Міністерство освіти і науки України
Кам’янець-Подільський національний університет імені Івана Огієнка
Історичний факультет
Кафедра політології та філософії

Дипломна робота
бакалавра
з теми: **“ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ”**

Виконала:
студентка 4 курсу, групи Р1-В20
спеціальності 052 Політологія
денної форми навчання
Повержук Ірина Вадимівна

Керівник:
Віннічук О. В.,
кандидат політичних наук, доцент,
завідувач кафедри політології та
філософії

Кам’янець-Подільський – 2024

ЗМІСТ

ВСТУП

В контексті сучасних викликів, що мають місце в умовах російсько-української війни, важливо розуміти, що інформаційна безпека стала визначальним аспектом функціонування суспільства та держави в цілому. Ворожі дії, спрямовані на поширення дезінформації та маніпулювання громадською думкою, підривають безпековий фундамент країни. Дослідження впливу інформаційних потоків та ідентифікація загроз в умовах війни є ключовими аспектами, які відіграють важливу роль у напрацюванні напрямів розвитку системи інформаційної безпеки. Розуміння цих факторів дозволить розробити ефективні стратегії захисту інформаційної безпеки та забезпечити стійкість суспільства в умовах кризи.

Повномасштабне вторгнення в Україну розширило спектр застосування пропагандистських методів, мови ворожнечі та інших інструментів, які використовуються з метою маніпулювання громадською думкою та сприйняття подій. В даному контексті, розуміння сутності та розробка ефективних стратегій інформаційного захисту є важливим завданням для українського суспільства в цілому.

Актуальність здійснення комплексного аналізу інформаційної безпеки в умовах російсько-української війни полягає у тому, що інформаційна безпека стає ключовим фактором забезпечення національної безпеки України. Дії рф включають широкомасштабну пропаганду, дезінформацію та кібератаки, спрямовані на “викривлення” громадської думки та дестабілізацію України в усіх сферах життя суспільства.

Таким чином, важливо проаналізувати головні аспекти, включаючи механізми формування та проблеми захисту, форми та методи поширення та сприйняття інформації в умовах війни, простежити прийоми захисту та проблеми забезпечення інформаційної безпеки. Це дозволить узгодити механізми інформаційного захисту суспільства та виклики, що постали в умовах гібридної війни.

Мета дослідження полягає у аналізі інформаційної безпеки в умовах російсько-української війни.

Під час написання роботи було поставлено декілька ключових **завдань**, які дозволять більш детально проаналізувати зміст цього дослідження:

- розкрити сутність поняття інформаційної безпеки та основні моделі;
- виокремити нормативно-правові аспекти регулювання інформаційної безпеки в Україні;
- проаналізувати політичну пропаганду та мову ворожнечі як ключові проблеми українського інформаційного простору в умовах війни;
- розкрити роль медіа та соціальних мереж в інформаційному протистоянні в умовах війни;
- охарактеризувати прийоми захисту інформаційного простору України через призму впливу громадянського суспільства;
- проаналізувати проблеми із забезпеченням інформаційної безпеки України в умовах повномасштабного вторгнення.

Об'єктом дослідження є інформаційна безпека.

Предметом дослідження є система інформаційної безпеки України в умовах російсько-української війни.

Методи дослідження. Для здійснення аналізу інформаційної безпеки в умовах російсько-української війни використовуються загальнонаукові методи, так і спеціальні політологічні методи.

За допомогою теоретичного методу було розкрито поняття "інформація" та "інформаційна безпека". Метод системного аналізу дозволив охарактеризувати основні моделі інформаційної безпеки, цілісно окреслити прийоми захисту інформаційного простору з метою обґрунтування системної цілісності поняття.

За допомогою методу контент-аналізу було проаналізовано нормативно-правову базу інформаційної безпеки України. Також розглянуто

ініціативи та проєкти такі як: “StopFake”, “BRAMA”, “MRIYA”, “ФактЧек”, що працюють задля захисту інформаційної сфери в умовах російсько-української війни.

Соціологічний підхід дозволив простежити вплив громадянського суспільства на процес захисту інформаційної безпеки в умовах російсько-української війни.

Зазначені методи дослідження дозволяють ефективно дослідити та зробити висновки щодо інформаційної безпеки в Україні в умовах російсько-української війни.

Наукова новизна. Кваліфікована робота полягає у впровадженні теоретичного аналізу з практичними дослідженнями інформаційної безпеки в контексті російсько-української війни, що є важливим внеском у розвиток наукового та практичного розуміння інформаційної безпеки.

Проаналізовано складнощі щодо забезпечення інформаційної безпеки та необхідність впровадження комплексних заходів для її ефективного забезпечення.

Системно розкрито роль та вплив громадського суспільства у контексті забезпечення інформаційної безпеки через громадські організації та проекти, що підкреслює важливість активної участі громадськості у захисті інформаційного простору. Проаналізовано основні тенденції інформаційного протистояння в умовах активної російсько-української війни. Простежено основні проблеми із забезпеченням інформаційної безпеки України в умовах російсько-української війни.

