Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему: «Інформаційна безпека України в контексті російсько-української війни»

Виконав здобувач вищої освіти 6-го курсу,
групи УМІБ-61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Охріменко Ілля Геннадійович
(прізвище, ім'я, по-батькові)

Керівник:
д. держ. упр., проф. кафедри міжнародних відносин
д.держ.упр., проф. Солових Віталій Павлович
(науковий ступінь, вчене звання, прізвище, ім'я, по-батькові)

Рецензент:
д.держ.упр., проф. Крюков Олексій ігорович
(науковий ступінь, вчене звання, прізвище, ім'я, побатькові)

ХАРКІВ – 2024 рік

ЗМІСТ

ВСТУП

Актуальність теми. Збройна агресія РФ проти України, починаючи з 2014 року супроводжувалася не тільки військовою складовою, але й активним веденням інформаційно-гібридної війни, яка значно посилилася з початком повномасштабного вторгнення у 2022 році. Держава-агресор веде активну інформаційну війну, використовуючи різноманітні інструменти, включаючи дезінформацію, маніпуляцію свідомістю, фейки, пропагандистські наративи та кібернетичні атаки, що ставить під загрозу не лише інформаційний простір України, а й усю систему національної безпеки в цілому. В умовах посилення інформаційних загроз виникає нагальна необхідність удосконалення системи інформаційної безпеки держави, що включає в себе як стратегічні, так і оперативні заходи для ефективного протистояння агресивним інформаційним кампаніям з боку кремлівського режиму. Дослідження цієї теми є важливим для розробки комплексних механізмів захисту, що сприятимуть стабільності та розвитку системи інформаційної безпеки України в рамках збройного конфлікту з росією.

Ступінь вивченості теми. Питанням визначення терміну «інформаційна безпека» займаються такі дослідники, як В. С. Цимбалюк, А. В. Бабінська, Л. О. Кочубей, І. Панарін, серед зарубіжних - Г. Одерман. Сутність міжнародної інформаційної безпеки досліджують: П. Д. Біленчук, О. О. Грицун. Аналіз проблеми інформаційної війни проводили: Г. Е. Екклз, Г. Г. Саммерс. Хоча Україна зробила значний прогрес у розвитку інформаційної безпеки в умовах війни, тема все ще потребує подальших досліджень і більш комплексного підходу в наукових та практичних дослідженнях. Проблеми, пов'язані з новітніми технологіями та змінними умовами війни, вимагають гнучкості, інноваційних підходів і постійного моніторингу ситуації.

. **Мета дослідження:** з’ясувати особливості функціонування системи інформаційної безпеки України в контексті російсько-української війни.

Під час проведення дослідження було визначено такі **завдання**:

– Визначити основні підходи до поняття та загальну характеристику інформаційної безпеки;

– Розглянути інформаційну безпеку як складову архітектури міжнародної безпеки;

– З’ясувати підходи забезпечення міжнародної інформаційної безпеки;

– Визначити складові елементи системи інформаційної безпеки України;

– З’ясувати особливості функціонування системи інформаційної безпеки України під час збройної агресії РФ у 2014 році та з початком повномасштабного вторгнення;

– Розглянути можливі напрямки забезпечення інформаційної безпеки України в контексті російсько-української війни.

Об'єктом дослідження є інформаційна безпека держави.

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

Теоретико-методологічна база дослідження. У процесі написання кваліфікаційної роботи були застосовані такі методи дослідження: метод узагальнення, за допомогою якого був визначений термін «інформаційна безпека» та «міжнародна інформаційна безпека». Використовуючи системний метод, в роботі було виділено основні складові елементи системи інформаційної безпеки України. За допомогою методу порівняння вдалося детально розглянути концепції та підходи щодо забезпечення інформаційної безпеки як складової архітектури міжнародної безпеки державами та міжнародними організаціями. Метод аналізу та синтезу, за допомогою яких було визначено напрямки забезпечення інформаційної безпеки України в контексті інформаційної агресії з боку росії.

Інформаційна база дослідження дипломної роботи включає в себе наступні джерела та матеріали: наукові статті, підручники, закони та нормативно-правові акти.

Практичне значення отриманих результатів. Отримані результати дослідження можуть значно покращити стан інформаційної безпеки України,

мінімізувати вплив дезінформації на громадянське суспільство. Покращення рівня медіаграмотності українського суспільства як одного із напрямків забезпечення інформаційної безпеки дозволить громадянам критично оцінювати інформацію, розпізнавати маніпуляції та фейки, що є важливим для протидії інформаційним атакам з боку держави-агресора та збереження стабільності в суспільстві. Результати дослідження сприятимуть створенню більш стійкої та захищеної системи інформаційної безпеки держави, що є критично важливим для забезпечення національної безпеки України в умовах російсько-української війни.

Апробація результатів дослідження здійснена на Всеукраїнському науково-практичному круглому столі «Стратегічні напрями зовнішньої політики та дипломатії країн світу» 21 листопада 2024 року (м. Харків). Тема тез доповіді: «Інформаційна безпека України під час повномасштабного вторгнення РФ».

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, який налічує 70 найменувань. Загальний обсяг роботи становить 74 сторінок, з яких основного тексту - 66 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК СКЛАДОВОЇ АРХІТЕКТУРИ МІЖНАРОДНОЇ БЕЗПЕКИ

1.1. Поняття та загальна характеристика інформаційної безпеки

Сьогодні інформаційні технології перебувають на етапі стрімкого розвитку, який визначає не лише економічні, але й соціальні, культурні та політичні аспекти життя. Завдяки розвитку Інтернету, мобільних технологій і штучного інтелекту, інформація стала доступною для мільйонів людей у всьому світі в реальному часі. Цей стрімкий прогрес створює нові перспективи для розвитку бізнесу, освіти та комунікацій, водночас ставлячи нові виклики, такі як інформаційна безпеки, кібербезпека, етика в даних та інформаційна нерівність.

У сучасному світі інформаційна безпека набуває вирішального значення, оскільки зростання цифрових технологій призводить до збільшення ризиків, пов'язаних з витоками даних, кіберзлочинністю та кібератаками. В умовах глобалізації та інтеграції інформаційних систем забезпечення конфіденційності, цілісності та доступності даних стає пріоритетом не тільки для бізнесу, а й для державних органів та приватних осіб. Атаки на інформаційні системи можуть мати серйозні наслідки, включаючи фінансові втрати, порушення репутації та навіть загрози національній безпеці. Тому забезпечення інформаційної безпеки є критично важливим для стабільного розвитку суспільства, зміцнюючи довіру до цифрових технологій та інновацій.

Категорія «інформаційна безпека» виникла з необхідності забезпечення інформаційних комунікацій та усвідомлення рівня загроз для інформаційного обміну між учасниками суспільства. Це поняття охоплює різноманітні практичні аспекти, що залежать від того, яке значення вкладається в термін «інформація», оскільки наразі немає єдиного загальноприйнятого визначення цього терміну, яке можна було б застосовувати в різних контекстах. В загальному розумінні, інформаційна безпека повинна гарантувати основні характеристики інформації, такі як конфіденційність (стан, коли доступ до

інформації мають тільки уповноважені особи), цілісність (запобігання несанкціонованим змінам інформації), доступність (уникнення приховування інформації від користувачів, які мають на неї право доступу). Також забезпечуються інші характеристики інформації, як-от неспростовність (можливість підтвердити, що дія або подія мали місце, і що автор є тим, ким він себе заявляє, а події не були змінені після їх здійснення), достовірність (ступінь точності та об'єктивності інформації, що відображає реальні події та факти), автентичність (гарантія того, що суб’єкт або ресурс є справжніми і відповідають заявленим характеристикам).

Інформаційна безпека (англ. Information Security) - це стан захищеності інформаційного простору (інформації) окремої особи, підприємства, суспільства або держави, за якого комплекс спеціальних заходів запобігає виникненню негативних наслідків впливу на інформаційне середовище та його складові внаслідок умисних, несанкціонованих чи випадкових маніпуляцій з інформацією [1; 2].

На думку В. С. Цимбалюка, А. В. Бабінської, під інформаційною безпекою України слід розуміти стан захищеності національних інформаційних ресурсів, технологій та систем, що забезпечує їх цілісність, конфіденційність і доступність, а також дає змогу ефективно протидіяти зовнішнім і внутрішнім загрозам, зокрема інформаційним атакам, маніпуляціям, пропаганді та дезінформації, які можуть загрожувати національній безпеці, суверенітету і стабільності держави [3].

Л. О. Кочубей визначає інформаційну безпеку як стан захищеності інформаційних ресурсів, технологій та інфраструктури, що забезпечує їх цілісність, конфіденційність і доступність, а також гарантує захист від впливу зовнішніх та внутрішніх загроз, що можуть дестабілізувати функціонування суспільства, держави та окремої особистості [4].

І. Панарін визначає інформаційну безпеку як захист інформації, інформаційних ресурсів та інфраструктури від несанкціонованого доступу, використання або пошкодження, а також від впливу на свідомість людей, що

може призвести до дестабілізації політичної ситуації та національної безпеки [5].

Аналізуючи вищезазначені підходи до поняття інформаційної безпеки, варто наголосити, що термін «інформаційна безпека» можна розглядати як стан захищеності інформаційного середовища, що забезпечує належний рівень захисту інформації на різних рівнях: особи, підприємства, суспільства або держави. Вона включає в себе комплекс заходів, які запобігають виникненню негативних наслідків, спричинених впливом несанкціонованих, умисних або неумисних маніпуляцій з інформацією. Інформаційна безпека має на меті захистити життєво важливі інтереси, інформаційну інфраструктуру та можливості розвитку суб'єктів (держава, суспільство, особистість), унеможливлюючи деструктивні інформаційні впливи, що можуть призвести до негативних наслідків на шляху стійкого розвитку.

Об'єкти інформаційної безпеки - це інформаційні ресурси, системи та технології, які потребують захисту. Це можуть бути дані, програмне забезпечення, інформаційні мережі, обладнання, а також самі процеси обробки та зберігання інформації.

Суб'єкти інформаційної безпеки - це органи державної влади, підприємства, організації та фізичні особи, які забезпечують захист інформаційних ресурсів. Вони включають державні структури (включаючи спеціальні органи), бізнес-сектор, постачальників інформаційних послуг, а також користувачів, які відповідають за дотримання стандартів безпеки та захист своїх даних.

Інформаційна безпека особистості характеризується захистом її приватної інформації, прав та цифрової ідентичності від несанкціонованого доступу, використання або маніпуляцій. Вона включає управління особистими даними, безпеку в онлайн-середовищі, захист від кіберзлочинності та дезінформації, а також здатність зберігати контроль над власною інформацією в умовах швидкого розвитку технологій та зростання кіберзагроз.

Інформаційна безпека держави характеризується здатністю ефективно захищати національні інформаційні ресурси, системи та інфраструктуру від внутрішніх і зовнішніх загроз. Вона включає забезпечення конфіденційності, цілісності та доступності інформації, а також здатність протидіяти кіберзлочинності, дезінформації та маніпуляціям. Це також передбачає розвиток надійних механізмів реагування на інциденти, адаптацію до нових технологічних викликів і міжнародну співпрацю в питаннях кібербезпеки.

Концепція інформаційної безпеки держави є системою знань та відомостей, що стосуються інформаційної безпеки держави та шляхів її забезпечення. Вона включає:

– системну класифікацію факторів і загроз, які можуть дестабілізувати безпеку особистості, суспільства та держави;

– обґрунтування основних положень організації забезпечення інформаційної безпеки;

– розробку пропозицій щодо способів і форм забезпечення безпеки [6].

Забезпечення інформаційної безпеки - це комплекс заходів, стратегій та процедур, спрямованих на захист інформаційних ресурсів, систем і технологій від загроз, що можуть порушити їхню конфіденційність, цілісність і доступність. Це включає в себе виявлення, оцінку та управління ризиками, захист від кіберзагроз, зловживань і технічних збоїв, а також забезпечення сталості та безперервності функціонування інформаційних систем у будь-яких умовах. Це включає в себе запобігання кіберзлочинності, захист від кіберзагроз, маніпуляцій, дезінформації та зловмисних атак. Основними аспектами є забезпечення конфіденційності, цілісності та доступності інформації, а також захист особистих даних і прав людини в цифровому просторі. Забезпечення інформаційної безпеки також вимагає співпраці між державами, бізнесом і громадськістю для створення ефективних стандартів і систем захисту від новітніх загроз у цифровому середовищі.

Ці заходи здійснюються державними органами, а також громадянами, суспільними організаціями, що мають відповідні повноваження згідно з

законодавством. У забезпеченні інформаційної безпеки держави повинні бути враховані такі принципи:

– активна співпраця з іншими державами та міжнародними організаціями для боротьби з глобальними інформаційними загрозами;

– чітке визначення законодавчої та нормативної бази для захисту інформаційних ресурсів;

– інтеграція національних і міжнародних систем безпеки.

До специфічних принципів інформаційної безпеки відносяться:

– превентивний характер заходів, спрямованих на запобігання загрозам до того, як вони можуть реалізуватися;

– адекватна інформованість об'єктів безпеки, включаючи міжнародні аспекти [7].

Основними принципами інформаційної безпеки є конфіденційність, цілісність і доступність. Кожен елемент програми інформаційної безпеки має бути розроблений таким чином, щоб реалізувати один або кілька з цих принципів. Разом ці принципи утворюють «Тріаду ЦРУ».

Конфіденційність: заходи конфіденційності спрямовані на запобігання несанкціонованому доступу до інформації. Основною метою є збереження інформації в таємниці та забезпечення доступу до неї лише для осіб, які мають відповідні права або потребують її для виконання своїх функцій.

Цілісність: цей принцип включає захист від несанкціонованих змін даних, таких як їх модифікація, видалення чи додавання. Гарантується, що інформація є точною, надійною і не може бути змінена зловмисно або випадково.

Доступність: принцип доступності забезпечує можливість своєчасного доступу до інформації та програмних систем, коли вони потрібні користувачам. Мета - забезпечити доступність технологічної інфраструктури, додатків і даних для організаційних процесів або для клієнтів організації [8].

Інформаційна безпека держави є надзвичайно важливим аспектом національної безпеки, оскільки в сучасному світі все більше зростає залежність від інформаційних технологій та цифрових комунікацій. Зростаючі загрози, такі

як кібератаки, шкідливе програмне забезпечення, витоки даних і дезінформація, ставлять під загрозу не лише державні інституції, але й приватний сектор, громадянське суспільство та критичну інфраструктуру. Актуальність цих викликів підкреслюється глобалізацією інформаційних мереж та активною діяльністю злочинних угруповань і держав-агресорів, які використовують інформаційні технології для здійснення агресії, підриву стабільності та маніпуляцій. У цьому разі слід зазначити, що формування ефективної системи захисту інформаційної безпеки є невідкладним завданням для забезпечення суверенітету та стратегічної стабільності держави.

Небезпечні інформаційні дії зазвичай поділяються на два основних види. Перший пов'язаний з втратою важливої інформації, що може знизити ефективність власної діяльності або, навпаки, посилити діяльність супротивника чи конкурента. Якщо такими діями порушується свідомість людей, то це може бути пов'язано з розголошенням державних таємниць, вербуванням агентів, а також спеціальними засобами для прослуховування, використанням детекторів брехні, медикаментозними, біологічними та хімічними впливами на психіку людини. Захист від такого роду інформаційних загроз здійснюють органи цензури, військова контррозвідка та інші суб'єкти, відповідальні за інформаційну безпеку. Коли ж джерелом загрози є технічні системи, це вже стосується технічної розвідки або шпигунства, зокрема прослуховування та перехоплення телефонних розмов, радіограм, сигналів комунікаційних систем, а також вторгнення в комп'ютерні мережі та бази даних. Другий вид інформаційних загроз полягає у впровадженні негативної або шкідливої інформації, яка не лише може призвести до помилкових рішень, але й спонукати до дій, які завдають шкоди і можуть призвести до катастрофи для суспільства. Захист від таких загроз здійснюють спеціалізовані структури, що займаються інформаційно-технічною боротьбою. Вони нейтралізують дії з дезінформації, зменшують маніпулювання громадською думкою і ліквідують наслідки комп'ютерних атак. Впровадження нових інформаційних технологій у

різні сфери життя, як і будь-які інші науково-технічні досягнення, не тільки забезпечує комфорт і прогрес, але також може нести потенційну небезпеку [9].

