходів щодо захисту систем державного управління на усіх рівнях держави від впливу на системи з боку злочинців. Держава, інститути, мають усвідомлювати весь вплив, який може бути нанесений без прийняття рішучих дій в плані забезпечення безпеки не тільки державі і суспільству, а також інтересам кожної окремої особи.

Інформаційне законодавство, і дослідження в цій сфері набувають особливої актуальності щодо питань прогнозування розвитку. З огляду на розширення використання методів стратегічного планування. Як приклад – видання в Україні актів стратегічного характеру, котрі визначають основні загальнодержавні напрями соціально-економічного розвитку та передбачають розробку прогнозів розвитку законодавства.

Також, необхідно підкреслити, що з моменту виявлення активних загроз інформаційній безпеки з боку Російської Федерації, постійної агресивної кампанії проти України було прийнято Стратегію сталого розвитку «Україна-2020». В стратегії було визначено загальні напрями щодо реформування національної безпеки. Стратегія національної безпеки України, де питанням інформаційної безпеки приділено значну увагу, і зокрема нормативно-правової бази. Стратегію кібербезпеки України, яка зумовлює розвиток технічно-технологічних засобів забезпечення інформаційної безпеки України [25, 27, 28, 31].

Згідно Закону України «Про інформацію» окрім визначення терміну «інформаційна безпека» нічого немає, а захист інформації – це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність та доступ до інформації. З огляду на закон, можна визначити, що законодавець не в повній мірі врахував усі

можливі ризики нанесення шкоди інформаційній безпеці у сфері державного управління [11].

В Україні упродовж останніх років були доповненні низка законодавчих документів, що регулюють інформаційну сферу, зокрема щодо забезпечення інформаційної безпеки держави, наприклад Закон України «Про інформацію». Однак, слід зауважити, що в сучасних умовах розвитку суспільства інформаційне законодавство потребує значних та якісних змін. Незважаючи на поправки, воно залишається суперечливим, не систематизованим і не кодифікованим.

Необхідність адаптації національного законодавства до вимог Європейського Союзу зумовлює інтенсивний розвиток інформаційного законодавства, зокрема про інформаційну безпеку, за різними напрямами. У рішенні Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» зазначалось, що пріоритетами забезпечення інформаційної безпеки є:

1. забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії;
2. створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;
3. протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства;
4. розробка і реалізація скоординованої інформаційної політики органів державної влади;
5. виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;

6. створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики держав - членів НАТО;
7. удосконалення професійної підготовки у сфері інформаційної безпеки, упровадження загальнонаціональних освітніх програм з медіакультури із залученням громадянського суспільства та бізнесу [27].

Виняткове значення має Рішення РНБО від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», введено в дію Указом Президента № 449/2014 від 01.05.2014. Головний акцент ставиться на питаннях інформаційної та кібернетичної безпеки, вдосконаленні системи формування та реалізації державної політики у сфері інформаційної безпеки України [29].

Модернізація механізмів державного управління інформаційною сферою шляхом внесення відповідних змін до нормативно-правової бази стане передумовою вирішення низки проблем загального розвитку інформаційної сфери. Подальші кроки України у формуванні довгострокової державної стратегії розвитку інформаційної сфери та підвищення ефективності виконання державно-управлінських рішень. Імплементація запропонованих задач вже починають знижувати інформаційну залежність України та забезпечують надійний захист національних інтересів.

РОЗДІЛ 2. ВИТОКИ ТА ФАКТОР ІНФОРМАЦІЙНОЇ АГРЕСІЇ РФ ПО ВІДНОШЕННЮ ДО УКРАЇНИ

2.1. Інформаційна агресія як фактор дестабілізації

Інформаційні технології змінили наш світ безповоротно; змінились фокуси і продукти багатьох сфер людської життєдіяльності. Розглядаючи безпекову сферу ми вже не можемо ігнорувати інформаційну складову, особливо, в той момент, коли в державі існує фактор зовнішнього інформаційне впливу, навіть тиску. В такому випадку, необхідно пильно стежити за ситуацією і виокремлювати приклади і моменти агресії, яким чином вони впливають на функціонування держави і внутрішньополітичну ситуацію. Окрім, звичайно реагуванню з законодавчої та міжнародної сторін.

Таким чином, слід розглянути інформаційну агресію, не як явище, а як фактор дестабілізації окремих об'єктів. За допомогою інформаційних технологій, коли ведеться активне інформаційне протистояння, відбувається здебільшого маніпуляція свідомістю, вчинення кіберзлочинів на стратегічні об'єкти жертви інформаційного злочинця. Об'єктом же виступає не лише громадянське суспільство і комп'ютерні мережи, а й широкі маси жертви інформаційної агресії. Тобто, якщо жертвою виступає незалежна держава, то інформаційний вплив охоплює не тільки стратегічно важливі сфери, а й найменш значущі. Такий розклад ставить у небезпечне становище кожну сферу діяльності, і створює необхідні умови для внутрішнього осередку дезінформації і внутрішньополітичного коливання.

Найефективніший засіб маніпуляції великої кількості людей одночасно – інформаційні технології, які мають широкий арсенал інструментів і методів. Звичайно, основними можна вважати пропаганду і дезінформацію, за допомогою яких формується певна, необхідна для «замовника», стратегія щодо дискредитації певного актора\явища, дестабілізації внутрішньої\зовнішньої ситуації, ескалації локальних і міжнародних конфліктів. А також важливо відмітити як фактор і наслідок – формування

потрібних наративів у свідомості різних соціальних груп. Зазвичай, негативних вплив інформаційних технологій проявляється у найбільш уразливих точках, сферах, суспільного життя. Застосовуючи технології на рутинній основі, маніпулятивний вплив проникає в усі сфери повсякденного життя, формуючи конкретно завчасно продумані цінності і світогляди.

Здається, за допомогою інформаційних технологій можна зробити усе, що тільки можна уявити в новому інформаційному світі. Сформувати будь-які потрібні тренди та тенденції для досягнення певної мети. Одним з основних прикладів останніх років можна вважати президентські вибори у США, де за допомогою сучасних інформаційних технологій велась виборча гонка. Такий розклад наводить на думку, що наступна боротьба буде за голоси послідовників в соціальних мережах, за їх соціальну активність. Фактично, крайні президентські вибори США вже доказали, що інформаційна складова є надважлива, не тільки з точки зору можливого втручання з боку інших акторів на результат, а й з точки зору використання інформаційних технологій як інструменту передвиборчої гонки. Сьогодні феномен «Твіттер-дипломатії» вже не є новим явищем; це факт нового засобу трансляції своєї політики і ідеології одночасно на широку масу людей.