Практичне значення роботи. Дослідження інформаційної безпеки в умовах російсько-української війни, її прояви та прийоми протидіїї можуть бути використані як у теоретичного, так і аналітичного змісту роботи. Це стосується проблем забезпечення захисту інформаційної безпеки, механізмів протидії, а також її активних проявів у суспільстві через призму використання пропаганди, мови ворожнечі, маніпулятивних технологій тощо.

Матеріали дослідження можуть бути використані у навчальному

процесі під час підготовки студентами до семінарських/практичних занять з таких дисциплін, як: “Інформаційні та комунікаційні технології в політиці”, “Політичні комунікації та паблік рілейшнз”.

Варто зазначити, що результати дослідження можуть використовуватися під час організації тренінгових заходів щодо забезпечення захисту громадянського суспільства від інформаційних загроз у мас-медіа та соціальних мережах.

Апробація результатів дослідження. Результати дослідження були апробовані під час наукової конференції студентів і магістрантів за підсумками НДР у 2023-2024 навчальному році (м. Кам’янець-Подільський, 9 квітня 2023 р.)

Публікації.

Повержук Ірина. Інформаційна пропаганда в умовах російсько-української війни. Збірник наукових праць студентів та магістрантів Кам'янець-Подільського національного університету імені Івана Огієнка. [Електронний ресурс]. Кам’янець-Подільський: Кам’янець-Подільський національний університет імені Івана Огієнка, 2024. Вип. 18.

Джерельна база. В контексті досліджуваної теми були використані роботи вітчизняних дослідників, а саме: Вітюк Н. “Особливості дискурсу політичної пропаганди в умовах інформаційно-психологічної війни” [2], Даценко А. Ю. “Боротьба з російською дезінформацією як напрям захисту інформаційного простору України в умовах «гібридної війни” [6], Дячков Д.В. “Формування моделі політики інформаційної безпеки на основі концепцій “глибинного захисту”” [10], Згуровський М. “Проблеми інформаційної безпеки в Україні, шляхи їх вирішення” [12], Ільніцька У. “Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам” [14], Ісакова Т. О. “Мова ворожнечі як проблема українського інформаційного простору Ісакова Т. О. “Мова ворожнечі як проблема українського інформаційного простору” [17], Карпчук Н. “Медіа як невоєнний метод впливу в гібридній

війні” [19], Косогов, О. М.; Сірик, А. О. “Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на Сході України” [23], Курбан С. О. “Сучасні інформаційні війни у мережевому он-лайн просторі: навчальний посібник” [26], Маркітантов В., Рибщун О., Віннічук О.В. “Російська гібридна війна: від доктрини до тактики : навчальний посібник” [29], Мельник М.О. “Аналіз побудови моделі політики інформаційної безпеки підприємства” [30], Новородовська Н.О., Вакулич В.М. “Російська пропаганда агресії проти України (2014–2021 рр.)” [36], Панченко О. А. “Види та складові інформаційної безпеки” [41], Прищепа Г. ““Мова ненависті” як лінгвістичний маркер гібридної війни”” [50], Чмир Я. “Сучасні проблеми інформаційної безпеки України та перспективні напрями їх вирішення” [72], Шпилик С. “Інформаційна війна, пропаганда та PR: такі схожі й такі різні...” [75] та інші.

Однією із актуальних робіт для дослідження є праця української дослідниці Младьонової О. Д. “Інформаційна безпека як складова національної безпеки України”. У даній роботі проаналізовано інформаційну безпеку як складову національної безпеки, а також визначено, що метою національної безпеки є задоволення національних інтересів держави, суспільства.

Важливою працею є навчальний посібник дослідників: Маркітантова В.Ю., Рибщуна О.В., Віннічук О.В. “Російська гібридна війна: від доктрини до тактики : навчальний посібник”. Він спрямований на дослідження сутності гібридної війни, стратегічні цілі та наміри російської федерації. Проаналізовано еволюцію російської-української війни, де описано основні тактики та види озброєнь, які використовують російські військові.

Актуальною для нашого дослідження є наукова публікація Чмира Я. “Сучасні проблеми інформаційної безпеки України та перспективні напрями їх вирішення”. У ній досліджено проблеми забезпечення інформаційної безпеки держави. Було зазначено, що однією із найголовніших проблем інформаційної безпеки України є інформаційна експансія та необ’єктивне

висвітлення подій з боку росії. У статті розкрито пріоритетні напрями державної інформаційної політики в Україні.

Структура та обсяг дипломної роботи включає вступ, три розділи, шість підрозділів, висновки, список використаної літератури та джерел. Всього 75 сторінок. Список використаних джерел і літератури налічує 83 позиції.

ВИСНОВКИ

1. Під час проведення дослідження було розкрито сутність інформаційної безпеки, яка полягає у забезпеченні доступності та цілісності інформації, особливо в контексті російсько-української війни.