Зважаючи на зростаючі загрози у сфері інформаційної безпеки, таких як кібернапади, дезінформація, інформаційні війни та тероризм, важливо забезпечувати інформаційну безпеку в рамках міжнародної безпеки. Це вимагає співпраці між державами для створення спільних стандартів, механізмів захисту та обміну інформацією, а також для боротьби з транснаціональними кіберзагрозами. Кожна держава повинна розробляти власні стратегії захисту інформаційної інфраструктури, зміцнювати кібербезпеку, забезпечувати захист прав громадян на приватність та боротися з дезінформацією. Тільки через міжнародне співробітництво та національні зусилля можна ефективно протидіяти новітнім загрозам та зберігати стабільність і безпеку в глобальному інформаційному середовищі.

1.2. Інформаційна безпека як складова архітектури міжнародної безпеки

У сучасному світі, де технології й інформаційні системи займають центральне місце в соціальних, економічних та політичних процесах, питання забезпечення інформаційної безпеки стало однією з ключових складових архітектури міжнародної безпеки. Інформація є стратегічним ресурсом, який здатен суттєво впливати на функціонування держав, міжнародних організацій, корпорацій та громадян. Водночас з розвитком технологій зростають і ризики, пов’язані з інформаційними загрозами: кібератаки, кібертероризм, витік чутливої інформації, маніпуляції даними, пропаганда та інші форми інформаційної війни. Інформаційна безпека, що передбачає захист інформаційних ресурсів від несанкціонованого доступу, використання, модифікації або знищення, має важливе значення не лише для окремих країн, а й для глобальної стабільності. В умовах глобалізації та інтеграції інформаційних технологій, міжнародна співпраця у галузі захисту інформації

стає необхідною для ефективного реагування на нові виклики й загрози. Інформаційна безпека виступає важливою складовою архітектури міжнародної безпеки, впливаючи на всі сфери міжнародних відносин.

Інформаційна революція та розвиток новітніх технологій призводять до виникнення нових проблем, які потребують ефективної протидії. Зокрема, швидке поширення цифрових технологій та Інтернету створює сприятливі умови для кіберзлочинності, хакерських атак, крадіжки даних і шантажу. Також зростає загроза використання інформаційної зброї та дезінформації, що може дестабілізувати політичну ситуацію в країнах, посіяти паніку та маніпулювати громадською думкою. Інші проблеми включають захист персональних даних і приватності в умовах глобальної цифрової взаємодії, а також загрози з боку штучного інтелекту, який може бути використаний для маніпуляцій і навіть автоматизованих атак. Відсутність ефективних міжнародних стандартів і регулювань у цій сфері ускладнює боротьбу з новими загрозами, що потребує розробки нових механізмів і стратегій для забезпечення глобальної інформаційної безпеки.

Світова спільнота розробила низку міжнародних актів для боротьби з хакерськими атаками на державні інформаційні системи та з використанням інформаційної зброї. Ці акти спрямовані на протидію загрозам інформаційних війн і тероризму, що можуть призвести до серйозних конфліктів з руйнівними наслідками для національних безпек та глобальної стабільності. Такі міжнародні механізми включають угоди про кібербезпеку, співпрацю в рамках ООН, а також розробку стандартів для запобігання зловживанням в інформаційному просторі. Ці ініціативи сприяють захисту від цифрових атак, що можуть підривати економіку, дестабілізувати політичну ситуацію та загрожувати національним інтересам держав. Такими актами є:

– Конвенція про кіберзлочинність (2001 рік);

– Декларація ООН про міжнародну інформаційну безпеку (2003 рік);

– Резолюція ООН 57/239 (2003) "Інформаційна безпека в контексті міжнародної безпеки";

– Європейська конвенція про захист прав людини та кібербезпеку.

Міжнародну безпеку можна розглядати як політику, яка сприяє створенню ефективних гарантій миру як для окремих країн, так і для всього світового співтовариства. Визнання проблеми інформаційної безпеки на міжнародному рівні зумовлене такими чинниками глобалізації:

– У більшості індустріально розвинутих країн проводяться дослідження та розробки нових видів інформаційної зброї, що дозволяє здійснювати безпосередній контроль над інформаційними ресурсами потенційного супротивника та, у разі потреби, впливати на них.

– Змінилося розуміння доктрини інформаційної безпеки в цілому та позиції більшості країн світу, які усвідомили важливість інформаційних загроз і необхідність створення механізмів для контролю інформаційного протиборства [10].

Згідно з науковою позицією П. Д. Біленчука міжнародна інформаційна безпека - це стан захищеності інформаційного середовища суспільства та сукупність заходів різного характеру (економічного, політичного, юридичного), спрямованих на її підтримку [11].

Інформаційна безпека як концепція в міжнародних відносинах означає захист інформаційних ресурсів, технологій та інфраструктури від загроз, що можуть виникнути через кібернапади, дезінформацію, пропаганду, маніпуляції та інші форми інформаційних атак. Вона включає забезпечення цілісності, конфіденційності та доступності інформації, а також захист від зовнішніх і внутрішніх інформаційних впливів, які можуть дестабілізувати політичну, економічну чи соціальну ситуацію в країні. У міжнародному контексті інформаційна безпека охоплює такі аспекти, як співпраця між державами в боротьбі з кіберзлочинністю, захист прав людини на інформацію та свободу слова, а також протидія інформаційним маніпуляціям і пропаганді. Концепція інформаційної безпеки стала особливо актуальною в умовах глобалізації та швидкого розвитку цифрових технологій, коли інформація стала важливим

інструментом геополітичного впливу та механізмом забезпечення національної безпеки [12].

ООН визначає міжнародну інформаційну безпеку як стан, при якому інформаційні ресурси та комунікаційні технології використовуються безпечно, не загрожуючи міжнародному миру та стабільності. Це включає захист від кіберзагроз, боротьбу з кіберзлочинністю та забезпечення етики і прозорості в глобальному інформаційному середовищі через міжнародне співробітництво [13].

Враховуючи підходи до визначення поняття «міжнародна інформаційна безпека», варто наголосити, що це комплексний стан глобальних інформаційних відносин, який забезпечує захищеність інформаційного середовища на світовому рівні, підтримуючи стабільність міжнародної системи. Вона охоплює сукупність заходів різного характеру (економічних, політичних, юридичних, організаційних), спрямованих на попередження загроз, забезпечення безпеки держав і міжнародної спільноти в інформаційному просторі. Міжнародна інформаційна безпека передбачає створення умов для сталого розвитку держав і суспільств, а також захисту прав та інтересів осіб в інформаційній сфері, забезпечуючи при цьому недопущення порушень світової стабільності.

До основних принципів, що стосуються міжнародних інформаційних відносин та міжнародної інформаційної безпеки, відносяться:

– принцип суверенітету в інформаційній сфері - кожна держава має право на контроль та управління інформацією, яка циркулює на її території. Це включає в себе право на захист від зовнішніх інформаційних впливів, маніпуляцій і дезінформації, а також на регулювання медіа-простору;

– принцип не інтервенції - країни не повинні втручатися в інформаційні системи та медіапростір інших держав, зокрема через використання інформаційних технологій для впливу на політичну, економічну чи соціальну ситуацію в інших країнах. Це стосується як фізичних, так і кібернетичних атак на інформаційну інфраструктуру;

– принцип прозорості та доступу до інформації - міжнародна інформаційна безпека передбачає забезпечення прозорості в обміні інформацією між державами, а також доступ громадян до достовірної та перевіреної інформації. Це є основою для формування демократичних процесів і підвищення рівня медіаграмотності;

– принцип захисту від дезінформації та пропаганди - міжнародні відносини в інформаційній сфері повинні включати боротьбу з дезінформацією, фальшивими новинами та пропагандою, що можуть призводити до соціальної і політичної дестабілізації в країнах, особливо в умовах конфліктів або війни;

– принцип співпраці у сфері кібербезпеки – міжнародне співробітництво в галузі кібербезпеки є важливим елементом забезпечення глобальної інформаційної безпеки. Це включає обмін даними щодо кіберзагроз, спільну боротьбу з кіберзлочинністю та захист інформаційних систем від атак з боку держав і недержавних акторів;

– принцип захисту прав людини в інформаційній сфері – важливо забезпечити баланс між захистом національної безпеки та правами людини, зокрема правом на свободу слова та доступ до інформації. Обмеження свободи інформації не повинні порушувати основні права громадян, такі як право на приватність і свободу вираження думок [14].

Сучасні загрози та виклики міжнародній інформаційній безпеці мають глобальний характер та охоплюють широкий спектр проблем, від кібератак до інформаційних війн. З розвитком цифрових технологій і зростанням залежності від Інтернету, країни та міжнародні організації стикаються з новими формами кіберзагроз, такими як хакерські атаки, фішинг, крадіжка персональних даних. Водночас, інформаційні війни, зокрема пропаганда, дезінформація та маніпуляції громадською думкою, стали важливим інструментом в міждержавних конфліктах, що призводить до ескалації напруги на міжнародній арені. Сучасні виклики також охоплюють питання етики та законодавства в контексті інформаційної безпеки, захисту прав людини в онлайн-середовищі та гарантування конфіденційності даних.

Загрози інформаційній безпеці - це потенційні або реальні дії, події чи фактори, які можуть спричинити шкоду інформаційним ресурсам, системам або процесам, порушити їхню цілісність, конфіденційність або доступність, а також негативно вплинути на функціонування інформаційної інфраструктури. Ці загрози можуть бути результатом як навмисних дій (наприклад, кіберзлочинність, шкідливе програмне забезпечення), так і випадкових подій (помилки користувачів, технічні збої), а також природних чи техногенних катастроф.

Основні загрози інформаційній безпеці можна класифікувати на три групи:

– технічні загрози (хакерські атаки, віруси, шкідливе ПЗ, DDoS-атаки);

– людські загрози - помилки або зловмисні дії користувачів (фішинг, крадіжка паролів);

– природні загрози - стихійні лиха, катастрофи, які можуть пошкодити інформаційні системи [15].

Однією з головних загроз міжнародній інформаційній безпеці є інформаційна війна, оскільки вона має здатність дестабілізувати політичні, економічні та соціальні системи держав. Використання дезінформації, пропаганди, маніпуляцій у медіа-просторі, а також кібернападів на критичну інфраструктуру може серйозно підривати довіру до урядів, міжнародних організацій та міждержавних відносин. В умовах глобалізації та швидкого поширення інформації через цифрові канали, ефективна протидія таким загрозам стає надзвичайно складною задачею для міжнародної спільноти, що вимагає розробки нових механізмів захисту та координації на глобальному рівні.

Інформаційна війна - це операція, спрямована на отримання переваги в інформаційній сфері над супротивником. Вона передбачає контроль за власним інформаційним простором, захист доступу до власної інформації, а також отримання і використання інформації супротивника, руйнування його інформаційних систем і порушення інформаційних потоків. Хоча інформаційна

війна не є новим явищем, вона містить інноваційні елементи, що зумовлені технологічним розвитком, який забезпечує швидше і масштабніше поширення інформації [16; 17].

Метою інформаційної війни є створення сумнівів у супротивника. Через величезну кількість суперечливої інформації, фактів і аргументів, часто неприязно налаштованих один до одного, розмивається поняття об'єктивності, і пересічний споживач новин важко розрізняє, яка з версій є правдивою. Основне завдання інформаційної війни полягає в маніпулюванні масами для впровадження в суспільну та індивідуальну свідомість шкідливих ідеї і поглядів супротивника, дезорієнтації та дезінформації, послаблення переконань, залякування власного населення образом ворога та створення враження потужності своєї сторони для супротивника [18].

Можна виокремити наступні методи ведення інформаційної війни у сучасних міжнародних відносинах:

– Відволікання уваги. Це стратегія, спрямована на відведення уваги від важливих питань і міжнародних подій, а також на запобігання громадському інтересу до ключових тем, таких як охорона здоров'я чи економіка. Наприклад, замість обговорення політичних новин, увагу суспільства зосереджують на передвиборчих шоу, розважальних заходах чи народних гуляннях.

– Маніпулювання інформацією. В контексті інформаційної війни маніпулювання інформацією означає зміну даних з метою спотворення реальності для супротивника. Це може включати використання різноманітних технологій, таких як програмне забезпечення для редагування текстів, графіки, відео, аудіо та інших форм передачі інформації. Процес маніпулювання зазвичай включає створення або коригування даних вручну, щоб ті, хто контролює інформаційний процес, могли впливати на те, як виглядає картина подій для противника. Технології використовуються для прискорення фізичного процесу маніпуляції після визначення бажаного змісту.

– Психологічні інформаційні операції (ПІО) ПІО - це захисні та наступальні інформаційні заходи, які формують ментальні карти суспільної

свідомості в процесі прийняття рішень. Вони ґрунтуються на широкому спектрі методів соціального управління (соціальної інженерії), що полягають у подачі опоненту спеціально відібраної (підготовленої) інформації з метою впливу на нього для прийняття вигідних для нападника рішень. Ця діяльність ведеться, по-перше, в неавтономній (зовнішній) інформаційній системі, спрямованій на зовнішнє середовище, а по-друге, в автономній (внутрішній) інформаційній системі, спрямованій на внутрішнє суспільство [19; 20; 21].

Серед прикладів інформаційних війн у сучасних міжнародних відносинах можна виділити наступні:

– Інформаційна війна росії проти України. Інформаційна війна в Україні з боку росії - це латентна вербальна атака, адже не кожен реципієнт може зрозуміти, що на нього намагаються вплинути за допомогою пропаганди. Інструменти російської інформаційної війни є надзвичайно різноманітними і підбираються відповідно до конкретних стратегічних завдань. До класичних методів можна віднести ЗМІ, «фабрики тролів», «ботів», створення «фейків», а також використання текстів, відео, аудіо, зображень і мемів. Головною метою Кремля є дестабілізація України зсередини, формування уявлення, що Україна і українці нерозривно пов'язані з образом росії як євразійської держави.

– Інформаційна війна Китаю. Двостороння стратегія Китаю включає глобальну експансію своїх державних ЗМІ, таких як Сіньхуа та його мережа China Global Television Network (CGTN), а також посилення контролю над усіма китайськомовними ЗМІ по всьому світу (в тому числі практично в кожній європейській країні, де існують китайськомовні ЗМІ). Пекін також розширив своє більш витончене використання дезінформації на платформах соціальних мереж і покладається на все більш популярні соціальні медіа-платформи, такі як TikTok, WeChat та інші інструменти. Однією з глобальних цілей Пекіна є просування своєї моделі авторитаризму, заснованого на технологіях. Він також продовжуватиме вчитися у росії, яка навчає Китай більш витонченим стратегіям дезінформації.

– Інформаційна війна Ірану. Інформаційна війна, як частина когнітивної кампанії, є, як зазначалося, елементом у комплексі зусиль, що використовуються Іраном для досягнення своїх цілей, серед яких розширення бази впливу на Близькому Сході; підрив внутрішньої стійкості своїх супротивників, включаючи країни Перської затоки; посилення впливу своїх військових зусиль (наприклад, шляхом перебільшення їхніх успіхів); поліпшення власного іміджу та іміджу своєї регіональної політики. Крім того, інформаційна війна Ірану підтримує і доповнює його здатність експортувати свої ідеологічні, релігійні та культурні принципи, включаючи боротьбу із Заходом і підтримку «опору» [22; 23; 24].