Інформаційні технології впливають на формування свідомості людини, на створення нових інформаційних продуктів. Кожен з них має різні характеристики, термін дії та ефективності в залежності від поставленої мети. Однак можна стверджувати, що максимальна результативність досягається лише в тому випадку, коли інформаційні продукти працюють одночасно чи частково одночасно задля досягнення спільної мети. В свою чергу це і створює ще більш небезпечне становище для постраждалої сторони. Подібними «букетами» з інформаційних продуктів і користується Російська Федерація по відношенню не тільки до України чи США, а й до власного народу – створюючи лише єдину правду, яка б абсурдна вона не була для усього світу.

Інформаційні продукти – широке поняття, а їх використовування як інструменту впливу почалось ще за тисячі років до створення мережі Інтернет.

Можливо в той час вони були не такими швидкими в застосуванні і результативності як зараз, однак вони добре працювали на перспективу. Мова йде здебільшого про мистецтво: література, однин з найбільш популярних засобів комунікації, можу створювати всі необхідні тенденції у суспільстві, які необхідні тому чи іншому актору; в історії є багато прикладів, коли саме література ставала основним, а може і головним, інструментом пропаганди ідеології і політики партії. Сьогодні часта літератури зменшується, однак актуальність все ще існує; театр і кіно, працюючий засіб за допомогою візуального відпочинку і розваги донести певну, задану, думку. Якщо наводити приклад сьогодення, то Російська Федерація активно використовує цей вид інформаційного продукту і виділяє на це гроші державного бюджету.

Можливості мистецтва застосовуються у більш тривалій перспективі ніж засоби масової комунікації, соціальні мережі. Російська Федерація зі своєю радянською системою, методами якої вона користується по сьогоднішній день здатна майже будь-яку продукцію перетворити на свій власний інформаційно-пропагандистський продукт масового застосування. Навіть сувенірна продукція має рацію в боротьбі за владу [40].

Про інструменти інформаційних технологій, за допомогою яких відбувається дестабілізація певних процесів, будування нової правди необхідної для досягнення амбітних цілей можна говорити достатньо довго і список буде розширюватись з кожним роком все більше. Однак, тим не менш можна виділити основні, найбільш популярні та ефективні на прикладі інформаційної агресії РФ проти України.

З появою перших телевізорів світ повністю змінився і отримувати інформацію стало набагато зручніше і цікавіше, втім це відкрило ще більше можливостей для маніпулювання свідомістю одночасно величезної кількості людей. І сьогодні, незважаючи на альтернативні джерела інформації телебачення все ще не втрачає своєї актуальності. Таким чином, одними із основних телевізійних інструментів є телепередачі і новинні сюжети,

кінофільми і телесеріали. Для деталізації слід розібрати кожен з реальними прикладами.

Телепередачі. Основний інструмент інформаційного тиску та дестабілізації суспільних відносин. За допомогою регулярного фінансування організуються численні телевізійні студії, де основна ціль – створити потрібний інформаційний продукт, відповідний до кінцевої цілі замовника. Головна зброя – емоції. Показуючи шокуючі сюжети, дискутуючи на суспільно гострі теми, формуючи образ держави-ворога, держави-вбивця відбувається формування настроїв у суспільстві. Навіть, якщо з першого разу людина не піддалась під інформаційний вплив, то постійна, довготривала, іноді фонова, пропаганда рано, чи пізно змусить або змінити думку на запропоновану, або посіяти зерно сумніву.

Новинні сюжети. Телебачення сьогодні – велике шоу, і новини також почали перетворюватись на шоу-подібні передачі. Особливо, коли мова йде про новини держав-ворогів. У випадку з Росією це Україна, США і ряд інших держав, кількість яких з кожним роком тільки збільшується. Частка новин про Україну на російському телебаченні набагато більша, ніж по відношенню до будь-якої іншої незалежної держави. Новини – це популярний спосіб викривлення інформації, маніпуляції фактами і джерелами. В історії вже багато прикладів, коли новинні сюжети ставали всесвітньо відомими скандалами та в решті решт були звинуваченими в брехні.

Кінофільми і телесеріали. Здавалось би, художні витвори, які не мали б жодного відношення до інформаційної зброї і дестабілізації, однак і з цим не все тай просто і однозначно. Навпаки, це чудовий засіб ненав’язливого впливу на думки пересічних громадян точкових держав, а іноді і регіонів. Одним із яскравих прикладів є фільм «Крымский мост. Сделано с любовью!» режисера Тиграна Кеосаяна і автора сценарію Маргарити Симоньян – основних пропагандистів Російської Федерації, відомих українофобів Росії. Навіть в назві фільму можна прослідкувати відкритий контекст проблеми – статус окупованого півострову і то наскільки стало краще при нових володарях.

Взагалі завзяте, негативне, відношення до України і всього українського в російському кіновиробництві достатньо багато. М'яка сила інформаційної зброї ідеально працює тоді, коли глядач вважає, що кінцева думка – лише його власне суб'єктивне мислення, а ні в якому разі думка Кремля.

Найбільш влучний і привабливий спосіб передачі інформації – аудіо-візуальний. Він легко сприймається для широкого кола користувачів. З появою соціальних мереж пости у Facebook, Telegram каналах стали більш популярні за телевізійні політичні ток-шоу. Авторитетність лідерів думок, відсутність цензури створює нові можливості до отримання інформації. З цим поширюється і потік дезінформації, неперевірених фактів. Також останні роки популярним стало замовлення політичної реклами у відомих блогерів.

Інформаційні компанії РФ по відношенню до України – це справжні агресивні дії. Безкінечні потоки інформаційного сміття створили стійке уявлення суспільної ненависті росіян по відношенню до українців. Кампанія максимально поставила на меті зруйнувати усе людяне, створивши чіткий образ ворога. Фактично, інформаційна агресія РФ дестабілізує не тільки окрему взяту державу, а й регіон. Створюю небезпечні виклики, які здатні призвести до національних, етнічних конфліктів. Процес вже настільки вкоренився в державну структуру, що сьогодні складно уявити Росію без фабрики фейків і пропаганди і єдине що залишається – створювати заходи і засоби інформаційній протидії, реалізовуючи їх на постійній основі.

2.2. Підготовка та початок активної інформаційно-пропагандистської кампанії РФ

Сьогодні вже константа – діяльність РФ в інформаційному просторі України, складно уявити буденність без інформаційної агресії з боку сусідньої держави. Однак для вирішення цього стану необхідно поглинутись у коріння проблематики; з'ясувати причини і справжній момент початку інформаційно-пропагандистської кампанії. Безперервна боротьба за ресурси, вплив і контроль над територією. Революційні події кінця 2013 – початок 2014 року

стали відправною точкою трансформації сучасних міжнародних відносин, систем забезпечення безпеки. Внаслідок дестабілізації внутрішньо політичної ситуації, анексії Автономної Республіки Крим, та ведення «гібридної війни» геополітична ситуація у світи змінилась. Поява нових акторів, загроз, викликів не лише в Європі, а й у світі залишили наслідки, з якими ми маємо працювати сьогодні.