У сфері політичної науки поняття “інформаційна безпека” є багатозначним та розглядається у наступних аспектах: забезпечення громадян якісною та доступною інформацією з різних джерел; комплекс заходів для контролю розповсюдження конфіденційної інформації для захисту від загроз та атак, а також є станом захищеності об'єктів від інформаційних загроз.

Описуючи моделі інформаційної безпеки: модель Белла-ЛаПадули, модель Clark-Wilson (BLP), модель “Адепт-50”, було визначено, що вони відображають комплекс заходів, спрямованих на запобігання порушення безпеки інформації та моніторинг ефективності забезпечення безпеки.

Тому, дослідження поняття та моделей інформаційної безпеки розкриває їхню актуальність у сучасному інформаційному простору.

2. Під час аналізу нормативно-правових актів, що регулюють інформаційну безпеку в Україні, відстежено особливості забезпечення захисту інформації на різних рівнях – від державних до приватних структур.

У процесі проведення дослідження з’ясовано, що законодавство України включає низку законів та нормативних актів, спрямованих на забезпечення захисту інформації: Конституція України, Закон України “Про інформацію”, Закон України “Про національну програму інформатизації”, Указ Президента України “Про доктрину інформаційної безпеки України”, Концепція національної безпеки України. Зазначені нормативні документи визначають права та обов'язки суб'єктів інформаційних відносин, механізми контролю та відповідальність за порушення інформаційної безпеки.

Варто зауважити, що запровадження стратегій інформаційної безпеки, є важливим кроком у виявленні, аналізі та протидії потенційним загрозам.

Завдяки комплексній підготовці та застосуванні стратегічних підходів, створено ефективну стратегію, яка гарантує безпеку на різних рівнях.

Також було зазначено, що розробка та впровадження електронної інформаційної системи “Електронний Уряд” є важливим кроком для забезпечення конфіденційності та доступу громадян до якісної інформації. Це відкриває шлях до більш ефективного та прозорого управління, яке відповідає потребам суспільства та сприяє розвитку держави.

В цілому, аналіз нормативно-правових аспектів регулювання інформаційної безпеки підтверджує, що важливо не лише впроваджувати та вдосконалювати законодавство, що включає розробку нових нормативно-правових актів, які враховують зміни в інформаційній сфері, а також постійно їх оновлювати відповідно до сучасних викликів.

3. З’ясовано, що політична пропаганда та мова ворожнечі в сучасному українському інформаційному просторі мають серйозний вплив на суспільство та знижує рівень довіри до політичних інститутів, формуючи негативне ставлення до провладної еліти.

Розглянуто методи пропаганди, які застосовуються для впливу на суспільство. Це дало змогу здійснити аналіз впливу пропагандистських зусиль на українське суспільство та виявити форми прояву маніпуляції в інформаційному просторі.

Аналіз методів маніпулювання в умовах російсько-української війни підтвержує застосування наративів з допомогою технік “наклеювання ярликів”, “блискучі узагальнення”, “пересмикування фактів”, “перенос”, “гра в простонародність” тощо, спрямованих на формування переконань, стереотипів та суспільних реакцій.

Ще однією проблемою в контексті інформаційної війни є мова ворожнечі, що використовується для маніпулювання суспільством, формування стереотипів, а також формування ненависті до певних етнічних груп.

В рамках українсько-російської війни висвітлено систематичне використання стереотипів та мови ворожнечі з боку росії з метою маніпулювання громадською думкою, а також негативного ставлення до “агресора”. Наведені лексико-асоціативні приклади, які використовувалися для позначення українців, кримських татар та інших етнічних груп, свідчить про активне проведення інформаційної кампанії задля дестабілізації та дискредитації українського суспільства.

В процесі дослідження доведено, що пропаганда та мова ворожнечі сприяє поділу суспільства на ворожі табори, створюючи серйозні перешкоди для розвитку демократичної держави в цілому.

4. Обґрунтовуючи питання ролі медіа та соціальних мереж в інформаційному протистоянні, було встановлено, що вони можуть використовуватися як засоби дезінформації та пропаганди стороною, що веде активну агресію.

З’ясовано, що блокування російських веб-сайтів та соціальних мереж у травні 2017 року, згідно указу Президента України Петра Порошенка, значно вплинуло на український інтернет-простір. Напередодні введення цих обмежень такі платформи, як “В контакте”, “Mail.ru”, “Яндекс” та “Одноклассники”, користувалися великою популярністю серед українських користувачів.

Ці обмеження були спрямовані на зменшення впливу російських медіа на українське суспільство через їхню можливу пропагандистську політику. Варто відзначити, що заборона доступу до цих російських медійних та соціальних каналів сприяла зменшенню їхнього впливу на українських користувачів, зокрема зменшилася кількість споживання інформації з потенційно прихованих пропагандистських джерел.