Отже, з урахуванням зазначених загроз та викликів для міжнародної інформаційної безпеки, світова спільнота змушена розробляти нові механізми співпраці та встановлювати стандарти, які забезпечать ефективне протистояння загрозам у інформаційній сфері.

1.3. Теоретичні підходи щодо забезпечення міжнародної інформаційної безпеки

Міжнародна інформаційна безпека є однією з ключових складових загальної безпеки країни в XXI столітті. У сучасному світі, де інформація виступає основним ресурсом і важливим чинником впливу, захист інформаційних процесів стає надзвичайно важливим. Існує багато підходів до вирішення цієї проблеми, залежно від специфіки кожної країни, її геополітичного становища, технічних можливостей та рівня взаємодії на міжнародній арені. Міжнародна інформаційна безпека охоплює не лише захист від кіберзагроз, а й механізми регулювання інформаційних потоків, забезпечення конфіденційності та захисту інтелектуальної власності, а також протидію інформаційним атакам та маніпуляціям.

Визнаючи зростаючу важливість інформаційної безпеки для виконання мандатів своїх організацій, у 2011 році Мережа ІКТ (ICTN) Комітету високого

рівня з питань управління (HLCM) домовилася про створення Групи спеціальних інтересів з інформаційної безпеки (UNISSIG), яка займається критично важливою сферою інформаційної безпеки. UNISSIG є основним механізмом в системі ООН для сприяння міжвідомчій співпраці та взаємодії з питань, пов'язаних з інформаційною безпекою. Її основною метою є оптимізація інформаційної безпеки в організаціях-членах. Ця мета досягається шляхом постійної та колективної оцінки вразливості системи ООН до (внутрішніх і зовнішніх) загроз, щоб зменшити ризик на всіх рівнях організації, особливо на стратегічному та оперативному рівнях. Організації-члени визнають, що ефективний захист інформаційних активів системи ООН забезпечує платформу довіри з усіма зацікавленими сторонами, а отже, вимагає цілісного підходу до інформаційної безпеки та захисту даних, щоб захистити, серед іншого, цілісність організацій, зовнішній імідж та операційну ефективність. Таким чином, ССОБ ООН займається управлінням організаційними ризиками, пов'язаними з конфіденційністю, цілісністю, доступністю та надійністю інформаційних активів організацій-членів. Скоординований і послідовний підхід до управління інформаційною безпекою в системі ООН підтримується UNISSIG через її прихильність до обміну знаннями, досвідом і рішеннями, а також реалізації спільних проектів. Виконавчі сесії надають групі можливість переглянути пріоритетність і прогрес у виконанні заходів, передбачених її робочим планом [25; 26].

НАТО є однією з найбільш впливових міжнародних організацій, яка переглянула свою політику в галузі інформаційної безпеки, визнала кіберпростір зоною інформаційної боротьби та зробила кібербезпеку ключовим напрямком своєї діяльності.

Інформаційна політика НАТО ґрунтується на принципах демократичного контролю над військово-політичною сферою та активній участі громадськості у міжнародному військово-політичному процесі. З початку 1990-х років, коли зріс інтерес громадськості до діяльності Альянсу, основну роль у формуванні інформаційної політики почали відігравати самі інституції НАТО.

Найважливішим органом, відповідальним за інформаційну політику, є Атлантична рада, яка публікує свої рішення та заяви для преси і загалу. Окрім Атлантичної ради, до інформування громадськості активно долучаються й країни-члени НАТО. Одним із основних структурних підрозділів, що реалізує інформаційну політику Альянсу, є Бюро інформації та преси, яке після Празького саміту 2002 року було перетворено на Департамент публічної дипломатії, що забезпечує інформаційну діяльність. Бюро інформації та преси реалізує різноманітні програми і заходи, спрямовані на підвищення обізнаності громадськості в країнах-членах і партнерах НАТО щодо ролі та напрямків політики Альянсу. Воно співпрацює з національними інформаційними органами та неурядовими організаціями, організовуючи заходи, що пояснюють громадськості мету, місії та досягнення НАТО, а також надає довідкову інформацію про діяльність та структуру Альянсу.

Проблема інформаційної безпеки НАТО, крім технічного забезпечення та стратегічного планування, включає також політичний вимір. Зокрема, це стосується можливості застосування статті 5 Вашингтонського договору у випадку інформаційних атак. Ключовими ініціаторами розширення концепції колективної відповідальності за інформаційну безпеку в межах НАТО є Естонія та США. У зв'язку зі зростанням загрози кібератак НАТО встановлює вимоги до всіх країн, що прагнуть зберегти цілісність, недоторканність та конфіденційність свого інформаційного простору. Зокрема, інформаційні системи країн-членів Альянсу мають постійно вдосконалюватися, а темпи впровадження новітніх інформаційних технологій і їх поширення повинні прискорюватися [27].

Оскільки забезпечення міжнародної інформаційної безпеки є відповідальністю кожної держави, можна розглянути стратегії забезпечення інформаційної безпеки на прикладі країн, таких як Франція та Данія.

Франція забезпечує інформаційну безпеку через комплексний підхід, який включає розробку законодавчих ініціатив, створення спеціалізованих органів і розвиток стратегій для захисту національних інформаційних ресурсів.

Франція також створила Агентство національної безпеки інформаційних систем (ANSSI), яке відповідає за координацію дій із забезпечення кібербезпеки, надає рекомендації та підтримку як державним органам, так і приватному сектору. Крім того, країна активно займається боротьбою з дезінформацією, зокрема в контексті виборчих процесів, через моніторинг та блокування фейкових новин. Франція також є частиною міжнародних ініціатив з кібербезпеки та активно співпрацює з ЄС, НАТО і іншими партнерами для обміну інформацією та реагування на глобальні кіберзагрози. Важливою складовою є розвиток освітніх програм з кібербезпеки для фахівців та громадян з метою підвищення загальної обізнаності щодо кіберзагроз [28].

У 2015 році Франція ухвалила Національну кіберстратегію (Stratégie nationale pour la sécurité du numérique), яка зазначає, що цифрові платформи, зокрема соціальні мережі, можуть мати неоднозначний вплив на формування громадської думки та часто просувають цінності, що не відповідають французьким принципам. Їх часто використовують для поширення дезінформації та пропаганди, що суперечить національним інтересам Франції і підпадає під законодавство про національну безпеку та оборону. Стратегія кібербезпеки Франції визначає п'ять основних цілей, орієнтованих на формування «цифрової республіки», одночасно гарантуючи безпеку та адаптивність ІКТ-систем. Ці стратегічні пріоритети включають: 1) захист ключових національних інтересів у кіберпросторі, зокрема державних інформаційних систем та критично важливої інфраструктури; 2) забезпечення довіри, приватності та захисту персональних даних у мережі через розробку кібербезпекових продуктів та надання юридичної й технічної підтримки; 3) підвищення обізнаності у питаннях кібербезпеки та розвиток потенціалу в цій сфері на національному рівні; 4) створення сприятливих умов для розвитку підприємництва, інвестицій в ІКТ та інноваційного бізнесу; 5) розробка «дорожньої карти» для досягнення європейської стратегічної цифрової автономії [29].

Національна стратегія Данії з кібер- та інформаційної безпеки на 2022-2024 роки була затверджена Міністерством фінансів Данії у грудні 2021 року. Її метою є підвищення технологічної стійкості, захист критично важливих державних ІКТ-систем, а також покращення знань і навичок громадян, бізнесу та органів влади.

У стратегії уряд Данії визначив чотири стратегічні цілі, які встановлюють рамки для розвитку сильнішої та безпечнішої цифрової Данії:

– Надійний захист життєво важливих суспільних функцій;

– Покращення та визначення пріоритетності рівнів навичок та управління;

– Зміцнення співпраці між державним і приватним секторами;

– Активна участь у міжнародній боротьбі з кіберзагрозами.

В органах державної влади та на підприємствах кібербезпека вимагає від вищого керівництва прагнення зробити безпеку більш невід'ємною частиною управлінської функції, а для забезпечення цього потрібні відповідні навички. Особливо малим і середнім підприємствам бракує навичок і ресурсів для впровадження належних заходів безпеки. Існує загальна проблема залучення та утримання фахівців з необхідними навичками в галузі кібер- та інформаційної безпеки. Тому для підвищення рівня безпеки на всіх рівнях потрібно збільшити кількість доступних професійних навичок. Крім того, існує також потреба в ініціативах, спрямованих на підвищення кваліфікації населення Данії в цілому. Серед іншого, стратегія встановлює низку нових вимог до безпеки для міністерств, відповідальних за суспільні функції або критичні ІТ-системи. Стратегія також передбачає ряд заходів, спрямованих на підвищення рівня компетентності та зміцнення управління кібернетичною та інформаційною безпекою. Стратегія також сприяє підвищенню рівня знань серед громадян. Водночас необхідно посилити міжнародну співпрацю в ЄС, ООН, НАТО та з країнами-однодумцями, щоб зробити кібератаки проти Данії більш обтяжливими [30].

Отже, кожна держава, що є частиною глобального інформаційного простору, повинна розробити комплексну систему заходів для забезпечення власної інформаційної безпеки, яка включає:

– розробку законодавчих актів і нормативно-правових документів, які регулюють питання інформаційної безпеки, захисту даних і кібербезпеки;

– забезпечення безпеки ключових інформаційних і технологічних ресурсів держави, таких як енергетичні, фінансові та комунікаційні системи;

– розробку механізмів для боротьби з інформаційними маніпуляціями, фальшивими новинами та кібер-пропагандою;

– створення системи навчання і підвищення кваліфікації фахівців у галузі інформаційної безпеки, а також підвищення рівня обізнаності громадян щодо питань кібербезпеки;

– активну участь у міжнародних ініціативах і співпраця з іншими країнами для обміну інформацією та спільного реагування на глобальні кіберзагрози;

– створення ефективних систем для збереження та відновлення критичної інформації в разі кібератак або інших надзвичайних ситуацій.

Висновки до розділу 1

У сучасному світі інформаційна безпека набуває вирішального значення, оскільки зростання цифрових технологій призводить до збільшення ризиків, пов'язаних з витоками даних, кіберзлочинністю та кібератаками. В умовах глобалізації та інтеграції інформаційних систем забезпечення конфіденційності, цілісності та доступності даних стає пріоритетом не тільки для бізнесу, а й для державних органів та приватних осіб. Атаки на інформаційні системи можуть мати серйозні наслідки, включаючи фінансові втрати, порушення репутації та навіть загрози національній безпеці. Тому забезпечення інформаційної безпеки є критично важливим для стабільного розвитку суспільства, зміцнюючи довіру до цифрових технологій та інновацій.

Аналізуючи вищезазначені підходи до поняття інформаційної безпеки, варто наголосити, що термін «інформаційна безпека» можна розглядати як стан захищеності інформаційного середовища, що забезпечує належний рівень захисту інформації на різних рівнях: особи, підприємства, суспільства або держави. Вона включає в себе комплекс заходів, які запобігають виникненню негативних наслідків, спричинених впливом несанкціонованих, умисних або неумисних маніпуляцій з інформацією. Інформаційна безпека має на меті захистити життєво важливі інтереси, інформаційну інфраструктуру та можливості розвитку суб'єктів (держава, суспільство, особистість), унеможливлюючи деструктивні інформаційні впливи, що можуть призвести до негативних наслідків на шляху стійкого розвитку.

Враховуючи підходи до визначення поняття «міжнародна інформаційна безпека», варто наголосити, що це комплексний стан глобальних інформаційних відносин, який забезпечує захищеність інформаційного середовища на світовому рівні, підтримуючи стабільність міжнародної системи. Вона охоплює сукупність заходів різного характеру (економічних, політичних, юридичних, організаційних), спрямованих на попередження загроз, забезпечення безпеки держав і міжнародної спільноти в інформаційному просторі. Міжнародна інформаційна безпека передбачає створення умов для сталого розвитку держав і суспільств, а також захисту прав та інтересів осіб в інформаційній сфері, забезпечуючи при цьому недопущення порушень світової стабільності.

Сучасні загрози та виклики міжнародній інформаційній безпеці мають глобальний характер та охоплюють широкий спектр проблем, від кібератак до інформаційних війн. З розвитком цифрових технологій і зростанням залежності від Інтернету, країни та міжнародні організації стикаються з новими формами кіберзагроз, такими як хакерські атаки, фішинг, крадіжка персональних даних. Водночас, інформаційні війни, зокрема пропаганда, дезінформація та маніпуляції громадською думкою, стали важливим інструментом в міждержавних конфліктах, що призводить до ескалації напруги на міжнародній

арені. Сучасні виклики також охоплюють питання етики та законодавства в контексті інформаційної безпеки, захисту прав людини в онлайн-середовищі та гарантування конфіденційності даних.

Отже, кожна держава, що є частиною глобального інформаційного простору, повинна розробити комплексну систему заходів для забезпечення власної інформаційної безпеки, яка включає:

– розробку законодавчих актів і нормативно-правових документів, які регулюють питання інформаційної безпеки, захисту даних і кібербезпеки;

– забезпечення безпеки ключових інформаційних і технологічних ресурсів держави, таких як енергетичні, фінансові та комунікаційні системи;

– розробку механізмів для боротьби з інформаційними маніпуляціями, фальшивими новинами та кібер-пропагандою;

– створення системи навчання і підвищення кваліфікації фахівців у галузі інформаційної безпеки, а також підвищення рівня обізнаності громадян щодо питань кібербезпеки;

– активну участь у міжнародних ініціативах і співпраця з іншими країнами для обміну інформацією та спільного реагування на глобальні кіберзагрози;

– створення ефективних систем для збереження та відновлення критичної інформації в разі кібератак або інших надзвичайних ситуацій.

РОЗДІЛ 2. ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В КОНТЕКСТІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

2.1. Загальна характеристика системи інформаційної безпеки України

Розвиток системи інформаційної безпеки України після здобуття незалежності в 1991 році проходив в умовах постійних змін, спричинених як внутрішньополітичними процесами, так і зовнішніми викликами. На етапі становлення незалежності було закладено основи нормативно-правової бази, що визначила ключові принципи захисту інформаційних ресурсів. Проте з початком збройної агресії Росії у 2014 році, яка включала анексію Криму та військові дії на Донбасі, система інформаційної безпеки зазнала значних змін. Відбулося значне посилення уваги до інформаційних загроз, включаючи кібератаки та дезінформаційні кампанії, що зумовило впровадження нових стратегій захисту та адаптацію міжнародних стандартів. З початком повномасштабного вторгнення у 2022 році система інформаційної безпеки України набрала критичного значення, адже протистояння державі-агресору вимагало оперативної реакції на зміни в інформаційному просторі. Даний період визначився активізацією інформаційних операцій, вдосконаленням технологій захисту та формуванням нових механізмів для забезпечення інформаційної стійкості, що стало важливою складовою стратегії національної безпеки.

Стратегія інформаційної безпеки України 2021 року визначає основні напрямки і завдання у сфері захисту інформаційних ресурсів і технологій держави на довгострокову перспективу. Вона передбачає комплексний підхід до забезпечення інформаційної безпеки, акцентуючи увагу на захисті від кіберзагроз, захисті державних інформаційних систем, боротьбі з інформаційними атаками та маніпуляціями, а також на забезпеченні прозорості та безпеки в інформаційних комунікаціях. Стратегія встановлює необхідність розвитку національної кібероборони, взаємодії з міжнародними партнерами у

галузі кібербезпеки, а також зміцнення правового та організаційного забезпечення у цій сфері. Окрім того, стратегія акцентує увагу на необхідності захисту стратегічних інформаційних ресурсів і збереження суверенітету інформаційного простору України [31].