Інформаційні війни – не нове явище на території сучасної України в тій чи інший мірі. Інформаційні впливи такі як: приховування інформації, викривлення фактів, транслювання інформації через певну думку та ідеологію, заплутування наслідків були відомі ще за часи Київської Русі. Літописцями було зафіксовано, наприклад, що князь Святослав зазвичай заздалегідь повідомляв противника про свій похід, при цьому не розкриваючи важливіших деталей як напрям та військові сили, які планували застосовувати. Такий підхід створював паніку та дезорієнтацію противника, що давало можливість швидко та ефективно розгромити противника [6, с. 18].

Маршалл Маклуен, канадській філософ, філолог і літературний критик був одним із перших хто писав про вплив медіа як засобів комунікації на аудиторію. Він здобув широку популярність завдяки дослідженню інформаційного впливу на формування людини і суспільства, зокрема його концепції глобального села. У 1960 він був одним із перших, хто писав про феномен інформаційних воєн у відкритому доступі. І вже на той час було зрозуміло, що з’явився новий вид воєн – інформаційних, коли навіть так звана «холодна війна» ведеться за допомогою фактично лише інформаційний технологій, без використання людських ресурсів та бойової техніки. Таким чином, війни наступного покоління будуть знищувати ворогів за допомогою лише телебачення та кіно, що можливо в певному сенсі зруйнує весь свій, як мінімум баланс сил. «Земна куля тепер – не більше, ніж село», - писав М.Маклуен [19, с. 7].

Фактично інформаційні технологій можуть використовуватись як зброя масового ураження, вони здатні створити катастрофи світового масштабу,

адже як інструмент ведення політики інформаційна війна означає де-факто панування одного суспільства чи держави шляхом зневаження, знищення державності і самостійності іншої країни. Нажаль, наслідки подібної політики ми можемо спостерігати на власному досвіті, через приклад відносин двох держав: РФ та України.

Українській політолог Євген Магда вважає, що інформаційна війна проти України, розпочата ще за довго до анексії Криму, спрямована не лише на дестабілізацію внутрішнього політичного середовища держави, а й на створення негативного іміджу України на світовій арені, показати усю ненадійність і нечемність подібного партнера[16].

Природні ресурси, незважаючи на появу нових, інформаційних, не втратили свою актуальність і впливовість, а також здатність до маніпулювання. Україна в даному контексті частково залежна від природних ресурсів Росії, так як є країною-транзитером, через своє відносно вигідне територіальне розташування. Відповідно це є приводом для сусіда мати повний контроль над внутрішньою і зовнішньою політики держави, яка може стати для нього загрозою. Розробка і початок реалізації плану по дестабілізації України можна вважати 2005 рік, коли тривала перша «газова війна». Відносно слабка на той час Україна на міжнародній арені попала під вплив Російської Федерації, і була представлена світу як нечесний, сумнівний транзитер газу. Враховуючи той факт, що за десятиріччя подібної співпраці Україна ніколи не зупиняла поставки природного гагу через свою територію. Цікаво, що незважаючи на відсутність доказів у крадіжках природного газу – поступали звинувачення. Одночасно з цим Росією було наголошено на необхідності будування нових газопроводів в обхід території України. [16, с. 140]

Україна за останні роки стала основним об’єктом інформаційної агресії зі сторони Російської Федерації. Серед прикладів інформаційних викликів можна відзначити «мовне питання», яке є одним із найулюбленіших у російських пропагандистів. Активне нав’язування ідеї надання російській мові статусу другої державної, надання більшої автономії деяким областям на

прикладі федералізації. Звичайно, з року в рік актуальність тих чи інших тем змінювався, в залежності від поточної політики. Але зазвичай все зводилось до таких проблем як:

- Питання Чорного моря, а також Чорноморського флоту;
- Крим і населення півострову, ще за довго до анексії був актуальною проблемою у відносинах двох держав;
- Енергетично-паливна проблематика, завжди була максимально уразливою до інформаційно-пропагандистських викликів [41].

Україна того часу, відносно нестабільна держава, яка не очікувала подібного від сусіда, була більш уразлива до викликів. Перша поразка на інформаційному фронті відбулась коли Україна добровільно позбулася ядерного статусу, втративши статус ядерної держави і позбулась певного відсотку впливу на міжнародній арені. Цей сценарій став реальність, адже велась активна інформаційна кампанія проти ядерного статусу України. Численні інформаційні вкидання про те, що Україна не здатна самостійно утримувати й обслуговувати ядерну зброю призвело до денуклеаризації. Вже сьогодні ми розуміємо усі масштаби наслідків цього процесу і можемо лише будувати здогадки, якою була б Україна зараз залишивши свій статус.

Насправді прикладів в історії відносин Україна – Росія, коли остання мала на меті підірвати Україну, її бренд, як з середини, так і з зовнішньої сторони було страшно як багато. Транслювання, викривлення фактів, дезінформації великої кількості людей відбувалось здається завжди. Україна ніколи не займала активно позицію в плані інформаційних атак, проте намагалась оборонятися.

Однак, одна із головних проблем інформаційно-пропагандистської кампанії РФ є те, що вона не завжди ведеться відкрито і заходи для зупинення не завжди є ефективними. Як вже було зазначено, однин із головних інструментів пропагандистів – телебачення. Нажаль в Україні впродовж останніх років, до 2020 гору якщо деталізувати, робота російських пропагандистів не розглядалась як реальна загроза національній безпеці. Втім

попит на російські засоби масової інформації продовжував зростати і не викликав жодних дій зі сторони держави, що їх наслідками можуть бути дестабілізація, сплив на людську свідомість і через це формування певного ставлення до того, чи іншого явища, і навіть до самої державності України.

У своїй політиці щодо України і не тільки, транслює думку – той, хто контролює потік інформацію, той має владу. Для реалізації цієї думки було створено безліч інструментів, штучних засобів, використано значну кількість державного бюджету лише через одне – доступ до людської свідомості [38].

2.3. Вплив інформаційно-пропагандистської кампанії РФ на внутрішню політику України

Інформаційно-пропагандистська кампанія розпочавшись задовго до Революції Гідності нанесла значний вплив на внутрішню політику України. Фактично, вона внесла свою лепту у формування сучасної України, розділивши її на до і після. Варто зазначити, що деякі наслідки були цілком сприятливі і навіть корисними, в якомусь сенсі. Тож відбувся такий собі хід, коли нападаючи на об'єкт ти сам стаєш уразливим і отримуєш частку наслідків. Однак, якщо в цілому розглядати вплив на внутрішню політику, то він має величезні масштаби і сьогодні, взагалі російські мотиви все ще існують в українському просторі, лише у 2020 році почались більш активні дії держави по відношенню до потенційних російських агентів, а також українських засобів масової комунікації, які транслюють солідарні з Росією думки щодо внутрішньої політики в Україні, тим самим розділяючи Україну на умовний Захід і Схід, як це було у 2014 році.