Вплив соціальних мереж та медіа простежується через їх складові. Так було досліджено “ботоферми”, що підкреслюють актуальність та необхідність обмежень на користування російськими медіа та веб-сайтами. Вони користуються спеціалізованим програмним забезпеченням для

автоматизації діяльності в соціальних мережах, що робило їхню діяльність прихованою.

Було розглянуто ще один відомий інструмент інформаційного впливу – медіа-віруси. Одним із прикладів медіа-віруса був проєкт “Русская весна”, що спрямований на формування позитивного образу росії та легітимізації російсько-української війни. Варто зауважити, що вплив даного проєкту був значний, особливо в контексті формування думок українського суспільства.

Таким чином, в умовах війни медіа та соціальні мережі відіграють вирішальну роль у мобілізації населення, піднятті морального духу та підтримці національної ідентичності. Однак, вони також можуть використовуватися ворогом для психологічних операцій, спрямованих на деморалізацію, дискредитацію влади та розкол суспільства.

5. Аналізуючи прийоми захисту інформаційного простору України через призму впливу громадянського суспільства, можна відзначити, що роль суспільства в даному процесі є вагомою. Інститути громадянського суспільства є визначальними у формуванні та реалізації стратегій захисту інформаційного простору.

У процесі дослідження було розкрито основні стратегії протидії дезінформації, запропоновані європейським агентством з протидії кремлівським дезінформаційним кампаніям та словацьким аналітичним центром the european values. Комплексний підхід до забезпечення інформаційної безпеки ґрунтується на розкритті дезінформаційних кампаній, підвищенні стійкості суспільства до пропаганди, пріоритеті щодо протидії дезінформації у формуванні зовнішньої та внутрішньої політики держави.

Вперше було простежено вплив громадянського суспільства через діяльність громадських організацій та проєктів, що мають на меті захистити інформаційне суспільство в умовах російсько-української війни. Таким чином, проаналізовано: програму “REALIES”, яка об’єднує 15 новаторів інформаційної сфери для боротьби з пропагандою та дезінформацією; Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві

культури та інформаційної політики, спрямований на фільтрацію інформації від викривлень та викидів; проєкт “MRIYA”, а також його бот у Telegram “StopRussiaChannel”, що збирають різні посилання на ворожі ресурси та інформацію про ворожу техніку ворога; проєкт “BRAMA”, який працює над захистом медіапростору від ворожих Telegram-каналів та незаконного контенту з боку російської федерації; проєкт “StopFake” має на меті аналіз та спростування фейкових новин та матеріалів, що транслюють російські ЗМІ; ініціатива “ФактЧек” є фактчек-ботом в Telegram для перевірки достовірної інформації з швидким інструментами пошуку.

Окремо виділено роль журналістської роботи у захисті інформаційного простору в Україні. Так було проаналізовано тематичні передачі “Антизомбі”, “Громадянська оборона” та проект “Кремль: брехуни при владі”. Основна мета їх діяльності полягає у проведенні детального аналізу та висвітленні пропагандистських матеріалів, що легітимізують російську владу та водночас дискредитують українських політичних представників.

Варто відзначити, що однією із ключових ініціатив, є впровадження чат-ботів у Telegram, які спрямовані на підтримку інформаційного простору та забезпечують ефективну комунікації з українським суспільством. Бот “Готовий до всього”, “Джгут 2.0. ”, “Турботник” “STOP Russian War”, “Народний месник” та інші забезпечують інформаційну безпеку громадян в умовах війни та надають оперативну інформацію на їх запити та потреби.

Здійснений аналіз впливу громадських ініціатив та проєктів на захист українського інформаційного простору та боротьби з медіа-вірусами, пропагандою, маніпуляціями дозволяє дійти висновків, що в подальшій перспективі важливо розширювати співпрацю з громадськими організаціями та активістами шляхом реалізації спільних проєктів та сприянню реалізації освітніх ініціатив для населення.

6. Аналіз інформаційної безпеки засвідчує, що в Україні існують значні проблеми у сфері забезпечення інформаційної безпеки в умовах російсько-української війни.

Поточний стан проблем вказує на недостатність захисних механізмів, слабкий рівень кібербезпеки та недоліки у захисті важливої інформації становлять серйозні загрози для національної безпеки України. В умовах повномасштабного військового конфлікту з росією, інформаційна безпека стає пріоритетною сферою для забезпечення стабільності та безпеки держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ І ЛІТЕРАТУРИ

1. Антизомбі. *Liveam.tv*. URL: https://liveam.tv/uk/antizombi-ictv.html (дата звернення: 12.05.2024).

2. Вітюк Н. Особливості дискурсу політичної пропаганди в умовах інформаційно-психологічної війни. Збірник наукових праць: психологія. 2019. Вип. 24. С. 29-38. URL:https://journals.pnu.edu.ua/index.php/psp/article/view/3249/3686

3. Волович В.І Соціологія : короткий енциклопедичний словник / За ред. В.І. Воловича; Соціологічна асоціація України. Київ : Український центр духовної культури, 1998. 736 с.