Основні нормативно-правові акти в Україні у сфері інформаційної безпеки включають Закон України "Про основи національної безпеки України" (2003), який визначає інформаційну безпеку як складову національної безпеки, а також Закон "Про інформаційну безпеку" (2017), що регулює захист інформаційних ресурсів та технологій. Закон "Про захист персональних даних" (2010) встановлює правила обробки персональних даних, а Закон "Про кібербезпеку" (2017) визначає правові основи захисту інформаційних систем від кіберзагроз. Постанова Кабінету Міністрів "Про забезпечення інформаційної безпеки державних інформаційних систем" (2017) регулює вимоги до захисту державних інформаційних систем, а Стратегія кібербезпеки України (2016) визначає пріоритети та завдання на державному рівні. Ці акти створюють правову основу для забезпечення інформаційної безпеки в Україні [32].

Нормативна база інформаційної безпеки в Україні виконує кілька ключових функцій, спрямованих на забезпечення національної безпеки в інформаційному просторі. По-перше, вона визначає правові основи для захисту критичної інформаційної інфраструктури та конфіденційних даних, встановлюючи вимоги до їх збереження і захисту від несанкціонованого доступу. По-друге, нормативна база регулює діяльність органів державної влади, надаючи їм повноваження для моніторингу, реагування на кіберзагрози та координації дій з іншими державами і міжнародними організаціями. По-третє, вона сприяє розвитку стандартів і рекомендацій для підприємств та організацій щодо забезпечення кібербезпеки та захисту інформаційних систем. Крім того, нормативні акти визначають відповідальність за порушення в сфері інформаційної безпеки, включаючи кіберзлочини, що дозволяє забезпечити правопорядок та ефективно реагувати на загрози. Нарешті, нормативна база

сприяє розвитку освітніх і дослідницьких ініціатив у галузі кібербезпеки, що забезпечує підготовку кваліфікованих кадрів для боротьби з новими видами загроз.

З 2014 року в Україні активно змінювалася законодавча база у сфері інформаційної безпеки, що було спричинено агресією Росії та потребою у посиленні національної кібербезпеки. У 2014 році було створено перші основи для захисту інформаційного простору, зокрема, через ухвалення закону про інформаційну безпеку, а також через розробку стратегічних документів, таких як Стратегія кібербезпеки України. У 2017 році був прийнятий закон «Про основи національної кібербезпеки України», який визначив основні принципи, органи та механізми захисту критичної інформаційної інфраструктури. Подальші зміни торкнулися посилення контролю за діяльністю в Інтернеті, введення санкцій проти ворожих кіберзагроз, а також активного розвитку співпраці з міжнародними партнерами, зокрема через створення кіберполіції та інших спеціалізованих органів. Протягом 2020-2023 років приймалися додаткові законодавчі ініціативи, що стосуються кіберзахисту критичної інфраструктури, посилення відповідальності за кіберзлочини та підвищення ефективності боротьби з інформаційними загрозами [33].

Незважаючи на наявність нормативно-правової бази в Україні, що регулює питання інформаційної безпеки, існує кілька суттєвих проблем. По-перше, низька ефективність імплементації законів через відсутність належних ресурсів і недостатню координацію між державними органами. По-друге, існують прогалини в законодавстві щодо захисту приватної інформації та забезпечення конфіденційності даних, що створює можливості для зловживань. По-третє, недосконаліть системи реагування на кіберзагрози і відсутність чітких механізмів для швидкого виявлення та нейтралізації атак ставить під загрозу національну безпеку. Крім того, значною проблемою є недостатня кіберосвітня підготовка кадрів, що ускладнює впровадження сучасних технологій та методів захисту інформаційних ресурсів. Також існує недоліки у

законодавчому регулюванні міжнародної співпраці в сфері кібербезпеки, що обмежує ефективність боротьби з глобальними кіберзагрозами.

Також варто зазначити, що одним із значних недоліків чинного українського законодавства в сфері інформації є його недостатня конкретність і певна неясність формулювань. Практично відсутні чіткі визначення механізмів оприлюднення інформації, а також конкретних документів, що повинні підлягати публікації. Не регламентуються терміни здійснення цієї діяльності, а норми, що стосуються фінансового та кадрового забезпечення, майже не містяться, що створює додаткові труднощі в реалізації законодавчих положень.

Органи, відповідальні за інформаційну безпеку, разом із законодавством формують державну систему захисту інформації. Ця система охоплює:

– органи законодавчої, виконавчої та судової влади;

– законодавчі акти, які регулюють питання захисту інформації та інформаційних ресурсів;

– нормативно-правову базу, що забезпечує захист інформації;

– служби та органи захисту інформації на рівні підприємств, організацій та установ.

Верховна Рада України регулює питання захисту інформації через прийняття законів та нормативних актів, спрямованих на забезпечення національної безпеки в інформаційній сфері. Одним із основних законодавчих актів є Закон України «Про захист інформації в інформаційно-комунікаційних системах», який встановлює вимоги до захисту інформаційних ресурсів і регулює безпеку в державних та комерційних інформаційних системах. Крім того, важливими є закони про доступ до публічної інформації та захист персональних даних, які забезпечують прозорість та захист прав громадян на інформацію. Верховна Рада також ухвалила ряд законів, що стосуються кібербезпеки, протидії дезінформації та інформаційним атакам, особливо в умовах військової агресії Росії, зокрема закон «Про основи національного спротиву», що включає заходи щодо захисту інформаційної безпеки країни.

Міністерства та відомства України регулюють питання захисту інформації через розробку та впровадження конкретних нормативно-правових актів, стандартів і процедур, що відповідають національним вимогам безпеки. Зокрема, Міністерство цифрової трансформації відповідає за розвиток політики кібербезпеки, захисту інформаційних систем та цифрових даних, а також за забезпечення безпеки в сфері електронних послуг та комунікацій. Міністерство внутрішніх справ координує питання, пов'язані з боротьбою з кіберзлочинністю та захистом інформаційних ресурсів на рівні правоохоронних органів. Інші відомства, такі як Служба безпеки України (СБУ), займаються протидією інформаційним загрозам, зокрема в контексті національної безпеки, аналізу й усунення ризиків інформаційних атак і дезінформації. Крім того, в Україні діє система сертифікації засобів захисту інформації, що здійснюється Держспецзв'язку, яке також координує роботу з кібербезпекою, встановлюючи стандарти для державних органів та критичної інфраструктури. Всі ці органи працюють у взаємодії, щоб забезпечити належний рівень захисту інформації на національному та державному рівнях.

Державна технічна комісія України (Держтехкомісія) є основним органом управління державною системою захисту інформації. Вона відповідає за розробку та впровадження державної політики у сфері технічного захисту інформації, визначення вимог до засобів та систем, які забезпечують безпеку інформаційних ресурсів. Держтехкомісія здійснює сертифікацію та атестацію засобів захисту інформації, проводить їх перевірку на відповідність стандартам безпеки. Крім того, вона координує заходи щодо захисту державної та комерційної інформації, зокрема в органах державної влади, а також забезпечує захист критичної інформаційної інфраструктури. Держтехкомісія також відіграє ключову роль у розробці нормативних актів та стандартів, що регулюють діяльність у галузі інформаційної безпеки, а також у здійсненні контролю за виконанням вимог щодо захисту інформації в Україні [34].

СБУ здійснює комплексний контррозвідувальний захист у сфері інформаційної та кібернетичної безпеки держави. Основними завданнями в цій сфері є:

– Запобігання, виявлення, припинення та розслідування кримінальних правопорушень у кіберпросторі, які становлять загрозу миру та безпеці людства.

– Виконання контррозвідувальних та оперативно-розшукових заходів для протидії кібертероризму і кібершпигунству.

– Протидія кіберзлочинності, наслідки якої можуть створити загрозу для критично важливих інтересів держави.

– Розслідування кіберінцидентів та кібератак на державні електронні ресурси й критичну інформаційну інфраструктуру [35; 36].

Наприклад, Національна поліція України для забезпечення інформаційної безпеки держави вживає низку заходів:

– Забезпечення інформаційної безпеки на сучасному етапі вимагає комплексного підходу, що поєднує як гуманітарні, так і технічні знання. Це зумовило створення спеціального підрозділу - Департаменту кіберполіції в структурі Національної поліції України;

– Організація протидії негативному впливу, який загрожує інтересам держави та суспільства, за допомогою технічних засобів захисту. Це також включає боротьбу з кіберзлочинами, які становлять пряме суспільне зло, а також оцінку матеріальних і моральних збитків та їхнє мінімізування у разі порушення функціонування інформаційних систем;

– Заходи щодо забезпечення інформаційної безпеки, які реалізуються поліцією, можна класифікувати з теоретико-методологічної точки зору на такі види: організація запобіжних заходів, організація блокування та протидії реальним інформаційним загрозам, а також організація відновлення після настання наслідків від цих загроз, якщо їх не вдалося уникнути;

– Основним завданням Національної поліції є своєчасна профілактика та запобігання правопорушенням в інформаційному середовищі суспільного життя [37].

Система інформаційної безпеки України є багатогранною і складається з кількох ключових елементів, які взаємодіють між собою для забезпечення ефективного захисту інформаційного середовища держави. Основними складовими цієї системи є державні органи, організації та установи, які відповідають за різні аспекти інформаційної безпеки, від технічного захисту інформації до протидії інформаційним загрозам. До основних органів, що беруть участь у забезпеченні інформаційної безпеки України, належать: Рада національної безпеки і оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Міністерство цифрової трансформації України та Національний центр кібербезпеки. Завдяки скоординованій діяльності цих органів забезпечується всебічний захист інформаційного середовища України, який включає як профілактику, так і оперативне реагування на інформаційні загрози, що виникають у різних сферах життя держави. Забезпечення інформаційної безпеки в умовах війни, економічної нестабільності та сучасних кіберзагроз є важливою складовою стратегії національної безпеки, що дозволяє Україні не тільки зберегти суверенітет, але й протистояти зовнішнім і внутрішнім викликам.

Серед основних викликів та загроз системі інформаційної безпеки України можна виділити наступні:

– Інформаційний вплив Росії як країни-агресора на громадян України;

– Панування інформаційної пропаганди Російської Федерації на тимчасово окупованих територіях України;

– Спроби маніпулювання громадською свідомістю українців щодо процесу європейської та євроатлантичної інтеграції України;

– Недостатній рівень медіаграмотності та інформаційної культури в суспільстві, що ускладнює ефективну протидію маніпуляціям та інформаційним впливам [38].

Після 24 лютого 2022 року, коли Росія розпочала повномасштабну агресію проти України, країна-агресор посилила інформаційні атаки, які стали невід'ємною частиною гібридної війни. Інформаційно-психологічні операції Росії тривали паралельно з військовими діями, спрямованими на дезінформацію, маніпуляцію громадською думкою і послаблення морального духу українців. Пропаганда, фейки та маніпуляції використовувалися для підриву довіри до уряду України, дискредитації ЗСУ та міжнародної підтримки, а також для поширення страху серед цивільного населення. Російські медіа активно поширювали неправдиву інформацію про нібито нацистську владу в Україні, використовуючи елементи психоопераций, що мали на меті деморалізувати та дестабілізувати ситуацію як усередині країни, так і за її межами [39].

Росія намагається сформувати власний інформаційний простір на тимчасово окупованих територіях України. Кремлівська пропаганда активно нав'язується через школи та ЗМІ. Міністерство оборони Великої Британії повідомляло про це ще у 2023 році. Згідно з британськими розвідданими, опублікованими 18 серпня 2023 року, було зазначено таку інформацію:

– «В Запорізькій області окупаційна влада отримала вказівки з Росії щодо впровадження нових стандартів акредитації для навчальних закладів. Крім того, журналісти з Росії знаходять роботу в медіа на окупованих територіях.

– Новий підручник з історії Росії з 1 вересня 2023 року надійде до шкіл в окупованих регіонах України та по всій Російській Федерації. У книзі вихваляється так звана спеціальна військова операція і описується Україна як ультратерористична держава.

– Метою росії є створення прокремлівського інформаційного простору в окупованих регіонах з метою розмивання української національної ідентичності» [40].

Стратегічний курс України на вступ до ЄС та НАТО є основними пріоритетами національних інтересів і безпеки, що закріплено в Конституції України. Більшість громадян підтримує цей курс. Однак водночас активно

поширюються міфи та дезінформаційні стереотипи про ЄС і НАТО, спрямовані на маніпулювання громадською свідомістю, з метою ослаблення єдності суспільства щодо зовнішньої політики України та уповільнення реформ [41].

Низький рівень інформаційної культури та медіаграмотності в суспільстві на тлі швидкого розвитку цифрових технологій створює сприятливі умови для маніпулювання громадською думкою і проведення дезінформаційних кампаній, що, у свою чергу, збільшує ризики для інформаційної безпеки України. [42].

Проаналізувавши згадані загрози для інформаційної безпеки України, можна зробити висновок, що основою ефективної системи забезпечення інформаційної безпеки є посилення державних інститутів та органів, які відповідають за цю сферу. Реалізація цього завдання вимагає вирішення низки комплексних завдань, зокрема розробки надійної системи інформаційної безпеки, пошуку нових і нестандартних підходів до організації, взаємодії та координації дій, а також вдосконалення всіх засобів управління ризиками та загрозами.

2.2. Функціонування системи інформаційної безпеки України з 2014 року та до повномасштабного вторгнення РФ

З початком анексії Криму Росією та збройної агресії на Донбасі в 2014 році питання забезпечення інформаційної безпеки стало надзвичайно важливим не лише для функціонування національної системи безпеки, але й для збереження державності України. Ці події виявили вразливості в національній безпеці та підкреслили потребу в комплексному підході до захисту інформаційного простору, що стало пріоритетом державної політики. Інформаційний аспект російської агресії є важливою частиною інформаційної війни між Україною та Росією. Це включає активне поширення неправдивої чи спотвореної інформації для дискредитації України, кібератаки, пропаганду російських цінностей серед українців тощо. Така ситуація загрожує

суверенітету та національній безпеці України, що робить необхідним розробку ефективних механізмів для протидії цим загрозам.

Під час російської агресії проти України в 2014 році світ став свідком використання нового типу війни, в якій головними елементами стали домінування в інформаційному просторі та гібридні, асиметричні методи ведення бойових дій.

У 2014 році Росія застосувала комплексну гібридну стратегію агресії проти України, поєднуючи військові, політичні та інформаційні інструменти для досягнення своїх цілей. Один з перших етапів цієї агресії відбувся через анексію Криму. Скориставшись політичною та соціальною нестабільністю в Україні після Євромайдану, Росія провела швидку і безкровну анексію півострова, використовуючи так званих «зелених чоловічків» — військових без розпізнавальних знаків, які взяли під контроль ключові об'єкти в Криму, одночасно маніпулюючи місцевим населенням і створюючи вигляд легітимності. Паралельно з анексією Криму Росія почала підтримувати сепаратистські рухи на сході України, зокрема в Донецькій та Луганській областях. Вона постачала бойовикам зброю, техніку і боєприпаси, а також організовувала підготовку та введення регулярних військ без офіційного визнання участі. Це дозволило Росії вести війну через проксі-сили, не визнаючи свою пряму участь у конфлікті, що сприяло її дипломатичній безкарності на міжнародній арені. Крім того, Росія вела активну інформаційну війну. Через свої медіа та соціальні мережі вона поширювала фальшиві новини і маніпулювала фактами, намагаючись виправдати свою агресію. Одним із основних наративів була історія про «геноцид» росіян в Україні, а також про необхідність захисту російськомовних громадян на сході країни. Пропаганда активно використовувала образи нацизму, створюючи образ України як держави, що не здатна забезпечити права російськомовного населення. Водночас Росія застосовувала економічний тиск. Вона блокувала постачання газу та вводила санкції, намагаючись створити додаткову нестабільність в Україні і підштовхнути її до політичних поступок. Це також включало

енергетичну залежність України від Росії, що ставало важливим важелем для маніпуляцій на міжнародному рівні. Крім прямої агресії, Росія здійснювала психологічний тиск, спрямований на зниження морального духу українців. Постійні маніпуляції в медіа, пропаганда страху і залякування разом з економічними труднощами створювали атмосферу невизначеності і страху. Росія також намагалася посіяти розбіжності всередині українського суспільства, створюючи конфлікти між різними політичними та соціальними групами [43].