Одна із основних тактик російської пропаганди – давити на емоційну складову суспільства і це працювало до певного часу на максимально широку аудиторію. Проблемою стало розповсюдження тези про Україну як братський народ, Україна – «молодший брат\сестра», однак по відношенню до

«правильної» частини населення. Фактично в російському інформаційному просторі Україну розподілили на «наших» і «ваших», де наші – бойовики проросійських сил в Донецьку та Луганську, а ваші – так звані «бандеровці», нова «нелегітимна» влада чи хунта. ЗМІ використовували і використовують цей розподіл як засіб маніпулювання, в тому числі на міжнародній арені. Наприклад, захищаючі інтереси окупованих і контрольованих територій ніби це вибір народу, який там проживає.

Проте, ми прослідковуємо цікавий наслідок. Кампанія була настільки агресивна, що замість збільшення впливу Кремля на українське суспільство – відвернула від себе українських глядачів, які на власному досвіді побачили реальні події, які відбувались на Сході, а також в Криму і інших містах України. Активне військове протистояння ніби відкрило очі на реальність і дало поштовх на формування нової про-української політичної еліти. В історії конфлікту є приклади, коли ця кампанія по розпаленню ненависті не працювала і деякі найбільш відважні росіяни переходили на бік української армії, тим самим показуючи реальність і масштаб протистояння. Але, звичайно, для більшості росіян ця військова компанія стала ще однією «перемогою» і черговим підняттям рейтингів чинного президента і влади. Для українців ж, відкрите падіння рейтингу російських і проросійських політиків й підняття власної ідентичності й гідності.

З першого погляду на ситуацію, Російська пропагандистська компанія після 2014 року втратила свою результативність на втручання у внутрішню політику України. І дійсно, вплив на українську аудиторію був програшним, адже вони бачили альтернативну подачу інформації, яка істотно відрізнялась від дійсності. Однак це не означає, що вплив перестав існувати і втратив свою актуальність, навпаки він став ще небезпечнішим і прихованим. Росія використовуючи емоційні компоненти, блокувала раціональне мислення і найбільш уразливі до сприйняття «близької» думки області попали під вплив стаючи точкою найбільшої лояльності, а з тим і промоутерами потрібної Кремлю думки. Особливо, якщо говорити про Схід та Південь України.

Пропагандистко-інформаційна кампанія мала на меті знищити право українців на самостійність, показати її жорстокість і дискримінацію по мовному признаку, довести не тільки росіянам, а й самим українцям, що вони не гідні своєї ідентичності.

Окрім цього, Росія вкладає значні ресурси для переконання всього світу у своїй правоті щодо України, в її повній дискредитації у європейському і світовому суспільстві. Існує низка відомих і авторитетних осіб зі Сполучених Штатів Америки та Європи, які активно підтримують і поширюють російську інформаційну політику на широке коло осіб одночасно. А також існування і фінансування низки російських англомовних телеканалів, де можна прослідити політику Кремля. Нажаль Україна подібної кількості ресурсів для боротьби на світовому рівні, окрім офіційної дипломатії. І тільки за останні роки Україна розпочала роботу із зарубіжною аудиторією.

Отже російська пропагандистська машина складається з ряду державних органів, інформаційних агенцій і засобів масової комунікації, які фінансуються за державні кошти. Сюди також можна віднести Російську Православну Церкву МП як інструменту пропагандистського впливу на конкретні шари населення. Російська машина включає в себе також низку топових олігархів як сучасної Росії, так і України, які фінансуються за рахунок Кремля. З проросійськими олігархами в Україні за останні декілька років почали активно працювати і відривати нові судові справи.

В 2021 році, незважаючи на сторонні чинники такі як пандемія «COVID-19» пропагандистська кампанія продовжує існувати і далі. Навпаки, вони знайшли спосіб використати це як фактор впливу, засіб маніпулювати. Як завжди, граючи на людських емоціях. Так, основні цілі політики РФ залишилось незмінними. За буд-які нові обставини, світові потрясіння Росія буде прагнути повернути Україну до своєї сфери впливу. Продовжуючи блокувати мирне врегулювання конфлікту в Донбасі, сприяючи розхитуванні внутрішньополітичної ситуації за допомогою агентів, проросійських партій та відомих українських проросійських політиків, продовжуючи вести активну

пропагандистську кампанію, провокування соціальної нестабільності за допомогою агентів впливу – відомих блогерів, акторів, літераторів.

Подальший вплив пропагандистської кампанії не тільки на Україну, а й на весь світ залежить також від ряду глобальних трендів, позицій провідних акторів. Це може сприяти і на здатність України ефективніше протидіяти гібридній агресії. Існує ряд чинників, які можуть допомогти, або завадити:

1) Пандемія COVID-19; відновлення економіки, здатність або нездатність світової спільноти подолати її без критичних наслідків; блокування російської пропаганди проти України на фоні пандемії, її дискредитація на фоні неспроможності швидко відреагувати на спалах вірусу; маніпуляція вакцинуванням;
2) Нова адміністрація Сполучених Штатів Америки президента Дж. Байдена, його персональне ставлення до ситуації в Україні, ефективність його зовнішньополітичної політики на фоні пандемії; відновлення відносин з ЄС, політики США щодо Росії;
3) Трансатлантична єдність щодо санкційної політики відносно РФ;
4) Політика Росії на пострадянському просторі, відносна успішність або неуспішність політики, зокрема щодо Республіки Білорусь, де останні роки були максимально напруженими, в тому числі у відносинами з Росією і Україною.
5) Внутрішньополітична ситуація в Російської Федерації, на фоні виборів в державні структури; спроба вбивства опозиціонера Навального, його подальший арешт; нова хвиля суспільних мітингів у підтримку чесних виборів та свободи Навальному [4].

Усі ці фактори в той чи інший мірі можуть впливати на політику РФ щодо України, на її інтенсивність, ескалацію або деескалацію, часткове припинення чи посилення. Однак, як показує час, зазвичай на фоні нестабільної внутрішньої ситуації в Росії, головна мета керуючої влади привернути увагу до зовнішньо-політичних чинників, тим самим створивши новий прецедент на покращення рейтингів, як це було з

анексією півострова чи черговою ескалацією конфлікту в Донбасі. Перетворюючі міжнародну арену на світове політичне шоу, де люди – лише пішки у долонях лялькаря.