4. Втрачені можливості: українці надають більшу перевагу розважальним соцмережам, ніж професійному LinkedIn | GlobalLogic Ukraine. *GlobalLogic Ukraine*. URL: https://www.globallogic.com/ua/about/news/social-networks-and-opportunitites/ (дата звернення: 12.05.2024).

5. В Україні створили фактчек-бот, який допомагає розпізнавати фейки. *Сихів Media*. URL: https://sykhiv.media/v-ukrayini-stvoryly-faktchek-bot-yakyj-dopomagaye-rozpiznavaty-fejky/ (дата звернення: 12.05.2024).

6. Даценко А. Ю. Боротьба з російською дезінформацією як напрям захисту інформаційного простору України в умовах «гібридної війни». Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.- практ. конф. (Київ, 30 березня 2018 р.). Київ: Нац. акад. СБУ, 2018. С. 348-350.

7. Денисенко О., Приступа К. Соціальний проєкт BRAMA: як протидіяти фейкам та пропаганді. *Суспільне Чернігів*. URL: https://suspilne.media/chernihiv/694806-socialnij-proekt-brama-ak-protidiati-fejkam-ta-propagandi/.

8. Дмитренко М. Проблеми інформаційної безпеки України. *Український науковий журнал "ОСВІТА РЕГІОНУ"*. Т. 2. № 2012. С. 178. URL: https://social-science.uu.edu.ua/article/807.

9. Дубас О. Особливості політичного маніпулювання в інформаційному просторі України. Сучасна українська політика. Політики і політологи про неї. 2009. Вип. 18. С. 231-239.

10. Дячков Д.В. Формування моделі політики інформаційної безпеки на основі концепцій «глибинного захисту». Підприємництво і торгівля : збірник наукових праць. Львів : Видавництво Львівського торговельно-економічного університету. 2019. Вип. 25. С. 116–121. URL: 2522-1256-2019-25-17.pdf (lute.lviv.ua)

11. Е-урядування – ключ до реформ в Україні. Урядовий портал. Єдиний веб-портал органів виконавчої влади України. URL: https://www.kmu.gov.ua/news/e-uryaduvannya-klyuch-do-reform-v-ukrayini

12. Згуровський, М. Проблеми інформаційної безпеки в Україні, шляхи їх вирішення. 2000. URL: https://ela.kpi.ua/handle/123456789/15949

13. Зміст пропаганди на сучасному етапі. Глобальна організація союзницького лідерства. URL: https://goal-int.org/zmist-propagandi-na-suchasnomu-etapi/ (дата звернення: 17.05.2024).

14. Ільніцька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*. 2016. Vol. 2, No. 1. С. 27–32. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf.

15. Інформаційна безпека: сучасний стан, проблеми та перспективи: Матеріали І науково-практичної конференції. 20 вересня 2019 р., м. Київ. Упоряд. : В. М. Фурашев, С. Ю. Петряєв. Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2019. 124 с. URL: https://ippi.org.ua/sites/default/files/maket.pdf (дата звернення 01.05.2024)

16. ІПС ЛІГА:ЗАКОН - система пошуку, аналізу та моніторингу нормативно-правової бази. *Đ† Đ½Ñ„ Đ¾Ñ€ Đ¼Đ°Ñ† Ñ– Đ¹Đ½Đ¾-Đ¿Ñ€ Đ°Đ²Đ¾Đ²Đ° Ñ•Đ¸Ñ•Ñ‚ĐµĐ¼Đ° LIGA:ZAKON*. URL:

https://ips.ligazakon.net/document/JG3TH00A?an=5&scop=146&fcop=201 (дата звернення: 12.05.2024).

17. Ісакова Т. О. Мова ворожнечі як проблема українського інформаційного простору. Стратегічні пріоритети. 2016. № 4 (41). С. 90–97. URL: https://ippi.org.ua/sites/default/files/isakova.pdf

18. Історія про «розіп'ятого хлопчика» у Слов'янську: шості роковини найганебнішого фейка російської пропаганди. URL: https://slavinfo.dn.ua/novosti/novosti-slavyanska/istoriya-pro-rozip-yatogo-khlopchika-u-slov-yansku-shosti-rokovini-najganebnishogo-fejka-rosijskoji-propagandi (дата звернення: 12.05.2024).

19. Карпчук Н. Медіа як невоєнний метод впливу в гібридній війні. Міжнародні відносини, суспільні комунікації та регіональні студії. 2018. № 2. С. 41–49. URL:. https://relint.vnu.edu.ua/index.php/relint/article/view/70/64

20. Кельм Н., Дукач Ю. Гумор і новини. Як російська пропаганда просочується крізь тікток. *Texty.org.ua - статті та журналістика даних для людей – Тексти.org.ua*. URL: https://texty.org.ua/articles/111303/tiktok-hashtags-net/ (дата звернення: 12.05.2024).