Російські традиційні ЗМІ, що підтримують Кремль, з самого початку кризи змальовували негативну картину Євромайдану та Києва в негативному світлі. Наприклад, російські ЗМІ стверджували, що сотні біженців залишають Україну в пошуках притулку в Росії через жорстокість української влади щодо (російськомовного) населення (ТАСС 2014a, 2014b, 2014c). У кількох випадках ці повідомлення супроводжувалися фото- і відеоматеріалами з українсько-польського, а не українсько-російського кордону (рис. 1). Серед інших неточностей були також твердження про те, що фрегат ВМС України «Гетьман Сагайдачний» дезертирував. Після спростування російські ЗМІ лише повідомили, що фрегат завантажив розвідувальне обладнання НАТО (Сівкова 2014, ТАСС 2014d) [44].

З 2014 року Росія активно використовувала дезінформацію та пропаганду для виправдання агресії на Донбасі. Російські медіа та офіційні особи поширювали фальшиві твердження про "геноцид" російськомовного населення на сході України, звинувачуючи українську армію в нібито жорстокому поводженні з цивільними. Пропаганда стверджувала, що Росія "захищає" етнічних росіян і російськомовних, а також нібито намагається стабілізувати регіон. Паралельно використовувалась теза про "самооборону" так званих ДНР та ЛНР, що дозволяло Росії виправдати постачання зброї, техніки та військових підрозділів на Донбас. Ці маніпуляції допомогли Росії створити образ "миротворця" в очах власного населення і міжнародної спільноти, відволікаючи увагу від реальних військових дій і підтримки сепаратистів [45].

Таким чином, російська агресія виявилася не лише у воєнних діях на фронті, але й у масштабних інформаційних операціях, спрямованих на дестабілізацію внутрішньополітичної ситуації в Україні, підрив довіри до державних інститутів, маніпуляції громадською думкою та поширення дезінформації. На початкових етапах збройної агресії у 2014 році система інформаційної безпеки України виявилася недостатньо готовою до таких загроз, зокрема через відсутність єдиної стратегії боротьби з інформаційною агресією та недостатню координацію між державними органами. Важливим кроком стало створення спеціальних органів, таких як Кіберполіція та Рада національної безпеки і оборони України (РНБО), які взяли на себе координацію заходів з кіберзахисту та інформаційної безпеки, а також розробка нових законодавчих актів у цій сфері. З початком повномасштабного вторгнення Росії в 2022 році, система інформаційної безпеки України зазнала значних змін та вдосконалень. Держава активно залучала міжнародних партнерів для боротьби з інформаційними загрозами, а також здійснила значний крок до зміцнення внутрішнього інформаційного простору. Протидія інформаційним атакам стала невід'ємною частиною національної безпеки, а забезпечення інформаційної безпеки стало критично важливим для стійкості державних інститутів та суспільства в цілому. Створення та удосконалення стратегій боротьби з інформаційними загрозами, активізація моніторингу інформаційних каналів та посилення кіберзахисту стали необхідними умовами для ефективної протидії російській інформаційній агресії. Збройна агресія РФ виявила вразливості в інформаційній безпеці України, але також стала каталізатором для розвитку ефективної системи інформаційного захисту. Враховуючи досвід боротьби з інформаційними загрозами в період з 2014 року, можна зробити висновок, що система інформаційної безпеки України значно покращилася і адаптувалася до нових реалій, проте залишаються актуальними питання удосконалення внутрішньої координації між органами влади та підвищення стійкості національної інформаційної інфраструктури.

2.3. Функціонування системи інформаційної безпеки України під час широкомасштабного військового нападу РФ

З початком повномасштабної війни росії проти України наша держава зіткнулася з новими викликами в контексті інформаційної війни. Російська сторона використовує потужні та деструктивні методи, зокрема дезінформацію, маніпуляцію фактами та пропаганду, щоб підірвати довіру до українських державних інститутів і сформувати негативний імідж України на міжнародній арені. Однак, незважаючи на ці загрози, Україна виявила здатність до адаптації та ефективної протидії агресії в інформаційній сфері. Завдяки впровадженню стратегій медіа-грамотності, активній роботі з фактчекінговими організаціями та мобілізації громадськості, українські фахівці домоглися значних успіхів у нейтралізації ворожих інформаційних атак, зберігаючи національну ідентичність та зміцнюючи підтримку з боку міжнародної спільноти.

В арсеналі інформаційних засобів, які використовує росія проти Україні, є безліч різноманітних інструментів та методів. Серед найпоширеніших і найчастіше застосовуваних є наративи.

Наратив у пропаганді має критичне значення, оскільки він слугує інструментом для формування певних уявлень, переконань та ставлень у суспільстві. Постійне повторення одного й того ж наративу зміцнює його присутність у свідомості аудиторії, створюючи ефект постійної переконливості. Це підсилює віру в історію, яку часто повторюють, і дає їй вигляд беззаперечної істини. У такий спосіб пропаганда здатна впливати на колективну свідомість і змінювати громадську думку, часто навіть без усвідомлення цього з боку самих людей, оскільки вони звикають до нав’язуваних ідей [46].

Багато наративів, створених під час повномасштабної війни, були спрямовані на підрив підтримки України з боку міжнародних партнерів, зокрема щодо постачання військової допомоги для Збройних Сил України. На самому початку повномасштабного вторгнення багато країн Заходу не відразу погоджувалися надати таку підтримку, оскільки чекали на розвиток подій і вивчали ситуацію. Російська пропаганда частково досягла очікуваного ефекту:

у колективному Заході з'явилися прихильники наративів, які намагаються виправдати вторгнення в незалежну державу та закликають до припинення військової допомоги Україні. Це також призвело до того, що деякі політики, які підтримують проросійську позицію, намагаються блокувати або затягувати процес ухвалення рішень щодо фінансової та військової допомоги Україні в парламентах різних країн. Така позиція значно зменшує можливості української армії в наступальних операціях та на оборонних позиціях, оскільки затримка з постачанням необхідної техніки та озброєнь створює додаткові труднощі для боротьби з агресором. У той же час Росія активно заручається підтримкою інших режимів, які розділяють її геополітичні інтереси, що дозволяє їй компенсувати частину своїх втрат у міжнародній арені.

Пропагандистська машина Росії активно використовує наративи, які є частиною добре відомих кремлівських методичок з пропаганди. Одним із основних наративів є заперечення існування України як незалежної держави, а також ствердження про спільність історії, культури та традицій між Україною та Росією. Пропагандисти активно поширюють ідею, що Україна нібито не відбулася як державність, що її створення стало результатом більшовицької політики. Цей наратив знайшов відображення у промові президента Росії Володимира Путіна, виголошеній 21 лютого 2022 року. У ній він заявив: «Власне, як уже сказав, унаслідок більшовицької політики і виникла радянська Україна, яку і в наші дні можна з повною підставою назвати «Україна імені Володимира Ілліча Леніна». Він її автор та архітектор. Це повністю підтверджується архівними документами, включаючи жорсткі ленінські директиви щодо Донбасу, який буквально втиснули до складу України». Саме на базі цього наративу 24 лютого 2022 року Путін оголосив початок «спеціальної воєнної операції» (СВО), яку Росія представляла як «денацифікацію» та «демілітаризацію» України. Важливою складовою цього підходу було й визнання самопроголошених Донецької та Луганської Народних Республік, що також стало частиною російської пропагандистської кампанії щодо легітимізації агресії та виправдання вторгнення [47; 48].

Теза про те, що в Україні до влади прийшли нацисти, стала основним елементом російської пропаганди ще з 2014 року після Революції Гідності. Кремль використовував цей наратив, аби виправдати агресію проти України, звинувачуючи нову владу в "фашизмі" та "екстремізмі". Пропаганда активно просувала образ України як нацистської держави, що підживлювалося маніпуляціями з приводу радикальних груп та зображенням націоналістів як основної політичної сили. Ця кампанія продовжилась у 2019 році після приходу до влади Володимира Зеленського, коли Росія намагалася використати нові політичні зміни для підсилення старих наративів і дискредитації української влади на міжнародній арені [49].

Наратив про дегуманізацію на основі релігійних переконань активно використовується російськими пропагандистами. Наприклад, Рамзан Кадиров заявляє, що всі росіяни - це воїни світла, військо Ісуса, а їхня війна з Україною є священною боротьбою проти антихриста. За його версією, антихристом є українці. Деякі російські пропагандисти навіть намагалися довести, що Володимир Зеленський - це антихрист, а весь народ України - його слуги. Цей наратив орієнтований на апеляцію до міфічного мислення і релігійних уявлень, зокрема серед вірян Російської православної церкви. Така риторика спрямована не лише на чеченців, а й на всю російську аудиторію, намагаючись створити образ України як ворога, що стоїть проти священних цінностей Росії [50].

Росія активно використовує пропагандистський наратив, що «Росія не може програти війну, бо якщо програє, то наступить кінець всього». Цей наратив має на меті створити враження, що війна з Україною для Росії - це не просто боротьба за території, а питання її існування як держави. Такий підхід Росія використовує для підвищення морального духу своїх військових і громадян, залучення внутрішньополітичних і зовнішньополітичних ресурсів, а також для виправдання своїх дій на міжнародній арені. Однак цей наратив є необґрунтованим, оскільки програш війни не означає «кінець всього», а може стати можливістю для нових політичних і соціальних змін у країні [51].

У інформаційній війні проти України росія також застосовує такий інструмент як дезінформація. Під поняттям «дезінформація» можна розуміти неправдиву, оманливу, маніпулятивну інформацію, яка створена навмисно заради економічних, політичних або інших вигод. Цей інструмент є частиною наративу, бо останній часто базується на неправді [52].

Український наступ на Курському напрямку став приводом для нової хвилі фейків з боку російської пропаганди. Російські медіа та офіційні джерела почали активно поширювати неправдиву інформацію про нібито значні втрати українських військ, використання заборонених методів ведення бою та навіть фальшиві заяви про відступ українських сил. Ці маніпуляції мали на меті знизити моральний дух українських військ і населення, а також дискредитувати Збройні Сили України на міжнародній арені. Російська пропаганда намагалася замаскувати реальні невдачі на фронті, перекладаючи відповідальність за ситуацію на українську сторону, створюючи уявлення про "неуспіхи" наступу [53].

ІПСО, або «інформаційно-психологічна операція», є терміном, що описує методи впливу на свідомість людей, за допомогою яких можна змінювати їхню психологічну установку чи настрій, а також сприйняття певних подій або ситуацій. В радянській традиції використовувалися терміни «спецпропаганда» або «психологічна війна», тоді як в західній, зокрема американській, практиці застосовують поняття «психологічні операції» (PsyOp) або «операції впливу». Мета ІПСО (інформаційно-психологічних операцій) полягає в маніпулюванні думкою, послабленні морального духу населення та військових, створенні хаосу та дезінформації з метою досягнення стратегічних цілей. Росія використовує ІПСО для поширення фейкових новин, викривлення фактів, дискредитації України на міжнародній арені та посилення внутрішніх розколів. Українцям під час війни важливо боротися з російським ІПСО, зокрема, критично оцінюючи джерела інформації. Це означає, що треба перевіряти новини через надійні та незалежні медіа, а також офіційні урядові та міжнародні канали. Важливо також не поширювати неперевірену інформацію,

уникаючи репостів фейкових новин та емоційних повідомлень, які можуть спричинити паніку або дезінформацію. Не менш важливим є навчання громадян через освітні програми з медіаграмотності, щоб вони могли розпізнавати маніпуляції та фейки. Для цього необхідно активно користуватися платформами для перевірки фактів. Окрім того, важливо долучатися до боротьби з пропагандою, беручи участь у волонтерських ініціативах, спрямованих на поширення правдивої інформації [54; 55].

На початку повномасштабного вторгнення багато українців, перебуваючи під великим стресом і під впливом величезного потоку інформації, мали труднощі у відрізнянні фейків від правди. До прикладу, росія поширювала ІПСО щодо міток на будівлях та дорогах України, стверджуючи, що ці позначки використовуються для ідентифікації цілей для обстрілів або як частина "таємних операцій" українських сил. Пропаганда намагалася створити враження, що Україна спеціально мітить цивільні об'єкти для подальших атак, аби дискредитувати українську армію та маніпулювати міжнародною думкою. Фальшиві фото і відео використовувались для поширення цих фальшивих тверджень через медіа та соцмережі [56].

Трагедія в Оленівці стала черговим етапом масштабної інформаційно-психологічної спецоперації (ІПСО). Росія активно просувала інформаційну операцію (ІПСО) щодо трагедії в Оленівці, де в липні 2022 року сталася масова загибель українських військовополонених внаслідок обстрілу, здійсненого російськими військами. Російська пропаганда намагалася перекласти відповідальність за трагедію на Україну, поширюючи фальшиві заяви, що українські військові нібито здійснили обстріл самі, щоб звинуватити Росію у військових злочинах. ІПСО полягала у маніпуляціях фактами, спотворенні доказів та використанні фальшивих свідчень, що мали на меті підрив довіри до української сторони та міжнародних організацій, які проводили розслідування. Російські медіа та офіційні особи активно поширювали ці твердження через різні канали, в тому числі через соціальні мережі, телеканали та спеціалізовані інформаційні платформи. Цей підхід був частиною більш широкої кампанії

дезінформації, спрямованої на відвернення уваги від реальних злочинів Росії та маніпулювання міжнародною громадськістю [57].

Слід зазначити, що всі проаналізовані інструменти росія використовує систематично і згідно з певним алгоритмом у своїй державі. Інформацію про успіхи так званої «спеціальної військової операції» та непереможність військ росії розповсюджують лише для внутрішнього споживача, при цьому перебільшують дані про кількість жертв і втрат у техніці українських Збройних сил. Російська пропаганда має широкий спектр інструментів для ведення інформаційної війни не тільки проти України, а й у глобальному масштабі. Кожен із цих засобів використовується кремлем у рамках продуманої стратегії з конкретними цілями. На сьогоднішній день кіберпростір став паралельним фронтом у російсько-українській війні. Поширення наративів, дезінформації, фейкових новин і кібератак є лише частиною методів протистояння в інформаційній сфері. Усі ці інструменти спрямовані на просування ідей ворога, маніпуляцію свідомістю, пропаганду та спонукання мас до певних емоційних реакцій. Комбінація всіх цих засобів формує потужну дезінформаційну кампанію, що прагне створити та поширити нові наративи, використовуючи емоційний стан населення як один із рушіїв для підриву політичного становища України. Однак навіть такі ретельно продумані дії можуть зазнати невдачі завдяки спростуванню фейків, належному контролю та довірі держав-партнерів. У сучасних умовах Україні надзвичайно важливо покращувати наступні аспекти: медіаграмотність населення, система інформаційної та кібербезпеки, а також ефективне розповсюдження інформації під час війни.

Змінилися і платформи для поширення пропаганди. Якщо в 2014 році основним каналом дезінформації було російське телебачення, то зараз це соціальні мережі та сайти. Важливим кроком у протистоянні Росії в інформаційній сфері було закриття доступу до цих платформ українською владою. «Якби Україна цього не зробила, - зазначає Євген Федченко, - ми б зараз мали ситуацію, подібну до 2014 року, з повним інформаційним домінуванням ворога на нашій території. Однак, оскільки доступ був

обмежений ще до активних бойових дій, це зіграло позитивну роль». За словами Вадима Міського, цей проєкт був запланований через загострення ситуації на кордонах, але він почав працювати саме в день повномасштабного вторгнення. «Хоча матеріали поширюються як подкасти, - додає Вадим Міський, - головний метод розповсюдження – це радіо України, яке функціонує навіть на окупованих територіях, таких як Маріуполь, Мелітополь, Бердянськ, Донбас і Крим. Як зазначає Євген Федченко, сьогодні в Україні немає вакууму інформації, як це було в 2014 році. Україна змогла привернути увагу Заходу та утримати його підтримку. Як зазначає Євген Федченко, «Ніхто краще за українців не знає агресора». Однак ця перемога ще не остаточна, оскільки ворог постійно адаптується, змінює тактику і продовжує маніпулювати, використовуючи соцмережі для просування своїх наративів, вкладаючи значні фінанси в пропагандистську машину, і створюючи альтернативну реальність [58].

Варто наголосити, що на сьогодні головними проблемами у забезпеченні інформаційної безпеки держави у контексті інформаційної агресії з боку так званої росії є:

– По-перше, поширення на міжнародній арені дезінформації, викривлених та упереджених фактів щодо України з боку росії, зокрема, залучаючи іноземні ЗМІ та організації, своїх поплічників, які готові заради грошей або з інших причин здійснювати різного роду "акції" в іноземних державах, проросійські політичні партії і кандидатів, здійснюючи фінансування кампаній і лобіювання інтересів.

– По-друге, важливим аспектом є медіаграмотність українського суспільства. Ця складова є важливою у забезпеченні інформаційної безпеки України, особливо в контексті війни росії проти України. Пропаганда та дезінформація стали одними з основних інструментів гібридної війни, спрямованої на підрив морального духу, посів сумнівів серед населення та дестабілізацію ситуації в країні. Тому важливою проблемою є недостатній рівень медіаграмотності серед частини населення, що сприяє сприйняттю

фейкових новин, маніпуляцій і пропаганди, а також труднощам у тому, щоб відрізнити достовірну інформацію від фальшивої.

Отже, ефективне забезпечення інформаційної безпеки України є критично важливим у контексті сучасних загроз, оскільки інформаційні атаки можуть мати серйозні наслідки для національної безпеки, економіки та соціальної стабільності. В умовах гібридних війн та інформаційних кампаній, спрямованих на дезінформацію та маніпулювання громадською думкою, важливо захищати національні інтереси та інформаційний простір від зовнішніх і внутрішніх загроз. Неправдива або спотворена інформація може підривати довіру до державних інституцій, послаблювати мобілізаційні можливості та сприяти конфліктам. Надійний захист інформації дозволяє забезпечити стабільність, зберегти державний суверенітет і захистити національну ідентичність України.

Висновки до розділу 2

Система інформаційної безпеки України є багатогранною і складається з кількох ключових елементів, які взаємодіють між собою для забезпечення ефективного захисту інформаційного середовища держави. Основними складовими цієї системи є державні органи, організації та установи, які відповідають за різні аспекти інформаційної безпеки, від технічного захисту інформації до протидії інформаційним загрозам. До основних органів, що беруть участь у забезпеченні інформаційної безпеки України, належать: Рада національної безпеки і оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Міністерство цифрової трансформації України та Національний центр кібербезпеки. Завдяки скоординованій діяльності цих органів забезпечується всебічний захист інформаційного середовища України, який включає як профілактику, так і оперативне реагування на інформаційні загрози, що виникають у різних сферах життя держави. Забезпечення інформаційної безпеки в умовах війни, економічної нестабільності та сучасних кіберзагроз є важливою складовою

стратегії національної безпеки, що дозволяє Україні не тільки зберегти суверенітет, але й протистояти зовнішнім і внутрішнім викликам.

Російська агресія виявилася не лише у воєнних діях на фронті, але й у масштабних інформаційних операціях, спрямованих на дестабілізацію внутрішньополітичної ситуації в Україні, підрив довіри до державних інститутів, маніпуляції громадською думкою та поширення дезінформації. На початкових етапах збройної агресії у 2014 році система інформаційної безпеки України виявилася недостатньо готовою до таких загроз, зокрема через відсутність єдиної стратегії боротьби з інформаційною агресією та недостатню координацію між державними органами. Важливим кроком стало створення спеціальних органів, таких як Кіберполіція та Рада національної безпеки і оборони України (РНБО), які взяли на себе координацію заходів з кіберзахисту та інформаційної безпеки, а також розробка нових законодавчих актів у цій сфері. З початком повномасштабного вторгнення Росії в 2022 році, система інформаційної безпеки України зазнала значних змін та вдосконалень. Держава активно залучала міжнародних партнерів для боротьби з інформаційними загрозами, а також здійснила значний крок до зміцнення внутрішнього інформаційного простору. Протидія інформаційним атакам стала невід'ємною частиною національної безпеки, а забезпечення інформаційної безпеки стало критично важливим для стійкості державних інститутів та суспільства в цілому. Створення та удосконалення стратегій боротьби з інформаційними загрозами, активізація моніторингу інформаційних каналів та посилення кіберзахисту стали необхідними умовами для ефективної протидії російській інформаційній агресії. Збройна агресія РФ виявила вразливості в інформаційній безпеці України, але також стала каталізатором для розвитку ефективної системи інформаційного захисту. Враховуючи досвід боротьби з інформаційними загрозами в період з 2014 року, можна зробити висновок, що система інформаційної безпеки України значно покращилася і адаптувалася до нових реалій, проте залишаються актуальними питання удосконалення внутрішньої

координації між органами влади та підвищення стійкості національної інформаційної інфраструктури.

Варто наголосити, що на сьогодні головними проблемами у забезпеченні інформаційної безпеки держави у контексті інформаційної агресії з боку так званої росії є:

– По-перше, поширення на міжнародній арені дезінформації, викривлених та упереджених фактів щодо України з боку росії, зокрема, залучаючи іноземні ЗМІ та організації, своїх поплічників, які готові заради грошей або з інших причин здійснювати різного роду "акції" в іноземних державах, проросійські політичні партії і кандидатів, здійснюючи фінансування кампаній і лобіювання інтересів.

– По-друге, важливим аспектом є медіаграмотність українського суспільства. Ця складова є важливою у забезпеченні інформаційної безпеки України, особливо в контексті війни росії проти України. Пропаганда та дезінформація стали одними з основних інструментів гібридної війни, спрямованої на підрив морального духу, посів сумнівів серед населення та дестабілізацію ситуації в країні. Тому важливою проблемою є недостатній рівень медіаграмотності серед частини населення, що сприяє сприйняттю фейкових новин, маніпуляцій і пропаганди, а також труднощам у тому, щоб відрізнити достовірну інформацію від фальшивої.

Отже, ефективне забезпечення інформаційної безпеки України є критично важливим у контексті сучасних загроз, оскільки інформаційні атаки можуть мати серйозні наслідки для національної безпеки, економіки та соціальної стабільності. В умовах гібридних війн та інформаційних кампаній, спрямованих на дезінформацію та маніпулювання громадською думкою, важливо захищати національні інтереси та інформаційний простір від зовнішніх і внутрішніх загроз. Неправдива або спотворена інформація може підривати довіру до державних інституцій, послаблювати мобілізаційні можливості та сприяти конфліктам. Надійний захист інформації дозволяє забезпечити стабільність, зберегти державний суверенітет і захистити національну ідентичність України.

РОЗДІЛ 3. НАПРЯМКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В КОНТЕКСТІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

3.1. Інструменти протидії дезінформації щодо України у світовому інформаційному просторі

Поширення дезінформації є однією з найбільш актуальних та небезпечних проблем сучасного інформаційного середовища, яка здатна серйозно вплинути на політичну стабільність, громадську думку та міжнародні відносини. У контексті війни росії проти України ця проблема набуває особливого значення. РФ активно використовує інформаційну агресію як частину гібридної війни, зокрема через поширення дезінформації щодо подій в Україні, що має на меті маніпулювати громадською думкою, дискредитувати українську державність, а також посіяти розбіжності між Україною та міжнародними партнерами. Застосування сучасних інформаційних технологій, таких як соціальні мережі, фейкові новини, бот-мережі та інші інструменти, дозволяє досягати глобального охоплення та впливати на аудиторію в різних країнах.

Наприклад, «Агенція соціального дизайну» працює на замовлення адміністрації президента росії та займається розробкою та реалізацією пропагандистських кампаній для підтримки політики кремля. Вона створює інформаційні стратегії, спрямовані на маніпулювання громадською думкою як в росії, так і за її межами. Агенція розвиває фальшиві громадські ініціативи, просуває ідеї «русского мира», дискредитує ворогів росії та створює позитивний імідж влади через медіа, соціальні мережі та інші платформи. Її діяльність є важливою частиною інформаційної війни росії на міжнародному рівні [62; 63].

Російська пропаганда активно контролює мережу іноземних порталів, які були створені або підтримуються з метою поширення вигідних для Кремля наративів. Ці портали часто маскуються під незалежні новинні ресурси, надаючи собі вигляд об'єктивних медіа. Вони сприяють поширенню дезінформації, фейків та маніпуляцій, що дискредитують Україну, Захід та

демократичні цінності. Зазвичай ці ресурси фокусуються на таких темах, як нібито "русофобія" в Україні, кризи в країнах Європи, критикують політику НАТО та ЄС, і підтримують російську агресію на міжнародній арені. Через подібні портали проводиться атака на міжнародну довіру до західних інституцій та створюється образ Росії як захисника "традиційних цінностей". Такі портали часто мають вигляд локальних новинних сайтів у країнах Європи або в країнах, що перебувають під впливом Росії, і можуть використовувати місцеву мову, щоб здобути довіру аудиторії. Вони часто співпрацюють із проросійськими блогерами, політиками та активістами для поширення своїх меседжів у соціальних мережах. Таким чином, Росія використовує цю мережу для досягнення своїх геополітичних цілей, маніпулюючи громадською думкою в інших країнах і намагаючись підривати міжнародні альянси, зокрема між Україною та її західними партнерами.

Польські сайти, які поширюють російську пропаганду, часто використовують антиукраїнські наративи, що сприяють розпалюванню напруження між Україною та Польщею. Ці ресурси розповсюджують фейки та дезінформацію, зокрема про ситуацію на польсько-українському кордоні, про нібито «антипольські» настрої в Україні та ускладнення співпраці між країнами. Через це вони намагаються посіяти недовіру до української влади, зміцнити проросійські настрої в Польщі і підривати підтримку України на міжнародній арені. Такі сайти часто мають зв'язки з проросійськими структурами та фінансуються з зовнішніх джерел, що дозволяє їм активно впливати на громадську думку. Приклади таких сайтів: "Sputnik Polska", "Russia Today (RT) Polska", "Polska dla Polaków" [64; 65].

Росіяни також активно використовують у своїй дезінформаційній кампанії псевдоекспертів. Наприклад, у дослідженні Інституту інноваційного врегулювання зазначається, що серед проросійських політичних експертів та коментаторів у Німеччині особливо виділяється Олександр Рар. Він є відомим німецьким консультантом з менеджменту та істориком Східної Європи, а також лобістом російської газової компанії «Газпром» і підтримує політику

російського уряду на чолі з Володимиром Путіним. Зокрема, Рар поширює проросійські пропагандистські наративи, стверджуючи, що Україна позбавлена суверенітету (за його версією, Росія і Захід є протиборчими силами), що перемога Путіна у війні неминуча, а після поразки України відновляться нормальні економічні відносини між Росією і Заходом.

До прикладу, наприкінці 2023 року Росія активно використовувала ситуацію з блокуванням польсько-українського кордону для поширення дезінформації. Російські медіа створювали наративи, що Польща нібито блокує економічні і гуманітарні зв'язки між Україною та Європою, щоб ослабити Україну та ускладнити її відносини з ЄС. Це мало на меті посіяти розбіжності між Україною та Польщею, а також знизити довіру українців до західних партнерів, створюючи вигляд, що Захід не підтримує Україну в її боротьбі з Росією [66].

Враховуючи зазначені приклади щодо поширення дезінформації у світовому інформаційному простору щодо України з боку рф, нашій державі слід удосконалити наступні механізми протидії таким загрозам з метою ефективного функціонування національної системи інформаційної безпеки:

– Створення за ініціативою України разом з державами-партнерами міжнародного майданчика з питань протидії російській дезінформації. Така платформа буде максимально корисною не тільки для України, але й держав-партнерів, оскільки дозволить ефективно та швидко проводити комунікацію щодо усунення та спростування кремлівських наративів, пропаганди, фейків, дезінформації, які агресор поширює про Україну та партнерів через певні іноземні ЗМІ та організації, проросійських політиків-прибічників та партії. Також миттєві консультації з партнерами щодо рішень про ведення жорстких санкцій для подібних осіб та організацій;

– Залучення національних та іноземних громадських організацій, журналістів до перевірки новин, створення прозорої системи для власних громадян, щоб вони могли перевіряти правдивість інформації перед тим, як поділитися нею. Також відкриття якомога більшої кількості представництв

українських ЗМІ закордоном. При цьому активно співпрацювати з партнерами щодо припинення діяльності будь-яких так званих представництв російських пропагандистів закордоном;

– Розбудова ефективної системи контрпропаганди, яка передбачає:

а) створення та поширення позитивного інформаційного контенту, який не тільки відповідає на дезінформацію, але й активно просуває правду про Україну, її історію, культуру, політику, економічні досягнення та роль у міжнародних відносинах;

б) підтримка й розвиток офіційних урядових ресурсів, таких як сайт Міністерства інформаційної політики, на яких надаються достовірні й перевірені дані, а також інструменти для верифікації новин та фактів;

в) робота з міжнародними ЗМІ та інфлюенсерами для створення контенту, який висвітлює об’єктивну ситуацію в Україні, протидіє пропаганді росії та мобілізує міжнародну підтримку.

3.2. Покращення рівня медіаграмотності українського суспільства як один із напрямків забезпечення інформаційної безпеки

Медіаграмотність є важливим складником інформаційної безпеки та стратегічним елементом у сучасному глобалізованому світі, де інформація поширюється миттєво і впливає на суспільні настрої, політичні процеси та навіть національну безпеку. В умовах війни, особливо в контексті російської агресії проти України, медіаграмотність набуває особливої значущості. РФ активно використовує інформаційну та медійну зброю для маніпулювання громадською думкою, поширення дезінформації, пропаганди та створення альтернативних реальностей, що підривають внутрішню стабільність України та її міжнародну репутацію.

Українське суспільство стикається з масштабними інформаційними викликами, що включають як зовнішні загрози, так і внутрішні проблеми з інформаційною взаємодією. Одним з основних завдань національної безпеки є

не лише захист від дезінформації ззовні, а й формування стійкості громадян до маніпуляцій та спотворених інформаційних наративів. Враховуючи масштаби інформаційної війни, в якій Україна є однією з головних мішеней, проблема медіаграмотності стає критично важливою для забезпечення єдності та національної безпеки.

Тест з медіаграмотності в Україні у 2024 році став важливою подією для оцінки рівня інформаційної обізнаності громадян. За результатами тестування, більшість учасників продемонстрували високий рівень розуміння основ медіаграмотності, зокрема здатність аналізувати джерела інформації, визначати фейки та маніпуляції. Проте, незважаючи на загальну позитивну картину, виявилися певні проблеми, зокрема в осіб старшого віку, які мають менше навичок критичного мислення щодо медіа. Загалом, тестування виявило необхідність подальшої роботи з популяризації медіаграмотності, особливо серед молоді та в сільських районах, де доступ до сучасних освітніх ресурсів обмежений. У 2024 році тест на медіаграмотність в Україні показав, що близько 70% учасників продемонстрували хороший рівень знань, з найкращими результатами серед молоді та людей з вищою освітою, а також у містах з розвиненою інфраструктурою. Проте, старші за 50 років учасники мали значно гірші результати (лише 40% правильних відповідей), а в сільських районах показники були нижчими, близько 50%. Основні труднощі виникли при визначенні фейків і оцінці надійності джерел, що вказує на необхідність подальшої роботи з підвищення медіаграмотності серед різних вікових та регіональних груп [67].