РОЗДІЛ 3. ПРОТИДІЯ ЗОВНІШНЬОЇ ІНФОРМАЦІЙНОЇ АГРЕСІЇ

3.1. Реакція України на зовнішню інформаційно-пропагандистську агресію

Агресія Росії в будь-якому сенсі проти України була неочікуваною в суспільстві і визвала широкий резонанс по всьому світу. Фактично, це був ніж у спину, так як ніхто не міг уявити подібний сценарій на момент 2013 – 2014 років. Однак вже зараз ми можемо аналізувати події минулого і розуміти, що передумов початку конфлікту було безліч і готуватись було до чого. Таким чином, в період з грудня 2013 року по березень 2015 був активний збройний конфлікт із Російською Федерацією, потужний вплив з боку пропаганди і основне – окупація частини території України.

Для досягнення своїх зовнішньополітичних амбіцій у військовій, політичній та економічній сфері Росія використовувала усі можливі ресурси задля потужного інформаційного впливу не тільки окупованих територій, а й територій під контролем українського уряду. Реакція українського суспільства мала певну не одностайність у баченні чи не баченні зовнішньої інформаційної агресії. Це сталось через певні чинники, такі як: належність частини українських громадян до російського ментального, культурологічного поля; доступ до російських соціальних мереж (під час активної фази конфлікту); проросійськи агенти впливу і домінування Росії і російської культури в інформаційному просторі України.

Реакцію України на зовнішню інформаційно-пропагандистську агресію не можна назвати швидкою і цілком успішною, особливо під час суспільного потрясіння. Однак її можна назвати комплексною і довготривалою, адже починають розроблятись механізми для запобігання подібних ситуацій у майбутньому.

З появою спільного ворога, який анексував частину території, розпочав збройний конфлікт і мав на мені окупувати ще більшу частину областей – український медіа простір почав працювати на випередження; створюючи свій

контент, більш об’єктивний і відносно незалежний. Відбувся поштовх для реалізації власного українського потенціалу на фоні піднятого патріотичного духу, що наводить на думку о лише часткової ефективності російської пропаганди на території України. Україна – незалежна держава, постраждала сторона і відповідно це призвело до широкого резонансу на міжнародній арені. Прийняття першої резолюції про підтримку територіальної цілісності України від 27 березня 2014 року [36].

Як вже було зазначено, протистояння проти інформаційного впливу РФ має бути комплексним і довготривалим, його також можна розподілити на внутрішнє і зовнішнє.

Зовнішнє протистояння – довготривале, основане на розумінні усього масштабу загрози з боку Російської Федерації на стабільність Європейського Союзу і кожної окремої держави, розуміння вірогідності появи нових постраждалих акторів. Сьогодні Європейський Союз – мішень російських інформаційних атак. Задля подолання спільної загрози слід розробляти і дотримуватись спільних програм розвитку, створення єдиного цифрового простору і постійний діалог «ЄС – Україна»

Реакція України має бути комплексною і максимально охоплювати усі сфери людської діяльності. Протидія має відбуватись, і відбувається на різних рівнях і стосуватись не лише очевидній протидії пропаганди, а й на забезпеченні власного незалежного медіа простору, який в майбутньому зможе самостійно забезпечити здатність до інформаційних викликів.

Прозорість медіа, особливо мережі Інтернет – одна із головних проблем не тільки в Україні, а й в багатьох західних сусідів. Необхідна розробка законодавства про прозорість медіа, яке має спростити погук інформації про власників, джерела того-чи іншого матеріалу, джерела фінансування певного медіа ресурсу.

Прозорість політичних та інформаційних кампаній, особливо у передвиборний період – є ключовим елементом за для подальшої внутрішньополітичної стабільності, адже сьогодні без налагодженого

законодавства в інформаційній сфері ми маємо безкінечний список кандидатів на виборах, деякі з яких є максимально відкрито проросійськими. Створення системи допоможе запобігти цього в майбутньому. Сьогодні Україна вже почата перші кроку у цьому боці, засуджуючи проросійських депутатів, блокуючі проросійські телевізійні канали, але це лише тимчасове зупинення ефективної машини, потрібні більш довгостроково орієнтовані дії.

З боку національних урядів існує затверджена стратегія інформаційної безпеки, яка звичайно потребує постійного оновлення і моніторингу, адже інформаційна сфера змінюється кожного дня і дуже важливо бути готовим до появи нових загроз і викликів які можуть задати шкоди. Також варто зазначити санкції проти російських інформаційних агентів впливу. В Україні вже більше 4 років існує практика заборони на в'їзд частині російських медіа персонам, які можуть створити певні прецеденти небезпеки, а не деяких накладені політичні санкції з боку не тільки України, но і ЄС й США. Зокрема один із топових пропагандистів РФ – Дмітрій Кісєльов та Володимир Соловйов, які фактично є лідерами усієї пропагандистської машини.

Також, важливим кроком для України стала розробка Доктрини інформаційної безпеки спрямованої на забезпечення цілей. В основному у ній прописано розподіл діяльності між різними інституціями державної влади, роль інституцій громадянського суспільства. Однак, сьогодні прописувати численні документи вже не є ефективним – варто працювати над їх практичним виконанням. Важливість розвитку стратегічних комунікацій не піддається сумніву, так у Доктрині прописані цілі щодо поєднання публічної дипломатії, зв'язків із громадськістю, військовий, інформаційних та психологічних операцій, заходів на просування цілей держави [30].

3.2. Міжнародні приклади протидії зовнішньо-інформаційної агресії

Україна одна із небагатьох держав, яка зіткнулась з активним прояво інформаційної агресії, однак Європейський Союз і Сполучені Штати Америки також потрапили під зону ураження, і отримали певну кількість інформаційного впливу. Втім реагування на новітні виклики були негайними. Сполучені Штати фактично є лідером серед демократичних держав по рівню забезпечення інформаційної безпеки і готовності до зовнішньо-політичним втручанням. Сьогодні найбільш вдосконаленою системою кіберзахисту критично важливої інфраструктури (тобто інформаційної інфраструктури, ураження або знищення якої може призвести до втрати працездатності відповідного простору й поставити під загрозу суспільну та державну безпеку в цілому) функціонує у Сполучених Штатах Америки.

Питанню інформаційної безпеки приділив увагу Президент США Б. Клінтон ще у липні 1996 року. Він оголосив про формування Президентської комісії із захисту критичних інфраструктур. І вже через рік, у заключному звіті, комісія повідомила, що загрози критичній інфраструктурі реальні. Фактично це вперше закріпило незворотність необхідності забезпечення потужної системи інформаційної безпеки та створення засобів протидії загрозам.

На сьогоднішній день, інформаційна безпека США – одна із найпотужніших у світі, здатна запобігти атаки критичного масштабу. На момент 2020 року щонайменше 38 штатів, Вашингтон, округ Колумбія, і Пуерто-Ріко представили або прийняли до розгляду понад 280 законопроектів або резолюцій, які в значній мірі стосуються кібербезпеки. Деякі з областей, в яких спостерігається найбільша законодавча активність, включають заходи:

- Вимоги до державних установ впровадити навчання або конкретні види політики і практики безпеки, а також поліпшити реагування на інциденти і готовність до них;
- Посилення покарань за комп'ютерні злочини;

- Регулювання кібербезпеки в страховій галузі або страхування кібербезпеки.
- Створення цільових груп, рад або комісій для вивчення або консультування з питань кібербезпеки.
- Підтримка програм або стимулів для підготовки і навчання в області кібербезпеки.