21. Кобко Є.В. Інформаційна безпека в системі національної безпеки: сучасність і перспективи. National law journal: teory and practice. 2019. March. С. 46–50.

22. Козиряцька С. А. Дискурсні практики медіа-сфери Росії: синтез двох ідеологій чи розмивання орієнтирів. Наукові праці Кам'янець-Подільського національного університету імені Івана Огієнка. Філологічні науки. 2016. Вип. 42. 239-244 С. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Npkpnu_fil_2016_42_59

23. Косогов О. М. Сірик А. О. Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на Сході України. *Системи озброєння і військова техніка*. 2017. 1. С.38-41.

24. Косогов О.М., Сірик А.О. Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на Сході України. *Системи озброєння і військова техні*ка. 2017. С. 38-41. URL: http://nbuv.gov.ua/UJRN/soivt_2017_1_7

25. Котеньова І. Ю., Яковець А. В. Медіа як інструмент ведення інформаційної війни у міжнародних конфліктах. *International scientific innovations in human life* : International scientific and practical conference, м. Manchester. Manchester, 2022. С. 607–623.

26. Курбан О. В. Інформаційне супроводження російської гібридної агресії в Донбасі (2014-2016). *Бібліотекознавство. Документознавство. Інформологія*. 2017. №2. С. 66-73.

27. Курбан С. О. Сучасні інформаційні війни у мережевому он-лайн просторі: навчальний посібник. Покажчик змісту. *Інтегровані комунікації*, 2016. № 2. С. 109-110. URL: https://mil.knu.ua/files/222_1044284240.pdf

28. Курси з медіаграмотності та цифрових навичок | EdEra. *EdEra*. URL: https://ed-era.com/course/media-literacy/ (дата звернення: 12.05.2024).

29. Львова, О. Л. Мова ворожнечі: теоретико-правовий аналіз поняття. *Правова держава*. 2018. Вип. 29. С.71-79. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/559991.pd

30. Маркітантов В., Рибщун О., Віннічук О.В. Російська гібридна війна: від доктрини до тактики : навчальний посібник. Вид. 2-ге, перероб. і доп. Кам'янець-Подільський : Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. 248 с.

31. Мельник М.О. Аналіз побудови моделі політики інформаційної безпеки підприємства. Системи обробки інформації. 2017. Вип. 2(148). С. 126–128.

32. Мехед, Д. Б., et al. Аналіз загроз інформаційної безпеки в мережах стандарту IEEE 802.11. *Захист інформації*. 2015. № 4. С. 285-291. URL:http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21

REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Zi_2015_17_4_5

33. Міненко Є. Організаційно-правовий аналіз забезпечення інформаційної безпеки як фактор суспільно-політичної стабільності. *Scientific journal of the national pedagogical dragomanov university. series 22. political sciences and teaching methodology of socio-political disciplines*. 2023. Т. 22. № 33. С. 76–84. URL: https://doi.org/10.31392/udu-nc.series22.2023.33.08 (дата звернення: 12.05.2024).

34. Младьонова О. Інформаційна безпека як складова національної безпеки України. *Вісник ХНУ імені В. Н. Каразіна, серія «Питання політології»*. 2017. № 31. С. 87–92. URL: https://periodicals.karazin.ua/politology/article/view/9596/9109.

35. Мужанова, Т. М. Інформаційна безпека держави. Навчальний посібник. Київ: Державний університет телекомунікацій. 2019. URL: https://nubip.edu.ua/sites/default/files/u34/posibnik_ibd_muzhanova_2019.pdf

36. Ніщименко, О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право*. 2016. № 1. С.17-23. URL: NP_2016_1.indb (unesco-socio.in.ua)

37. Новородовська Н.О., Вакулич В.М. Російська пропаганда агресії проти України (2014-2021 рр.). *Український інформаційний простір.* Київ, 2023. №1(11). С. 119-132. https://www.researchgate.net/publication/372016138_Rosijska_propaganda_agresii_proti_Ukraini_2014-2021_rr

38. Онкович А. Соцмережа Фейсбук та захист українського інформаційного простору в умовах російсько-українського конфлікту. *Український інформаційний простір*. 2020. № 1(5). С. 233–242. URL: https://doi.org/10.31866/2616-7948.1(5).2020.206131 (дата звернення: 12.05.2024).

39. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України. *Політичний менеджмент*. 2008. ДЕ СТОРІНКИ АБО ПОСИЛАННЯ

40. Панченко О.А., Антонов В.Г., Малєєва А.М. Державне управління інформаційною безпекою як запорука особистісного благополуччя. Вчені записки ТНУ імені В.І. Вернадського. Серія «Державне управління». Том 31 (70). No 4. 2020.https://www.pubadm.vernadskyjournals.in.ua/journals/2020/4_2020/16.pdf

41. Панченко О. Інформаційна складова національної безпеки. *Вісник Національної академії Державної прикордонної служби України. Серія: державне управління*. 2020. № 3. URL: https://doi.org/10.32453/governance.vi3.296 (дата звернення: 12.05.2024).