За даними дослідження громадської організації «Детектор медіа», показники індексу медіаграмотності української аудиторії за 2023 рік зазнали значних змін. Частка осіб з рівнем медіаграмотності вище за середній зменшилась з 81% до 76%, що свідчить про помітний регрес у порівнянні з попередніми роками. Варто зазначити, що з 2020 по 2022 рік індекс медіаграмотності зріс з 55% до 81%.

Згідно з результатами 2023 року, 3% українців мають низький рівень медіаграмотності (у 2022 році цей показник становив 6%), 21% - рівень нижчий за середній (у 2022 році - 13%), 62% володіють вищим за середній рівнем медіаграмотності (у 2022 році - 50%), і 14% - високим рівнем (у 2022 році - 31%) [68].

Дослідження також показує, що рівень медіаграмотності громадян залежить від їхньої освіти, віку, рівня добробуту та місця проживання. Чим нижчий освітній рівень, тим гірший рівень медіаграмотності. Так, серед осіб з загальною середньою освітою 29% мають низький або нижчий за середній рівень медіаграмотності, тоді як серед тих, хто має вищу освіту, ця частка становить лише 13%. Водночас половина людей з вищим за середній рівнем медіаграмотності мають дипломи про вищу освіту. Серед тих, хто демонструє високий рівень медіаграмотності, 61% мають вищу освіту. Високий рівень медіаграмотності, як правило, характерний для молодих людей віком 18-25 років, що, зокрема, обумовлено їхньою високою цифровою компетентністю. У той час як низький рівень медіаграмотності характерний для осіб старшого віку, зокрема в групі 56-65 років [69; 70].

Слід зазначити, що покращення рівня медіаграмотності українського суспільства є одним із найважливіших напрямків забезпечення інформаційної безпеки держави. З цією метою можна удосконалити наступні ініціативи, які допоможуть громадянам України адекватно оцінювати інформацію та запобігати маніпуляціям:

– Організація освітніх ініціатив для школярів та студентів, щоб навчити молодь правильно сприймати медіа-контент, виявляти фейки та перевіряти факти;

– Створення кампаній для широкої аудиторії, що будуть сприяти розвитку критичного мислення, заохочення до аналізу джерел інформації та використання перевірених ресурсів;

– Проведення тренінгів для журналістів та медіа-професіоналів з технік виявлення фейкових новин, розпізнавання маніпуляцій і дотримання етичних стандартів.

Висновки до розділу 3

Поширення дезінформації є однією з найбільш актуальних та небезпечних проблем сучасного інформаційного середовища, яка здатна серйозно вплинути на політичну стабільність, громадську думку та міжнародні відносини. У контексті війни росії проти України ця проблема набуває особливого значення. РФ активно використовує інформаційну агресію як частину гібридної війни, зокрема через поширення дезінформації щодо подій в Україні, що має на меті маніпулювати громадською думкою, дискредитувати українську державність, а також посіяти розбіжності між Україною та міжнародними партнерами. Застосування сучасних інформаційних технологій, таких як соціальні мережі, фейкові новини, бот-мережі та інші інструменти, дозволяє досягати глобального охоплення та впливати на аудиторію в різних країнах.

Враховуючи зазначені приклади щодо поширення дезінформації у світовому інформаційному просторі щодо України з боку рф, нашій державі слід удосконалити наступні механізми протидії таким загрозам з метою ефективного функціонування національної системи інформаційної безпеки:

– Створення за ініціативою України разом з державами-партнерами міжнародного майданчика з питань протидії російській дезінформації. Така платформа буде максимально корисною не тільки для України, але й держав-партнерів, оскільки дозволить ефективно та швидко проводити комунікацію щодо усунення та спростування кремлівських наративів, пропаганди, фейків, дезінформації, які агресор поширює про Україну та партнерів через певні іноземні ЗМІ та організації, проросійських політиків-прибічників та партії.

Також миттєві консультації з партнерами щодо рішень про ведення жорстких санкцій для подібних осіб та організацій;

– Залучення національних та іноземних громадських організацій, журналістів до перевірки новин, створення прозорої системи для власних громадян, щоб вони могли перевіряти правдивість інформації перед тим, як поділитися нею. Також відкриття якомога більшої кількості представництв українських ЗМІ закордоном. При цьому активно співпрацювати з партнерами щодо припинення діяльності будь-яких так званих представництв російських пропагандистів закордоном;

– Розбудова ефективної системи контрпропаганди, яка передбачає:

а) створення та поширення позитивного інформаційного контенту, який не тільки відповідає на дезінформацію, але й активно просуває правду про Україну, її історію, культуру, політику, економічні досягнення та роль у міжнародних відносинах;

б) підтримка й розвиток офіційних урядових ресурсів, таких як сайт Міністерства інформаційної політики, на яких надаються достовірні й перевірені дані, а також інструменти для верифікації новин та фактів;

в) робота з міжнародними ЗМІ та інфлюенсерами для створення контенту, який висвітлює об’єктивну ситуацію в Україні, протидіє пропаганді росії та мобілізує міжнародну підтримку.

Медіаграмотність є важливим складником інформаційної безпеки та стратегічним елементом у сучасному глобалізованому світі, де інформація поширюється миттєво і впливає на суспільні настрої, політичні процеси та навіть національну безпеку. В умовах війни, особливо в контексті російської агресії проти України, медіаграмотність набуває особливої значущості. РФ активно використовує інформаційну та медійну зброю для маніпулювання громадською думкою, поширення дезінформації, пропаганди та створення альтернативних реальностей, що підривають внутрішню стабільність України та її міжнародну репутацію.

Українське суспільство стикається з масштабними інформаційними викликами, що включають як зовнішні загрози, так і внутрішні проблеми з інформаційною взаємодією. Одним з основних завдань національної безпеки є не лише захист від дезінформації ззовні, а й формування стійкості громадян до маніпуляцій та спотворених інформаційних наративів. Враховуючи масштаби інформаційної війни, в якій Україна є однією з головних мішеней, проблема медіаграмотності стає критично важливою для забезпечення єдності та національної безпеки.

Слід зазначити, що покращення рівня медіаграмотності українського суспільства є одним із найважливіших напрямків забезпечення інформаційної безпеки держави. З цією метою можна удосконалити наступні ініціативи, які допоможуть громадянам України адекватно оцінювати інформацію та запобігати маніпуляціям:

– Організація освітніх ініціатив для школярів та студентів, щоб навчити молодь правильно сприймати медіа-контент, виявляти фейки та перевіряти факти;

– Створення кампаній для широкої аудиторії, що будуть сприяти розвитку критичного мислення, заохочення до аналізу джерел інформації та використання перевірених ресурсів;

– Проведення тренінгів для журналістів та медіа-професіоналів з технік виявлення фейкових новин, розпізнавання маніпуляцій і дотримання етичних стандартів.

ВИСНОВКИ

У сучасному світі інформаційна безпека набуває вирішального значення, оскільки зростання цифрових технологій призводить до збільшення ризиків, пов'язаних з витоками даних, кіберзлочинністю та кібератаками. В умовах глобалізації та інтеграції інформаційних систем забезпечення конфіденційності, цілісності та доступності даних стає пріоритетом не тільки для бізнесу, а й для державних органів та приватних осіб. Атаки на інформаційні системи можуть мати серйозні наслідки, включаючи фінансові втрати, порушення репутації та навіть загрози національній безпеці. Тому забезпечення інформаційної безпеки є критично важливим для стабільного розвитку суспільства, зміцнюючи довіру до цифрових технологій та інновацій.

Аналізуючи зазначені у роботі підходи до поняття інформаційної безпеки, варто наголосити, що термін «інформаційна безпека» можна розглядати як стан захищеності інформаційного середовища, що забезпечує належний рівень захисту інформації на різних рівнях: особи, підприємства, суспільства або держави. Вона включає в себе комплекс заходів, які запобігають виникненню негативних наслідків, спричинених впливом несанкціонованих, умисних або неумисних маніпуляцій з інформацією. Інформаційна безпека має на меті захистити життєво важливі інтереси, інформаційну інфраструктуру та можливості розвитку суб'єктів (держава, суспільство, особистість), унеможливлюючи деструктивні інформаційні впливи, що можуть призвести до негативних наслідків на шляху стійкого розвитку.

Враховуючи підходи до визначення поняття «міжнародна інформаційна безпека», варто наголосити, що це комплексний стан глобальних інформаційних відносин, який забезпечує захищеність інформаційного середовища на світовому рівні, підтримуючи стабільність міжнародної системи. Вона охоплює сукупність заходів різного характеру (економічних, політичних, юридичних, організаційних), спрямованих на попередження загроз, забезпечення безпеки держав і міжнародної спільноти в інформаційному просторі. Міжнародна інформаційна безпека передбачає створення умов для

сталого розвитку держав і суспільств, а також захисту прав та інтересів осіб в інформаційній сфері, забезпечуючи при цьому недопущення порушень світової стабільності.

Сучасні загрози та виклики міжнародній інформаційній безпеці мають глобальний характер та охоплюють широкий спектр проблем, від кібератак до інформаційних війн. З розвитком цифрових технологій і зростанням залежності від Інтернету, країни та міжнародні організації стикаються з новими формами кіберзагроз, такими як хакерські атаки, фішинг, крадіжка персональних даних. Водночас, інформаційні війни, зокрема пропаганда, дезінформація та маніпуляції громадською думкою, стали важливим інструментом в міждержавних конфліктах, що призводить до ескалації напруги на міжнародній арені. Сучасні виклики також охоплюють питання етики та законодавства в контексті інформаційної безпеки, захисту прав людини в онлайн-середовищі та гарантування конфіденційності даних.

Отже, кожна держава, що є частиною глобального інформаційного простору, повинна розробити комплексну систему заходів для забезпечення власної інформаційної безпеки, яка включає:

– розробку законодавчих актів і нормативно-правових документів, які регулюють питання інформаційної безпеки, захисту даних і кібербезпеки;

– забезпечення безпеки ключових інформаційних і технологічних ресурсів держави, таких як енергетичні, фінансові та комунікаційні системи;

– розробку механізмів для боротьби з інформаційними маніпуляціями, фальшивими новинами та кібер-пропагандою;

– створення системи навчання і підвищення кваліфікації фахівців у галузі інформаційної безпеки, а також підвищення рівня обізнаності громадян щодо питань кібербезпеки;

– активну участь у міжнародних ініціативах і співпраця з іншими країнами для обміну інформацією та спільного реагування на глобальні кіберзагрози;

– створення ефективних систем для збереження та відновлення критичної інформації в разі кібератак або інших надзвичайних ситуацій.

Система інформаційної безпеки України є багатогранною і складається з кількох ключових елементів, які взаємодіють між собою для забезпечення ефективного захисту інформаційного середовища держави. Основними складовими цієї системи є державні органи, організації та установи, які відповідають за різні аспекти інформаційної безпеки, від технічного захисту інформації до протидії інформаційним загрозам. До основних органів, що беруть участь у забезпеченні інформаційної безпеки України, належать: Рада національної безпеки і оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Міністерство цифрової трансформації України та Національний центр кібербезпеки. Завдяки скоординованій діяльності цих органів забезпечується всебічний захист інформаційного середовища України, який включає як профілактику, так і оперативне реагування на інформаційні загрози, що виникають у різних сферах життя держави. Забезпечення інформаційної безпеки в умовах війни, економічної нестабільності та сучасних кіберзагроз є важливою складовою стратегії національної безпеки, що дозволяє Україні не тільки зберегти суверенітет, але й протистояти зовнішнім і внутрішнім викликам.

Таким чином, російська агресія виявилася не лише у воєнних діях на фронті, але й у масштабних інформаційних операціях, спрямованих на дестабілізацію внутрішньополітичної ситуації в Україні, підрив довіри до державних інститутів, маніпуляції громадською думкою та поширення дезінформації. На початкових етапах збройної агресії у 2014 році система інформаційної безпеки України виявилася недостатньо готовою до таких загроз, зокрема через відсутність єдиної стратегії боротьби з інформаційною агресією та недостатню координацію між державними органами. Важливим кроком стало створення спеціальних органів, таких як Кіберполіція та Рада національної безпеки і оборони України (РНБО), які взяли на себе координацію заходів з кіберзахисту та інформаційної безпеки, а також розробка нових

законодавчих актів у цій сфері. З початком повномасштабного вторгнення Росії в 2022 році, система інформаційної безпеки України зазнала значних змін та вдосконалень. Держава активно залучала міжнародних партнерів для боротьби з інформаційними загрозами, а також здійснила значний крок до зміцнення внутрішнього інформаційного простору. Протидія інформаційним атакам стала невід'ємною частиною національної безпеки, а забезпечення інформаційної безпеки стало критично важливим для стійкості державних інститутів та суспільства в цілому. Створення та удосконалення стратегій боротьби з інформаційними загрозами, активізація моніторингу інформаційних каналів та посилення кіберзахисту стали необхідними умовами для ефективної протидії російській інформаційній агресії. Збройна агресія РФ виявила вразливості в інформаційній безпеці України, але також стала каталізатором для розвитку ефективної системи інформаційного захисту. Враховуючи досвід боротьби з інформаційними загрозами в період з 2014 року, можна зробити висновок, що система інформаційної безпеки України значно покращилася і адаптувалася до нових реалій, проте залишаються актуальними питання удосконалення внутрішньої координації між органами влади та підвищення стійкості національної інформаційної інфраструктури.

Варто наголосити, що на сьогодні головними проблемами у забезпеченні інформаційної безпеки держави у контексті інформаційної агресії з боку так званої росії є:

– По-перше, поширення на міжнародній арені дезінформації, викривлених та упереджених фактів щодо України з боку росії, зокрема, залучаючи іноземні ЗМІ та організації, своїх поплічників, які готові заради грошей або з інших причин здійснювати різного роду "акції" в іноземних державах, проросійські політичні партії і кандидатів, здійснюючи фінансування кампаній і лобіювання інтересів.

– По-друге, важливим аспектом є медіаграмотність українського суспільства. Ця складова є важливою у забезпеченні інформаційної безпеки України, особливо в контексті війни росії проти України. Пропаганда та

дезінформація стали одними з основних інструментів гібридної війни, спрямованої на підрив морального духу, посів сумнівів серед населення та дестабілізацію ситуації в країні. Тому важливою проблемою є недостатній рівень медіаграмотності серед частини населення, що сприяє сприйняттю фейкових новин, маніпуляцій і пропаганди, а також труднощам у тому, щоб відрізнити достовірну інформацію від фальшивої.

Враховуючи зазначені приклади щодо поширення дезінформації у світовому інформаційному просторі щодо України з боку рф, нашій державі слід удосконалити наступні механізми протидії таким загрозам з метою ефективного функціонування національної системи інформаційної безпеки:

– Створення за ініціативою України разом з державами-партнерами міжнародного майданчика з питань протидії російській дезінформації. Така платформа буде максимально корисною не тільки для України, але й держав-партнерів, оскільки дозволить ефективно та швидко проводити комунікацію щодо усунення та спростування кремлівських наративів, пропаганди, фейків, дезінформації, які агресор поширює про Україну та партнерів через певні іноземні ЗМІ та організації, проросійських політиків-прибічників та партії. Також миттєві консультації з партнерами щодо рішень про ведення жорстких санкцій для подібних осіб та організацій;

– Розбудова ефективної системи контрпропаганди, яка передбачає:

а) створення та поширення позитивного інформаційного контенту, який не тільки відповідає на дезінформацію, але й активно просуває правду про Україну, її історію, культуру, політику, економічні досягнення та роль у міжнародних відносинах;

б) підтримка й розвиток офіційних урядових ресурсів, таких як сайт Міністерства інформаційної політики, на яких надаються достовірні й перевірені дані, а також інструменти для верифікації новин та фактів;

в) робота з міжнародними ЗМІ та інфлюенсерами для створення контенту, який висвітлює об’єктивну ситуацію в Україні, протидіє пропаганді росії та мобілізує міжнародну підтримку.

Українське суспільство стикається з масштабними інформаційними викликами, що включають як зовнішні загрози, так і внутрішні проблеми з інформаційною взаємодією. Одним з основних завдань національної безпеки є не лише захист від дезінформації ззовні, а й формування стійкості громадян до маніпуляцій та спотворених інформаційних наративів. Враховуючи масштаби інформаційної війни, в якій Україна є однією з головних мішеней, проблема медіаграмотності стає критично важливою для забезпечення єдності та національної безпеки.

Слід зазначити, що покращення рівня медіаграмотності українського суспільства є одним із найважливіших напрямків забезпечення інформаційної безпеки держави. З цією метою можна удосконалити наступні ініціативи, які допоможуть громадянам України адекватно оцінювати інформацію та запобігати маніпуляціям:

– Організація освітніх ініціатив для українського суспільства, щоб навчити правильно сприймати медіа-контент, виявляти фейки та перевіряти факти;

– Створення кампаній для широкої аудиторії, що будуть сприяти розвитку критичного мислення, заохочення до аналізу джерел інформації та використання перевірених ресурсів;

– Проведення тренінгів для журналістів та медіа-професіоналів з технік виявлення фейкових новин, розпізнавання маніпуляцій і дотримання етичних стандартів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Рижук О. Аналіз концепцій визначення «інформаційної безпеки» в умовах глобалізації. *Український науковий журнал «Освіта регіону». Політологія, Психологія, Комунікації.* 2016. № 4. С. 74–77.

2. Інформаційна безпека. URL: https://www.pharmencyclopedia.com.ua/article/8023/informacijna-bezpeka#:~:text=Information%20Security (дата звернення: 09.10.2024).

3. Бондаренко Р. В., Михальчук В. М. Інформаційна безпека держави. *Інвестиції: практика та досвід*. 2021. № 5. С. 95–101.

4. Кочубей Л. О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі). *Наукові записки.* 2015. № 3. С. 220–237.

5. Антонова С. Є., Мартинюк Г. Ф. Інформаційна безпека. *Державне управління: удосконалення та розвиток.* 2019. № 11.

6. Види, об'єкти та суб'єкти інформаційної безпеки. URL: https://studfile.net/preview/7435414/page:4/ (дата звернення: 10.10.2024).

7. Тимчук О. Г., Потапова Н. А. Принципи забезпечення інформаційної безпеки. *Прикладні аспекти сучасних міждисциплінарних досліджень*. 2022. № 2. С. 214–215.

8. Information Security: The Ultimate Guide. URL: https://www.imperva.com/learn/data-security/information-security-infosec/ (дата звернення: 11.10.2024).

9. Панченко О. А. Інформаційна безпека в контексті викликів і загроз національній безпеці. *Державне управління та місцеве самоврядування*. 2020. № 2. С. 57–63.

10. Міжнародна інформаційна безпека. URL: http://dspace.wunu.edu.ua/bitstream/316497/40666/1/274.pdf (дата звернення: 15.10.2024).

11. Сємко М.О. Нормотворча діяльність ООН щодо забезпечення інформаційної безпеки у воєнній сфері. *Юридичний науковий електронний журнал.* 2022. № 8. С. 580–583.

12. Політика міжнародних організацій з питань інформаційної безпеки. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/10/66.pdf (дата звернення: 17.10.2024).

13. Інформаційна безпека як стан. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/06/41-1.pdf (дата звернення: 17.10.2024).

14. Політико-правове регулювання сфери міжнародної інформаційної безпеки. URL: https://core.ac.uk/download/pdf/153580376.pdf (дата звернення: 18.10.2024).

15. Інформаційна безпека держави. URL: https://ir.stu.cn.ua/jspui/bitstream/123456789/21177/1/Інформаційна%20безпека%20держави..pdf (дата звернення: 18.10.2024).

16. Інформаційна війна. URL: https://vue.gov.ua/Інформаційна_війна#:~:text=Інформаційна%20війна%20(ІВ)%20—%20форма,та%20захисту%20власної%20безпеки%20інформаційної (дата звернення: 20.10.2024).

17. ЗМІ-Дезінформація-Безпека. Інформаційна війна. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf (дата звернення: 20.10.2024).

18. Війна інформаційна. URL: http://librarychl.kr.ua/kn_in/informatoria/inf-v.php (дата звернення: 21.10.2024).

19. Пахота Н. В. Інформаційні війни у сучасних міжнародних відносинах. *БІЗНЕСІНФОРМ.* 2022. № 1. С. 53–58.

20. Information Warfare: What and How? URL: https://www.cs.cmu.edu/~burnsm/InfoWarfare.html (дата звернення: 23.10.2024).

21. R. Białoskórski. The theoretical concept of information warfare: a general outline. *Humanities and Social Sciences.* 2023. Vol. 30, No. 4. P. 7–24.

22. Dzhus O. A. Key indicators of information warfare Russia against Ukraine. *Політична культура та ідеологія.* 2023. № 2. С. 83–88.

23. China's Media and Information Warfare. URL: https://www.cfr.org/article/chinas-media-and-information-warfare (дата звернення: 25.10.2024).

24. Iran's Information Warfare. URL: https://www.inss.org.il/wp-content/uploads/2019/10/Haiminis.pdf (дата звернення: 25.10.2024).

25. Копійка М. В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. *«ПОЛІТИЧНЕ ЖИТТЯ».* 2020. № 1. С. 102–109.

26. Cybersecurity community of practice. URL: https://unsceb.org/unissig (дата звернення: 27.10.2024).

27. Journal of security and sustainability issues. URL: https://www.researchgate.net/profile/Oleksii-Kostenko-3/publication/340441519_ORGANIZATIONAL_COMPETENCE_OF_NATO_INFORMATION_SECURITY_POLICY/links/603b4ebaa6fdcc37a8596ef7/ORGANIZATIONAL-COMPETENCE-OF-NATO-INFORMATION-SECURITY-POLICY.pdf?origin=publication_detail&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uRG93bmxvYWQiLCJwcmV2aW91c1BhZ2UiOiJwdWJsaWNhdGlvbiJ9fQ (дата звернення: 28.10.2024).

29. Яковлєв П. О. Досвід державного регулювання забезпечення інформаційної безпеки зарубіжних держав (на прикладі Сполучених Штатів Америки, Канади, Німеччини, Франції). *Серія «ПРАВО».* 2020. № 30. С. 106–113.

30. Фурсай О. Система забезпечення інформаційної безпеки Франції. *Вісник Львівського університету.* 2021. № 34. С. 222–227.

31. Denmark - National Cyber and Information Security Strategy 2022-2024. URL: https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/denmark-national-cyber-and-information-security (дата звернення: 01.11.2024).

32. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 02.11.2024).

33. Валюшко І. О. Інформаційна безпека України: трансформація законодавства після російського вторгнення. *Історико-політичні студії*. 2017. № 2. С. 30–43.

34. Лапінська Є. І. Основні питання законодавства України у сфері інформаційної безпеки. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*. 2019. № 39. С. 64–67.

35. Гур'єв В. І., Мехед Д. Б., Ткач Ю. М., Фірсова І. В. Інформаційна безпека держави : навч. посібн. Ніжин :ТПК «Орхідея», 2018. 166 с.

36. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 04.11.2024).

37. Захист інформаційного та кіберпросторі. URL: https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky (дата звернення: 04.11.2024).

38. Пересада О. М. Роль Національної поліції України в забезпеченні інформаційної безпеки держави: теоретико-методологічні аспекти. *Правовий часопис Донбасу.* 2019. № 4. С. 183–189.

39. Указ Президента України Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://www.president.gov.ua/documents/6852021-41069#:~:text=Стратегія%20інформаційної%20безпеки%20 (дата звернення: 05.11.2024).

40. Чому російська інформаційна отрута досі діє на Україну. URL: https://glavcom.ua/publications/hovorit-i-pokazyvaet-moskva-chomu-rosijska-informatsijna-otruta-dosi-dosjahaje-tsilej-v-ukrajini-969631.html (дата звернення: 06.11.2024).

41. Росія створює свій інформпростір на окупованих територіях України - британська розвідка. URL: https://suspilne.media/553379-rosia-stvorue-svij-informprostir-na-okupovanih-teritoriah-ukraini-britanska-rozvidka/ (дата звернення: 06.11.2024).

42. Інформація. URL: https://overallhorizon.org/?page_id=364 (дата звернення: 06.11.2024).

43. Концептуальні засади забезпечення державою інформаційної безпеки громадянина України. URL: https://dspace.kntu.kr.ua/server/api/core/bitstreams/be9e0824-b8c0-4312-b5db-289f6bb25187/content (дата звернення: 06.11.2024).

44. Analysis of Russia's information campaign against Ukraine. URL: https://stratcomcoe.org/cuploads/pfiles/russian_information_campaign_public_12012016fin.pdf (дата звернення: 07.11.2024).

45. Russian InformationWarfare of 2014. URL: https://www.ccdcoe.org/uploads/2018/10/Art-03-Russian-Information-Warfare-of-2014.pdf (дата звернення: 07.11.2024).

46. Інформаційна війна Російської Федерації проти України: оцінка міжнародного співтовариства. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/2115f2fc-7a32-4f79-a598-f476122c861c/content (дата звернення: 09.11.2024).

47. Що таке Наратив (Narrative)? URL: https://tseivo.com/b/jargoniist/t/3rvj6jkrzr#B-naratyvy-v-propahandi (дата звернення: 09.11.2024).

48. Близняк О. А., Гуменна К. М. Інструменти інформаційної війни росії проти України під час повномасштабного вторгнення 2022-2024 рр. *Політична культура та ідеологія.* 2024. № 2. С. 145–149.

49. путін майже годину висловлював своє бачення життя в Україні: фактчекінг звернення. URL: https://www.slovoidilo.ua/2022/02/22/stattja/polityka/putin-majzhe-hodynu-vyslovlyuvav-svoye-bachennya-zhyttya-ukrayini-faktchekinh-zvernennya (дата звернення: 10.11.2024).

50. 10 головних наративів російської пропаганди, що супроводжували напад на Україну. URL: https://www.rfi.fr/uk/міжнародні-новини/20230113-10-

головних-наративів-російської-пропаганди-що-супроводжували-напад-на-україну (дата звернення: 11.10.2024).

51. Шість найпоширеніших наративів російської пропаганди, які допомагають убивати українців. URL: https://www.ukrinform.ua/rubric-ato/3875878-sist-najposirenisih-narativiv-rosijskoi-propagandi-aki-dopomagaut-ubivati-ukrainciv.html (дата звернення: 11.10.2024).

52. Романишин А. М., Черевичний С. В., Остапчук О. П. та ін. 100 брехливих російських наративів про російсько-українську війну: збірник інформаційно-аналітичних матеріалів. Київ: НДЦ ГП ЗС України, 2023. 77 с.

53. Дезінформація: як розпізнати та боротися. URL: https://law.chnu.edu.ua/dezinformatsiia-yak-rozpiznaty-ta-borotysia/ (дата звернення: 12.11.2024).

54. Український наступ «надихнув» роспроп на фейки про «великі втрати» ЗСУ в Курській області. URL: https://www.ukrinform.ua/rubric-factcheck/3895514-ukrainskij-nastup-nadihnuv-rosprop-na-fejki-pro-veliki-vtrati-zsu-v-kurskij-oblasti.html (дата звернення: 12.11.2024).

55. Що таке ІПСО та як протидіяти? URL: https://tviykrok.com.ua/info/articles/shcho-take-ipso-ta-yak-protidiyati/ (дата звернення: 12.11.2024).

56. ІПСО - чому про них говорять та звідки взялися? URL: https://www.pravda.com.ua/columns/2024/10/4/7478120/ (дата звернення: 13.11.2024).

57. Що таке ІПСО та як росія використовує їх у війні проти України. URL: https://chas.news/current/scho-take-ipso-ta-yak-rosiya-vikoristovue-ih-u-viini-proti-ukraini (дата звернення: 13.11.2024).

58. РФ вбила полонених в Оленівці заради медійного ефекту - Оксана Мороз. URL: https://detector.media/infospace/article/201455/2022-07-30-rf-vbyla-polonenykh-v-olenivtsi-zarady-mediynogo-efektu-oksana-moroz/ (дата звернення: 15.11.2024).

59. Битва за громадську думку: як Україна воює з Росією на інформаційному фронті. URL: https://explainer.ua/bitva-za-gromadsku-dumku-yak-

ukrayina-voyuye-z-rosiyeyu-na-informatsijnomu-fronti/ (дата звернення: 15.11.2024).

60. Журналісти викрили діяльність з дезінформації агенції, яка працює на Кремль. URL: https://lb.ua/society/2024/09/16/635119_zhurnalisti_vikrili_diyalnist_z.html (дата звернення: 16.11.2024).

61. Росія поширює свої фейки через іноземні портали. URL: https://behindthenews.ua/pravda/rosiya-poshiryue-svoyi-feyki-cherez-inozemni-portali-724/ (дата звернення: 16.11.2024).

62. Європейські руки Путіна: як Росія впливає на громадську думку в ЄС. URL: https://espreso.tv/poyasnuemo-evropeyski-ruki-putina-yak-rosiya-vplivae-na-kraini-es#part-2 (дата звернення: 20.11.2024).

63. Тест з медіаграмотності пройшли вп'ятеро більше людей, аніж торік: результати проєкту. URL: https://shotam.info/test-iz-mediahramotnosti-proyshlo-vp-iatero-bilshe-liudey-anizh-torik-rezultaty-proiektu/ (дата звернення: 20.11.2024).

64. В Україні стартував тест із медіаграмотності: як долучитися та які призи. URL: https://suspilne.media/culture/859961-v-ukraini-startuvav-test-z-mediagramotnosti-ak-dolucitisa-ta-aki-prizi/ (дата звернення: 20.11.2024).

65. Національний тест з медіаграмотності: 20 тисяч учасників за дві години. URL: https://ms.detector.media/internet/post/36462/2024-10-17-natsionalnyy-test-z-mediagramotnosti-20-tysyach-uchasnykiv-za-dvi-godyny/ (дата звернення: 20.11.2024).

66. Кількість українців з високим індексом медіаграмотності знизилася за другий рік війни, - дослідження «Детектора медіа». URL: https://ms.detector.media/proekti-go-detektor-media/post/34730/2024-04-22-kilkist-ukraintsiv-z-vysokym-indeksom-mediagramotnosti-znyzylasya-za-drugyy-rik-viyny-doslidzhennya-detektora-media/ (дата звернення: 22.11.2024).

67. Christou G., Prokop M. Strategic Communications and Information Warfare in Ukraine. *International Politics Review*. 2020. Vol. 37, No. 1. P. 22–38.

68. Kucherenko I. Cybersecurity in the Context of Russia's Aggression: Ukraine's Response and Policy Recommendations. *International Journal of Cybersecurity*. 2022. Vol. 10, No. 2. P. 88–101.

69. Tucker P., Silver A. Fighting the Invisible Enemy: The Role of Social Media in Ukraine’s Information Security Strategy. *Global Cybersecurity Journal*. 2019. Vol. 12, No. 4. P. 112–128.

70. Hansen H. The Role of Media Literacy in Defending Ukraine Against Disinformation. *Journal of Media Ethics*. 2021. Vol. 36, No. 3. P. 227–245.