У 2020 році щонайменше 20 штатів прийняли 46 ключових законопроектів, пов'язаних з кібербезпекою [50].

Одним із суттєвих наслідків пандемії COVID-19 – є перехід більшості сфер діяльності на онлайн формат роботи, що створила ще більший попит на забезпечення системи інформаційної безпеки. Сьогодні Європейський союз працює за різними напрямками для підвищення інформаційній стійкості, захищаючи комунікації і дані, забезпечуючи безпеку онлайн суспільства і економіки.

Європейська комісія і Верховний представник із закордонних справ і політики безпеки представили нову Стратегію кібербезпеки ЄС на кінець 2020 року. Стратегія охоплює безпеку основних служб, таких як лікарні, енергетичні мережі та залізні дороги. Вона також охоплює безпеку постійно зростаючого числа підключених об'єктів в наших будинках, офісах і на заводах, створення колективного потенціалу для реагування на великі кібератаки і роботу з партнерами по всьому світу для забезпечення міжнародної безпеки і стабільності в кіберпросторі. Стратегія описує, як Об'єднане кіберпідрозділ може забезпечити найбільш ефективне реагування на кіберзагрози, використовуючи колективні ресурси і досвід, наявні в розпорядженні ЄС і держав-членів [26].

Звичайно, законодавча база в європейських державах також сконцентрована на боротьбою з дезінформацією та інформаційним впливам. Однім із помітніших є проект французького закону про боротьбу маніпуляцією за допомогою інформації. Проект передбачає:

- Боротьбу з навмисною маніпуляцією інформацією

- Санкції у раз навмисних дій;
- Поширення на виборчий період;
- Ключову роль спеціальних суддів у винесенні швидких рішень про санкції;
- Певні вимогу від інтернет-платформ щодо забезпечення прозорості, яка дозволятиме відстежувати тих, хто веде кампанії з дезінформації.

Всеосяжної метою ЄС є просування моделі кіберпростору, заснованої на верховенстві закону, правах людини, свободи і демократичних цінностях. Для просування цих цінностей Європейський Союз повинен:

1) розширити свою участь в процесі стандартизації, в тому числі шляхом збільшення свого представництва в європейських і міжнародних організаціях з розробки стандартів;
2) взяти на себе активну роль в просуванні позицій держав-членів на міжнародних форумах, а також розробити позицію ЄС щодо застосування міжнародного права в кіберпросторі;
3) продовжувати просувати і захищати права людини та основні свободи в Інтернеті;
4) зміцнювати і розширювати діалог щодо кіберпростору з третіми країнами, зміцнювати співробітництво ЄС і НАТО в області кібербезпеки;
5) захищати багатостороннє управління Інтернетом;

Стратегія кібербезпеки ЄС ставить амбітні цілі, як в плані нових нормативних актів, так і в плані міжнародного співробітництва. Проте, поки кіберзлочинність залишається надзвичайно прибутковою справою для злочинців, безпеку критично важливих інфраструктур, компаній і звичайних громадян залишатиметься під загрозою. Таким чином, ЄС необхідно активізувати зусилля, щоб мати можливість протистояти кібератакам майбутнього[44].

3.3. Проблематика інформаційного простору: механізми регулювання

Інформаційний простір – це сукупність суб'єктів інформаційної взаємодії або впливу; інформаційна інфраструктура, яка забезпечує можливість обміну між суб'єктами суспільних відносин, котрі формуються в наслідок утворення, передачі і зберігання інформації, обміну інформації всередині суспільства [4].

Науковець Л.Біловус вважає, що у центрі інформаційного простору знаходиться суб'єкт, який створює, накопичує, передає та зберігає інформацію. Тобто суб'єкт – усі, хто використовують сучасні технології. Інформаційний простір – відмінний від звичайного відсутністю фізичного місця, проте він має й певні обмеження – конвенціональні межі, наприклад державна таємниця. Інформаційний простій надважливий і має займати ключове місце в державній політиці. Україна має забезпечити формування і безпеку власного інформаційного простору, особливо в сучасних реаліях, коли інформаційна сфера стає найважливішою [20, с. 189].

У Законі України від 05.10.2017 № 2163-19 "Про основні засади забезпечення кібербезпеки України" відсутнє поняття "інформаційний простір". Однак, наведено визначення поняття "національні електронні інформаційні ресурси" – систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється - інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів [46].

Коли говорять про захист національного інформаційного простору, як такого, то мають на увазі державний інформаційний суверенітет. Інформаційний суверенітет означає виняткове право держави на формування

й використання усіх інформаційних засобів, створених на засадах і за державний кошт. Порушення інформаційного суверенітету може привести до інформаційної війни між державами, чи організаціями.

В Україні забезпечення інформаційної безпеки має відбуватися шляхом практичної реалізації державної політики і за рахунок: дотримання й забезпечення реальних прав і свобод кожного громадянина України; максимально доступної інформаційної політики для всіх користувачів нею поза межами України; захисту національного інформаційного простору та потужного розвитку інформаційних технологій, інформаційної індустрії у самій Україні" [39].

Державна інформаційна політика здійснюється як у межах інформаційного простору так і поза ним, інформаційний простір України є складовою європейського і світового інформаційного простору. Світовий простір – розгалужена система структур, яка забезпечує виробництво, зберігання та використання інформації як всередині країни так і поза неї [22].

Адаптація до глобального інформаційного простору є одним із головних як внутрішньо- так і зовнішньополітичних завдань для України. Зокрема регулювання обміну інформацією як відкритої, так і з обмеженим доступом, експорту товарів та технологій, що підлягають експортному контролю відповідно до міжнародних зобов'язань України.