42. Панченко О. А. Види та складові інформаційної безпеки. URL: https://www.inter-nauka.com/uploads/public/15861858673617.pdf

43. Паш Б.В. Складові інформаційної безпеки держави: постановка питання. Закарпатські правові читання. 2017. Том 1. С. 509-512.

44. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал* 2009. № 5. С.122-134. URL:http://www.justinian.com.ua/article.php?id=3222 (дата звернення 10.04.2022)

45. Петручок Ю. Пропаганда як метод інформаційної війни Російської Федерації проти України. Природничі та гуманітарні науки. Актуальні питання : збірник тез Міжнародної студентської науково-технічної конференції. Том 2. Тернопіль : ТНТУ, 2018. С. 183–184.

46. Попереджають про ризик діпфейків із Зеленським. *The Village Україна*. URL: https://www.village.com.ua/village/business/business-question/323775-oles-petriv-reface-deep-fake-machine-learning-videos-2022 (дата звернення: 13.05.2024).

47. Почепцов Г. Інформаційна війна як інтелектуальна війна. URL: URL: https://ms.detector.media/manipulyatsii/post/5380/2012-12-16-informatsiyna-viyna-yak-intelektualna-viyna/

48. Правове забезпечення державної інформаційної політики. URL: https://minjust.gov.ua/m/str_22116 (дата звернення 16.04.2022)

49. Презентовано Центр стратегічних комунікацій та інформаційної безпеки. *Урядовий портал. Єдиний веб-портал органів виконавчої влади України*. URL: https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki.

50. Президент України : Конституція України Розд. V. URL: https://www.president.gov.ua/ua/documents/constitution/konstituciya-ukrayini-rozdil-v (дата звернення: 12.05.2024).

51. Прищепа Г. «Мова ненависті» як лінгвістичний маркер «гібридної війни». Психолінгвістика. Психолингвистика. Psycholinguistics. 2017. Вип. 22 (2). С. 98–112.

52. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 12.05.2024).

53. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 12.05.2024).

54. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 12.05.2024).

55. Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України : Указ Президента України від 22.01.2002 р. № 63/2002 : станом на 18 черв. 2009 р. URL: https://zakon.rada.gov.ua/laws/show/63/2002#Text (дата звернення: 13.05.2024).

56. Про нас. *StopFake*. URL: https://www.stopfake.org/uk/pro-nas/ (дата звернення: 12.05.2024).

57. Про Національну програму інформатизації : Закон України від 01.12.2022 р. № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення: 12.05.2024).

58. 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 р. № 449/2014. URL: https://zakon.rada.gov.ua/laws/show/449/2014#Text (дата звернення: 13.05.2024).

59. Розділ 7. нормативно-правове регулювання інформаційної безпеки України. *TextBook*. URL: https://textbook.com.ua/politologiya/1473452012/s-45?page=1 (дата звернення: 12.05.2024).

60. АВТОР Скільки росія витрачає на пропаганду?. *Фільтр. Національний проєкт з медіаграмотності*. URL: https://filter.mkip.gov.ua/skilky-rosiya-vytrachaye-na-propagandu/.

61. Скочиляс-Павлів О. Сучасні загрози інформаційній безпеці України в умовах правового режиму воєнного стану. *Юридичний науковий електронний журнал*. 2023. № 9. С. 263-266. URL: http://lsej.org.ua/9_2023/65.pdf.

62. Степко О. Аналіз головних складових інформаційної безпеки держави. *Науковий вісник Інституту міжнародних відносин НАУ*. 2013. Т. 1, № 3. С. 90–99. URL: https://jrnl.nau.edu.ua/index.php/IMV/article/view/3214.

63. Стратегія інформаційної безпеки: указ президента України від 28 грудня 2021 року№ 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069

64. Стратегія національної безпеки України: інформаційна захищеність серед основних пріоритетів - Центр демократії та верховенства

права. *Центр демократії та верховенства права*. URL: https://cedem.org.ua/news/strategiya-natsionalnoyi-bezpeky/ (дата звернення: 12.05.2024).

65. Стратегія національної безпеки України**:** Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037

66. Захарченко Т. «Мова ворожнечі» як технологія ведення гібридної війни рф проти України. Медіафорум : аналітика, прогнози, інформаційний менеджмент : зб. наук. праць. Чернівці : Чернівецький нац. ун-т, 2019. Том 7. 322 с. URL:https://journals.chnu.edu.ua/mediaforum/article/view/153/150

67. Трапезон О.Г. Гумен Т.Ф. Трапезон К.О. Граб В.А. Золотарева Н.С. Моделі безпеки в інформаційних системах. Київ: WORLD SCIENCE. Page 2. ISSN 2413-1032. № 12(16), Vol.1, December 2016. 22-24 с. URL: https://cyberleninka.ru/article/n/modeli-bezpeki-v-informatsiynih-sistemah.pdf

68. Турчак А. (2019). Основні складові інформаційної безпеки держави. Аспекти публічного управління. 7(5). С. 44-56. URL: https://core.ac.uk/download/pdf/233892903.pdf

69. Українська бібліотечна енциклопедія. *Українська бібліотечна енциклопедія*. URL: https://ube.nlu.org.ua/article/Інформація (дата звернення: 12.05.2024).