Чинником формування здорової української спільноти є національний інформаційний простір, який впливає на всі сфери суспільних відносин. Формування подібного суспільства зумовлює подолання цифрового відриву, продовження розвитку засобів масової інформації в Україні, а також сприяти покращенню безпеки інформаційних та телекомунікаційних систем

В той же час, інформатизація попри усі свої переваги створює величезну різноманітність інформаційних загроз: від витіснення на внутрішньому інформаційному ринку вітчизняних продуктів більш конкурентоспроможними аж до ведення цілеспрямованих інформаційних війн. Інформаційні війни будуть домінантним фактором у нинішньому столітті

згідно з доповіддю Національної ради з розвідки США, і Україна, як держава з довготривалим конфліктом гібридного характеру підпадає під пряму загрозу. Інформаційні війни можуть вестимуть на всіх рівнях соціальної структури, в тому числі між блоками держав. З урахуванням цього функція інформаційної безпеки держави в усіх регіонах світу набуває особливої важливості [23]

Складна ситуація в світовому інформаційному просторі обумовлена наступним:

- багато акторів зіштовхнулись щ проблемами пов'язаними з кіберзлочинністю, кібертероризмом та іншим загрозам сучасного інформаційного суспільства;

- з'являються ще більше випадків інформаційної агресії як проти конкретних осіб, так і державних структур;

- агресивна реклама, маніпуляція свідомістю людей за допомогою телевізійних шоу, реалізація нових інформаційно-психологічних операцій;

- усі передові країни так чи інакше ведуть розробку нових інформаційних технологій, інформаційної зброї або її елементів;

- використання інформаційної зброї може бути порівняно зі застосуванням зброї масового ураження;

- реальну небезпеку людства та міжнародному порядку становлять нові, потужніші інформаційні загрози й виклики [2, с. 3-7].

Сучасні інформаційні технології змінюють характер інформаційної взаємодії між суспільством і державою. Так, держава може стати координатором дій різних суб'єктів суспільства. Сформувати необхідну законодавчу і нормативно-правову базу, спрямовану на ці дії, а також створити усі умови для розвитку.

Інформаційний простір – глобальний чинник трансформації. Отже, формування єдиного світового інформаційного простору стає глобальним чинником світового розвитку, що зумовлює суспільний прогрес, і перетворюють інформацію на найважливішій стратегічній ресурс держав.

ВИСНОВКИ

Термін інформаційне суспільство – не новий, однак це відносно новий стан історичного розвитку, коли більшість займається створенням, зберіганням, переробкою і реалізацією інформації. Масштабні виклики і загрози в інформаційній сфері вже не нове явище, а скоріше константа з якою не треба боротись, але яку потрібно контролювати. Контроль за інформаційними ресурсами необхідний, адже у випадку анархії – інформація перетворюється на уразливу зброю світового масштабу. Інформація – нове золото, ресурс, і в той ж момент інструмент, за допомогою якого можна змінювати світ, руйнувати держави, створювати нові державотворення і змінювати світовий порядок. Фактично, інформація сьогодні – це влада; а той, хто володіє інформацією – править світом. Коли інформаційна сфера актора слабка, вона буде максимально уразлива до інформаційного впливу більш впевненого і сильного гравця. Таким чином відбувається часткова, або повна інформаційна експансія в новому столітті.

Було проаналізована сучасний стан нормативно-правового забезпечення інформаційної безпеки. Стрімкий попит на покращення нормативно-правового забезпечення відповідно до нових реалій, збільшення кількості інформаційно-комунікаційних операції через перехід на онлайн формат майже всіх сфер людської діяльності. Україна в випадку нормативно-правового забезпечення намагається відповідати стандартам Європейського Союзу і робить правильні кроки до досягнення високого рівню інформаційної безпеки.

Було окреслено інформаційну агресію Російської Федерації по підношенню до України, проти України і українців як цілком важливий фактор дестабілізації внутрішньополітичного середовища в Україні. Так, за допомогою інформаційних технологій можна зробити усе, що тільки можна уявити в новому інформаційному світі. Сформувати будь-які потрібні тренди та тенденції для досягнення певної мети, сформувати суспільну думку, створити свою правду, дезінформуючи одночасно велику кількість людей –

саме так формується «нова правда», нове уявлення на події відмінне від думки більшості.

Встановлення межі початку інформаційно-пропагандистської кампанії РФ по дестабілізації і світової дискредитації України як самостійного актора на міжнародній арені. Насправді, в історії відносин Україна – Росія, можна навести достатньо багато прикладів підриву України, її бренду як надійного партнера – тим самим ще більше віддаливши Європейській Союз. Україна ж в свою чергу ніколи не займала позицію нападаючого, маючи на меті лише захистити власну позицію, власні цінності і держаний суверенітет.

Інформаційно-пропагандистська кампанія, яка розпочавшись задовго до Революції гідності, нанесла значний вплив на внутрішню політику України. Фактично, вона внесла свою лепту у формування сучасної України, розділивши її на до і після. Варто зазначити, що деякі наслідки були цілком сприятливі і навіть корисними, в якомусь сенсі. Тобто – ми маємо ситуацію, коли бажання дискредитувати зіграло проти агресора, даючи поштовх до розвитку і покращенню власної спроможності вести боротьбу з найсильнішим актором.

Протидія зовнішньої інформаційної агресії – головний пріоритет сучасної України. Сьогодні головне поля боя – в медіа просторі, і незважаючи на відносно вивий вид ведення війні – головна задача створити власний механізми забезпечення безпеки на основі прикладів більш прогресивних європейських і американських колег. Необхідність наздогнати ЄС і США в забезпеченні інформаційної безпеки стоїть дуже гостро, адже інформаційна сфера крайнє динамічна у своєму розвитку. И виклики сьогодні можуть стати неактуальними, а замість них з’являться нові – ще більш небезпечні.

Головна задача і стратегія, яку має переслідувати Україна – перестати говорити, почати діяти і реалізовувати усі зазначені плані, вкладаючи весь потенціал, адже є вірогідність, що ще декілька років і змінити ситуацію певної інформаційної експансії України – Росією буде майже неможливо.

СПИСОК ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Біловус Л. Український інформаційний простір: сьогодення та перспективи. URL: http://dspace.wunu.edu.ua/handle/316497/8741
2. Бондаренко В.О., Литвиненко О.В. Інформаційна безпека сучасної держави: концептуальні роздуми // Стратегічна панорама. – 1999. – № 1-2. – С. 127-133.
3. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики : Вибр. наук. праці / О. С. Власюк. – К. : НІСД, 2016. – 528 с.
4. Герасимчук С., Шелест Г. Сценарії і тренди 2021: міжнародна політика. Фонд імені Фрідріха Еберта, 2021. – 46 с.
5. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. О. Гнатюк // Ukrainian Scientific Journal of Information Security, 2013. – Vol. 19/ – Issue-2.
6. Гуз А.М. Історія захисту інформації в Україні та провідних країнах світу: Навчальний посібник. – К.: КНТ, 2007 – 260 с.
7. Данилишина Е.А. Роль рекламы в контексте современного этапа процесса глобализации. Актуальні проблеми політики. Збірник наукових праць. - Одеса: “Юридична література”. - 2001. - Вип. 10-11. - С.702-708
8. Данилишина К.О. Впливи інформаційних світових потоків на пострадянське суспільство // Актуальні проблеми політики. Збірник наукових праць. – Одеса: „Юридична література”. – 2003. – Вип. 17. – С.257-263
9. Димлевич, Н. Информационные войны в киберпространстве — Великобритания и Израиль. URL: http://www.otechestvo.org.ua/main/201011/1612.ht
10. Захаренко К. Глобальна природа інформаційної безпеки / К. Захаренко// Нова парадигма. - № 132. – С.87-94