70. Українська правда. В Україні ліквідували мільйонну ботоферму “Євросолідарності” – джерело. *Українська правда*. URL: https://www.pravda.com.ua/news/2022/08/2/7361495/ (дата звернення: 12.05.2024).

71. Фейки, за допомогою яких Росія намагається звинуватити Україну в теракті у «Крокусі». *StopFake*. URL: https://www.stopfake.org/uk/fejki-za-dopomogoyu-yakih-rosiya-namagayetsya-zvinuvatiti-ukrayinu-v-terakti-u-krokusi/ (дата звернення: 12.05.2024).

72. Цатурян М., Лопатина И. Контактний бій: українцям заборонили доступ до російських

соцмереж, телеканалів та сайтів. *РБК-Украина*. URL: https://daily.rbc.ua/ukr/show/ukraintsam-zapretili-dostup-rossiyskim-sotssetyam-1494946023.html (дата звернення: 12.05.2024).

73. ЧМИР Я. Сучасні проблеми інформаційної безпеки України та перспективні напрями їх вирішення. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2022. 2(62) (Жовтень). С.149-154. URL: https://journals.maup.com.ua/index.php/political/article/view/2153/2650

74. Чорна О. Наталія Лигачова: Необхідно зробити єдиний марафон якісних ЗМІ. *detector.media*. URL: https://detector.media/infospace/article/218017/2023-10-12-nataliya-lygachova-neobkhidno-zrobyty-iedynyy-marafon-yakisnykh-zmi/ (дата звернення: 12.05.2024).

75. Чукут С. А. Клименко І. В. Линьов К. О. Електронний уряд: науково-практичний довідник. *URL: https://ktpu. kpi. ua/wpcontent/uploads/2016/02/Elektronnij-uryad_nauk_prakdovidnik_CHukut_Linov_Klimenko. pdf (дата звернення: 28.04. 2021).*

76. Шпилик С. Інформаційна війна, пропаганда та PR: такі схожі й такі різні... *Галицький економічний вісник*. 2014. № 4 (47). С. 178–188.

77. Що змінить національна програма інформатизації? Закон підписано | FEMIDA.UA. *FEMIDA.UA*. URL: https://femida.ua/novyny/shho-zminyt-natsionalna-programa-informatyzatsiyi-zakon-pidpysano/#:~:text=Що%20змінить%20Національна%20програма%20інформатизації?%20Закон%20підписано (дата звернення: 13.05.2024).

78. Команда ГО «Детектор медіа» запустила інтернет-видання «Детектор медіа». URL: https://detector.media/production/article/112678/2016-02-09-komanda-go-detektor-media-zapustyla-internet-vydannya-detektor-media/ (дата звернення: 12.05.2024).

79. Doctrine of information security of Ukraine. URL: https://rm.coe.int/doctrine-of-information-security-of-ukraine-developments-in-member-sta/168073e052

80. ms.detector.media. MediaSapiens. *ms.detector.media*. URL: https://ms.detector.media/ (дата звернення: 12.05.2024). – ЩО САМЕ ЗВІДСИ ВЗЯТО???

81. REALIES – програма підтримки з протидії дезінформації - Media League. *Media League*. URL: https://medialeague.com.ua/realies-programa-pidtrymky-z-protydiyi-dezinformacziyi/ (дата звернення: 12.05.2024).

82. Starlight Media. Команди «Антизомбі» та «Громадянської оборони» створили документальний спецпроект «Кремль: брехуни при владі». *CASES*. URL: https://cases.media/en/news/komandi-antizombi-ta-gromadyanskoyi-oboroni-stvorili-dokumentalnii-specproekt-kreml-brekhuni-pri-vladi (дата звернення: 12.05.2024).

83. Спам, реклама, фейки. Як російська пропаганда атакує українців у соцмережах. *Ukrinform.* 2024. (12 червня). URL: https://www.ukrinform.ua/rubric-factcheck/3816655-spam-reklama-fejki-ak-rosijska-propaganda-atakue-ukrainciv-u-socmerezah.html (дата звернення: 12.05.2024).

84. Vogue.ua. 11 корисних чат-ботів у Telegram у період війни. *Vogue UA - жіночий журнал про моду, красу і стиль. Vogue Ukraine - fashion, beauty, arts, society and living*. URL: https://vogue.ua/article/culture/lifestyle/11-korisnih-chat-botiv-u-telegram-u-period-viyni-47862.html (дата звернення: 12.05.2024)