11. Закон України «Про інформацію» від 02 жовтня 1992 р..Відомості Верховної Ради України (ВВР). – 1992. – № 48. – С. 650
12. Кесареева Т. П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. канд. юрид. Наук : 12.00.08 / Т. П. Кесареева. – М., 2002. – С. 20,36.
13. Кирильчук Є.О. Проблеми національної інформаційної безпеки України в контексті сучасних національних державотворчих процесів та світової інтеграції. Наукові праці МАУП. 2013. №1(36). С. 60-63.
14. Конституція України : Закон України від 08.06.1996 р. № 254к/96-ВР / Відомості Верховної Ради України. 1996. № 30. Ст. 141.
15. Лисенко С. О. Конституційні засади розуміння інформаційної безпеки. Публічне урядування. 2016. № 4. С. 154-161.
16. Магда Є. Виклики гібридної війни: інформаційний вимір [Текст] / Євген Магда // Наукові записки Інституту законодавства Верховної Ради України . – 2014. – № 5. – С. 138-142
17. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України. Автореферат дисертації на здобуття наукового ступеня кандидата юридичних наук. Спеціальність: 12.00.01 − теорія та історія держави і права, історія політичних і правових учень. − К., 2007. – 22
18. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. ... канд. юрид. наук: 12.00.01. Київ, 2007. 236 с.
19. Маклюэн М. Понимание Медиа: Внешние расширения человека / Пер. с англ. В. Николаева; Закл. ст. М. Вавилова. – М.; Жуковский: «КАНОН-пресс-Ц», «Кучково поле», 2003. – 464 с.
20. Манойло А. Государственная информационная политика в особых условиях: монография / А. Манойло. – М. : МИФИ, 2003. – 388 с

21. Нестеряк Ю.В. Аналіз моделей іфнормаційної політики та державного регулювання засобів масової комунікації. Публічне управління та митне адміністрування, №2(15)/2016. – с. 65-70.
22. Онищенко О.С. Національні інформаційні ресурси як інтегративний чинник вітчизняного соціокультурного середовища. Монографія / [О.С. Онищенко, В.М. Горовий, В.І. Попик та ін.] ; НАН України, Національна бібліотекака України ім. В.І. Вернадського. – К., 2014
23. Пилипчук В.Г. Системні правові проблеми формування інформаційного суспільства Х.: НДІ державного будівництва та місцевого самоврядування, 2012. 214 с.
24. Почепцов Г. Г. Коммуникативные технологии XX века : монография / Г. Г. Почепцов. – К. : Ваклер, 2000. – 352 с.
25. Про Заяву Верховної Ради України «Про відсіч збройній агресії Російської Федерації та подолання її наслідків : Постанова Верховної Ради України від 21.04.2015 р. № 337-VIII / Відомості Верховної Ради України. 2015. № 22. Ст. 153.
26. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-19 .URL : http://zakon0.rada.gov.ua/laws/show/2163-viii.
27. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : Указ Президента України від 26.05.2015 р. № 287/2015
28. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 р. № 96/2016
29. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Указ Президента України від 01.05.2014 № 449/2014. URL : http://zakon5.rada.gov.ua/laws/show/449/2014

30. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. №47/2017
31. Про Стратегію сталого розвитку «Україна – 2020» : Указ Президента України від 12.01.2015 р. № 5/2015
32. Радутний О.Е. Кримінальна відповідальність юридичної особи стане кроком до закріплення віртуальності життєвого простору. "Юридична Академія України ім. Ярослава Мудрого". – № 1/2011.
33. Радутний О.Е. Поняття та ознаки інформаційної агресії на законодавчому рівні в кримінально-правовій сфері. "Інформація і право" № 2(14)/2015. С. 58-63.
34. Рассолов И. М. Право и Интернет. Теоретические проблемы / И. М. Рассолов. – М. : НОРМА, 2003. – С. 251-254.
35. Ромащенко В. А. Правове регулювання інформаційного суспільства в Україні: загальнотеоретичне дослідження: автореф. дис. канд. юрид. наук: спец.: 12.00.01. Одеса, 2018. 26 с.
36. Резолюція Генеральної Асамблеї ОООН про територіальну цілісність України від 27 березня 2014 р. № 68/262
37. Савінова Н.А. Інформаційна політика України у дискурсі безпеки людини і громадянина : зб. матер. наук.-практ. конф. ["Актуальні проблеми управління інформаційною безпекою держави"], (м. Київ, 19 березня 2015 р.). – К. : Центр навч., наук. та період. видань НА СБ України, 2015. – 512 с. – С. 119-123.
38. Сасин Г.В. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір). «Політологія» №3(119)/2015. С. 18-23.
39. Собків Я. М. Класифікація інформаційних прав і свобод людини та громадянина. URL: https://goal-int.org/klasifikaciya-informacijnix-prav-i-svobod-lyudini-ta-gromadyanina/

40. Сувенірна продукція як засіб радянської пропаганди. URL: https://knife.media/soviet-merch/
41. Цуканова О.В. Інформаційні війни: вплив на суспільство / О.В. Цуканова. URL: http://www.sworld.com.ua/konfer34/800.pdf.
42. Шимченко Л.А. Українське суспільство в умовах глобалізації // Український соціум: соціально-політичні виміри: Матеріали круглого столу від 28 грудня 2004 р. / За заг. ред. Крисаченка В.С. – К.: Знання України, 2005.
43. Cohen B. The Press and Foreign Policy, Princeton / B Cohen. - NJ: Princeton University Press – 1963. – 288 p.
44. Cybersecurity Legislation 2020. URL : https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx
45. European Union's new cybersecurity strategy. URL: https://www.lexology.com/library/detail.aspx?g=ad1630cc-5172-4600-9a53-985fb6c845db
46. Freedom House опасается, что в Украине может усилиться цензура в интернете URL: https://strana.ua/news/127317-freedom-house-opasaetsja-chto-v-ukraine-mozhet-usilitsja-tsenzura-v-internete.html
47. Kamel, S., and Hussein, M., "The Emergence of E-Commerce in a Developing Nation" Benchmarking, Bradford: 2014. P. 146– 15
48. Lemos Robert. Cyberterrorism: The real risk [Електронний ресурс] / Robert Lemos; Центр дослідження комп'ютерної злочинності. URL: http://www.crimeresearch.org/library/Robert1.htm.
49. O'Heffernan P. Mass Media and American Foreign Policy: Insider Perspectiveson Global Journalism and the Foreign Policy Process / P. O'Heffernan – Norwood, NJ: Ablex – 1991. – 262 p
50. The Cybersecurity Strategy. URL : https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy