ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД

«УНІВЕРСИТЕТ ЕКОНОМІКИ ТА ПРАВА «КРОК»

Кафедра міжнародних відносин та журналістики

Спеціальність: 061 «Журналістика»

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«БЕЗПЕКОВИЙ КОНТЕНТ У СУЧАСНИХ ЗМК»

Студентка 4 курсу, групи Жур-20зн

Ткаченко Єлизавета Юріївна

Науковий керівник:

Завідувач кафедри МВЖ

Момот Неля Миколаївна

_____ _____ _____

(підпис студента) (дата) (підпис)

Попередній захист:

_____

(Висновок: «До захисту в Екзаменаційній комісії»)

Завідувач кафедри _____ Момот Н. М. _____

(підпис) (прізвище, ініціали) (дата)

Київ — 2024 рік

ЗМІСТ

ВСТУП

Безпека медіа включає в себе комплекс заходів, спрямованих на забезпечення безпеки інформаційного простору, зокрема, і захисту від кібератак та забезпечення прав людини і свободи слова. медіабезпека охоплює заходи щодо захисту від маніпуляційної інформації, фейків та недостовірних даних, а також визначення правил діяльності медіа з урахуванням етичних, професійних, та правових норм. Безпека медіа також означає створення умов для розвитку свободи медіа, де журналісти можуть працювати без перешкод і страху, а громадяни мають доступ до об'єктивної та достовірної інформації.

Актуальність теми. З появою Інтернету та соціальних мереж виникли нові проблемиі загрози у сфері інформаційної безпеки, зокрема, поширення фейкових новин, дезінформації, кібератаки на ЗМК та порушення особистої приватності користувачів. Розуміння та дослідження методів забезпечення безпекового контенту стає ключовим для збереження довіри громадськості до медіа та забезпечення безперешкодного доступу до об'єктивної та достовірної інформації. Дослідження цієї проблеми необхідне для розвитку стратегій та технологій, спрямованих на підвищення рівня безпеки інформаційного простору та забезпечення високих стандартів медіаетики і журналістики.

Мета роботи полягає у дослідженні специфіки формування безпекового контенту у сучасних вітчизняних засобах масової комунікації.

Реалізація поставленої мети зумовила вирішення наступних **завдань дослідження:**

– з'ясувати сутність поняття «інформаційна безпека» та його зв'язок із медіа;

– охарактеризувати стан наукової розробки досліджуваної проблеми;

– розглянути характеристику та напрями діяльності медіаресурсів «Детектор. Медіа» та Центру протидії дезінформації;

– означити методи та прийоми забезпечення якості та безпеки контенту у досліджуваних ЗМК;

– проаналізувати особливості медіаосвіти як інструменту захисту від дезінформаційного впливу країни-агресора в умовах гібридної війни;

– сформувати уявлення про міжнародний досвід захисту медійного контенту від кіберзагроз.

Об'єктом дослідження є інформаційна безпека ЗМК в умовах сучасного розвитку медіапростору.

Предметом дослідження виступає аналіз стратегій та методів захисту медіаресурсів від інформаційних загроз.

Серед **методів дослідження**, які застосовувались при підготовці дипломної роботи, можна виділити наступні: аналітико-синтетичної обробки інформації (використано при дослідженні сутності поняття «інформаційна безпека» та його взаємозв'язку з медіа), узагальнення (за допомогою цього методу розкрито основні напрями діяльності медіаресурсів «Детектор. Медіа» та Центру протидії дезінформації), систематизація (даний метод дозволив означити методи та прийоми захисту медійного контенту від кіберзагроз у світовому інформаційному просторі).

Наукова новизна дипломної роботи полягає у комплексному аналізі та систематизації теоретичного матеріалу щодо проблеми формування безпекового контенту у сучасних ЗМК. На основі теоретичного матеріалу було також сформовано практичний кейс методів та прийомів забезпечення якості медійного контенту на основі аналізу медіаресурсів «Детектор. Медіа» та Центру протидії дезінформації.

Практичне значення результатів дослідження. Матеріали дипломної роботи можуть стати основою для створення навчальних курсів та матеріалів, що допоможуть користувачам відрізняти достовірну інформацію від маніпулятивного контенту. Також це дослідження може бути корисним для здобувачів освіти, які готують аналітичні та наукові матеріали у сфері медіа, дозволяючи їм краще розуміти та аналізувати сучасний медіапростір. Крім того, зацікавленим громадянам, які бажають підвищити свій рівень знань у сфері

захисту від маніпулятивного контенту, ці матеріали можуть надати важливу інформацію та інструменти для безпечного користування медіаресурсами.

Структура дипломної роботи складається зі вступу, трьох розділів, висновків та списку використаних джерел. Загальний обсяг роботи становить – 59 сторінок, список використаних джерел нараховує 63 найменування.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ПРОБЛЕМИ БЕЗПЕКОВОГО КОНТЕНТУ У СУЧАСНИХ ЗМІ

1.1. **Поняття «інформаційна безпека», його зв’язок із медіа**.

Інформаційна безпека стає все більш актуальною в умовах сучасного цифрового світу, де обмін інформацією відіграє ключову роль у всіх сферах життя. Поняття інформаційної безпеки на сьогоднішній день є надзвичайно важливим як для держав, так і для бізнесу, суспільства та кожного окремого користувача. У зв’язку з цим розуміння функцій та складових інформаційної безпеки стає ключовим завданням для забезпечення ефективного захисту інформації та збереження довіри до цифрового середовища.

Закон України «Про національну безпеку України» визначає інформаційну безпеку як ключову складову національної безпеки, що гарантує захищеність життєво важливих інтересів людини, громадянина, суспільства і держави. Це охоплює широкий спектр аспектів, включаючи сталий розвиток суспільства, запобігання та нейтралізацію реальних та потенційних загроз національним інтересам у сферах правоохоронної діяльності, боротьби з корупцією, прикордонної діяльності, оборони, міграційної політики, охорони здоров’я, освіти та науки, науково-технічної та інноваційної політики, а також забезпечення свободи слова та інформаційної безпеки [47].

Інформаційна безпека України – це один з аспектів національної безпеки, який є важливою функцією держави. Ця сфера включає:

– Розроблення законодавства щодо державної інформаційної політики.

– Забезпечення можливостей для досягнення достатнього рівня інформації для ухвалення рішень державними органами, громадянами, об'єднаннями громадян та іншими суб'єктами права в Україні відповідно до законодавства.

– Гарантування свободи інформаційної діяльності та права на доступ до інформації в національному інформаційному просторі України.

– Постійний розвиток інформаційної структури.

– Підтримка розвитку національних інформаційних ресурсів з урахуванням досягнень науки і техніки, а також особливостей духовно-культурного життя народу України.

– Впровадження безпечних інформаційних технологій.

– Захист прав держави на стратегічні об’єкти інформаційної інфраструктури.

– Охорона державної таємниці та інформації з обмеженим доступом, що є об’єктом права власності або тільки володіння, користування або розпорядження державою [25, с. 113].

У XXI столітті інформаційна безпека стає пріоритетним напрямом у національній безпеці держави, що дозволяє їй здійснювати лідерство в економічних, військово-політичних та інших сферах. Це дає можливість мати стратегічні і тактичні переваги, управляти економічними витратами на розвиток збройних сил і техніки, підтримувати перевагу в передових технологіях, особливо в інформаційному сегменті. Впродовж останніх десятиліть сформувалась тенденція, що докорінно ослабити державу можна не лише військовим шляхом, але і через використання тактик квазі-зброї, до якої належить інформаційний вплив, економічні санкції, фінансові атаки тощо. Інформаційна боротьба часто виявляється ефективнішою, ніж інші методи дії [4, с. 43].

На думку О. Крюкова, інформаційна безпека представляє собою комплекс суспільних правовідносин, спрямованих на організацію процесів створення, підтримки, захисту та забезпечення необхідних умов безпеки для особи (як фізичної або юридичної особи, установи, підприємства чи організації), а також для суспільства і держави в цілому. Ці правовідносини пов’язані з організацією технологій, які стосуються створення, поширення, зберігання та використання інформації (включаючи дані, знання) для забезпечення функціонування та розвитку інформаційних ресурсів людини, суспільства та держави [22].

На основі запропонованих можна сформувати власну дефініцію поняття «інформаційна безпека». На наш погляд, це система заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, яка є важливою для організації, держави чи особи. Вона створюється для захисту інформації від несанкціонованого доступу, руйнування, зміни або розголошення. Інформаційна безпека має важливе значення як для захисту конфіденційної інформації, так і для забезпечення надійності та безперебійності роботи інформаційних систем.

Основною змістовною характеристикою визначень поняття «інформаційна безпека», які сьогодні пропонує переважна більшість науковців та український законодавець, є «захищеність». Однак, автори підтримують думку В. Полевого про те, що забезпечення вказаних інтересів вимагає не стільки захисту, скільки створення умов для їх реалізації та розвитку [44, с. 45]. Зокрема, будь-які спроби захистити вітчизняний інформаційний простір від неякісного продукту шляхом введення заборон на його розповсюдження завжди призводило до звинувачень у цензурі, в обмеженні прав доступу громадян до інформації, і, як наслідок, лише викликало інтерес до «забороненого плоду». Всепроникна здатність інформації та пов’язаних з нею процесів зводить нанівець будь-які заходи заборон і обмежень. У той же час, вирішити проблему може власний конкурентноздатний інформаційний продукт [26, с. 125].

Стрімкий розвиток інформатизації привів до появи нових видів злочинів, таких як комп’ютерна злочинність і комп’ютерний тероризм. Як нове і недостатньо вивчене злочинне явище, кібертероризм заслуговує на окрему увагу і вимагає особливого підходу до вирішення цієї, небезпечної для людства, проблеми. Особливе занепокоєння у правоохоронних органів викликають терористичні акти, пов’язані з використанням глобальної мережі Інтернет, з відкритих джерел якої можна отримати технологію виготовлення біологічної, хімічної і навіть ядерної зброї терористів. Зламуючи сайти, кібертерористи отримують доступ до різної інформації, зокрема секретної [19, с. 394].

Кібертероризм є складним явищем, яке постає внаслідок безконтрольного використання глобальних мереж, недостатньої уваги з боку держави, громадянського суспільства і спецслужб до цього сегменту інформаційного простору. Він проявляється через атаки на комп'ютери, комп'ютерні програми та мережі, а також розміщену в них інформацію, з метою створення атмосфери страху та безпорадності в суспільстві з метою досягнення цілей і інтересів суб'єктів терористичної діяльності. Це вимагає об'єднання зусиль світової спільноти для ефективної протидії цьому явищу [5, с. 107].

Кібертероризм чітко відрізняється від інших злочинів в кіберпросторі, в першу чергу в його цілях, які є загальними для політичного тероризму в цілому. Кібертерорист як суб'єкт злочину також істотно відрізняється від хакера, комп'ютерного хулігана чи комп'ютерного злодія, чиї дії обумовлені жадібністю або хуліганством.

Основна тактика кібертероризму полягає у забезпеченні того, щоб конкретний кіберзлочин мав небезпечні наслідки, широкий громадський резонанс і створював атмосферу постійної загрози повторення, не визначивши конкретну мету. Кібертероризм орієнтований на використання різних форм і методів вимкнення інформаційної інфраструктури держави або використання інформаційної інфраструктури для виникнення ситуації, що створює катастрофічні наслідки для суспільства [24, с. 23].

Так, О. О. Климчук розглядає кібератаку як вид інформаційної операції, форму її активної реалізації у кіберпросторі. На його думку, кібератака полягає у діях із застосуванням апаратно-програмних засобів, спрямованих на використання, спотворення, підміну або знищення інформації, що міститься в базах даних комп'ютерів і інформаційних мережах, а також на зниження ефективності функціонування або виведення з ладу самих комп'ютерів і комп'ютерних мереж [20, с. 31].

Кібератаки можуть бути спрямовані проти конкретних цілей і виконуватися з урахуванням приховання слідів активності на всіх етапах. Таргетована кібератака є тривалим процесом несанкціонованої активності

кіберзлочинців, спрямованим на конкретний об’єкт критичної інфраструктури. Метою таких атак є подолання механізмів забезпечення безпеки та завдання різних видів збитку, включаючи фізичний, інформаційний, моральний тощо. Цей процес керується організованою професійною групою кіберзлочинців, які мають доступ до потужних апаратно-програмних засобів і діють у реальному часі [2, с. 46].

Збиток від кібертерористичних дій в основному пов’ язаний з людськими жертвами або матеріальними втратами, викликаними знищенням елементів інфраструктури; з можливими втратами від несанкціонованого використання інформації з високим рівнем секретності або інфраструктури управління в життєво важливих для держави сферах діяльності; з витратами на відновлення мереж. Відповідно, кібертероризм надає цілий ряд серйозних викликів громадськості. По-перше, кібератаку важко прогнозувати або відстежити в реальному часі, вона може початися в будь-який час, в країні або за кордоном, і стояти за нею може хто завгодно; потрібні значні ресурси, щоб визначити, хто несе за це відповідальність. По-друге, через складність законів, що діють у всьому світі, переслідування за законом, пошук, захоплення і видача окремих осіб представляються проблематичними.

Можна констатувати, що загроза кібертероризму в даний час є дуже складною і актуальною проблемою, причому вона буде посилюватися із розвитком технологій. Зловмисники діють без кордонів. Їх атаки провокують виникнення глобальних криз в економіці та дипломатичних відносинах між багатьма країнами [2, с. 47].

У сучасному світі роль медіа у забезпеченні інформаційної безпеки набуває особливої ваги, оскільки інформаційний простір перетворюється на арену геополітичних і соціальних протистоянь. З розвитком цифрових технологій і всеохоплюючого впливу Інтернету, медіа стають важливим засобом формування громадської думки, впливу на політичні процеси та соціальну стабільність. Вони не лише поширюють інформацію, але й активно формують сприйняття реальності, впливаючи на рішення та поведінку громадян. У цьому

контексті розуміння механізмів і наслідків діяльності медіа є ключовим для забезпечення національної та міжнародної безпеки.

Інформаційні війни, дезінформація, пропаганда – ці феномени стали звичайною частиною сучасного інформаційного простору. Уміння критично оцінювати інформацію, розуміння ролі медіа у формуванні соціальних наративів і здатність протистояти маніпуляціям стають необхідними навичками для кожного свідомого громадянина. З іншого боку, це ставить перед державою завдання розробки ефективних стратегій інформаційної безпеки, зокрема не тільки правові та технічні заходи, але й освітні програми, спрямовані на розвиток медіаграмотності. Особливий акцент слід зробити на ефективних системах соціально-психологічного захисту на рівні суспільства загалом. Традиційні механізми захисту або руйнуються під впливом сучасних маніпулятивних технологій, або не встигають адаптуватися до нових обставин. Сучасні маніпулятивні технології мають значний вплив нарізні сфери суспільства, включаючи політику. Важливо знайти способи забезпечення належної якості інформації, зокрема шляхом розвитку медіаграмотності в суспільстві, підвищення відповідальності медіа за поширення недостовірної інформації, та водночас запобігання цензурі й обмеженню плюралізму поглядів [14, с. 31].

Засоби масової інформації, спрямовані на широку аудиторію, мають важливу роль у забезпеченні масово-інформаційної безпеки (МІБ). Їх завдання полягає в доставці необхідних інформаційних ресурсів для прийняття рішень споживачами, а також у захисті від маніпулятивної дезінформації, яка може поширюватися через ці самі засоби масової інформації.

Масово-інформаційна безпека значною мірою залежить від того, як в суспільстві встановлений інформаційний порядок, який забезпечує максимальний рівень інформаційної підтримки демократії шляхом всебічної інформованості громадян [10, с. 86].

Для того щоб громадянин був достатньо інформованим для прийняття та реалізації максимально обґрунтованого рішення:

– По-перше, від ЗМІ очікується активна робота з усіма аспектами масової свідомості, включаючи світогляд, світобачення, історичну свідомість та громадську думку.

– По-друге, інформування має враховувати об’єктивні потреби кожної соціальної групи та соціального шару, а також відмінності в їх уявленнях, поглядах та настроях.

– По-третє, важливо враховувати поняття суспільства як системно організованої цілісності, де кожна група функціонує лише у взаємозв’язку з іншими групами та в органічному зв’язку з ними [40, с. 253].

Отже, інформаційна безпека – це захист інформації та інформаційних систем від несанкціонованого доступу, використання, розголошення, зміни чи знищення. Інформаційна безпека у ЗМІ відіграє ключову роль, оскільки медіа є одним із головних каналів розповсюдження інформації. Кібератаки часто спрямовані саме на медійний простір, що може призвести до витоку конфіденційної інформації, фальсифікації новин і поширення дезінформації. Важливо, щоб медіаорганізації впроваджували суворі заходи безпеки, аби забезпечити цілісність та автентичність розповсюджуваної інформації. Крім того, заходи інформаційної безпеки допомагають зберегти довіру суспільства, яка є вирішальною для медійних інститутів. Забезпечення інформаційної безпеки в медіа сприяє захисту інформаційному простору та мінімізує вплив маніпулятивних технологій та дезінформації на громадськість.

1.2. **Стан наукової розробки теми**.

Аналіз безпекового контенту в сучасних засобах масової комунікації є важливою темою дослідження у вітчизняній науці, зосереджуючись на створенні та впровадженні стандартів безпеки, які забезпечують захист інформації. Важливим аспектом є розробка методів шифрування, систем аутентифікації та механізмів контролю доступу. Регуляторні механізми медіа впливають на вимоги до збереження та обробки персональних даних, підвищуючи вимоги до конфіденційності та безпеки. Наукові дослідження також звертають увагу на

розробку інструментів для моніторингу та виявлення кіберзагроз, що дозволяє медіаорганізаціям оперативно реагувати на кіберзагрози.

Стаття Р. Бараненко «Кібератаки як одна з форм кібертероризму» [2] зосереджує увагу на обговоренні заходів протидії кібератакам, розглядаючи їх як прояви кібертероризму в рамках національної та міжнародної кібербезпеки. Особлива увага приділена використанню інформаційного простору злочинцями та терористами, що призводить до таких явищ, як кіберзлочинність та кібертероризм. Підкреслюється, що кібертерористи можуть загрожувати значній кількості людей, не беручи безпосередньо участь у терористичних діях, оскільки діють з безпечних місць. В статті визначено ключові заходи кібербезпеки, проаналізовано сутність кібертероризму, його складові та методи проведення атак. Також наведено цілі, які терористичні групи досягають за допомогою інтернету і сучасних технологій, і розглянуто різні рівні можливостей кібертерористичних актів, з особливим акцентом на стратегії проведення кібератак типу «Kill Chain» та DoS-атаки. Висвітлено проблему ідентифікації джерела кібератаки.

У роботі Я. Бєлошевич «Інформаційна безпека України в сучасних умовах» [4] детально аналізуються ключові аспекти інформаційної безпеки держави, освітлюючи, як процеси глобалізації впливають на інформатизацію суспільства. Глобалізація прискорює обмін інформацією між країнами, тим самим підвищуючи вразливість перед зовнішніми загрозами і втручаннями. В цьому контексті розглядаються основні тенденції та виклики, які виникають перед Україною в умовах розширення цифрового простору і збільшення залежності від цифрових технологій. Особливу увагу приділено аналізу недавніх конфліктів та інформаційних загроз, які ставлять під сумнів стабільність та безпеку інформаційного простору країни.

Досліджується роль інформації як стратегічного ресурсу в сучасному світі, що визначає політичні, економічні та соціальні процеси на глобальному рівні. Інформація, будучи невичерпним ресурсом, займає центральне місце в стратегіях розвитку багатьох держав. У контексті цифрової ери інформаційна

безпека стає вирішальною для забезпечення стійкості держав до зовнішніх і внутрішніх викликів. У статті підкреслюється важливість розуміння сучасних характеристик інформаційного простору та здатності адаптуватися до швидких змін в глобалізованому світі.

З. Гой та Ю. Білявська у науковому доробку «Медіаосвіта як засіб протистояння гібридним загрозам» [9] досліджують роль медіаосвіти у плані протистояння гібридним загрозам в сучасному інформаційному середовищі. Основним завданням статті є аналіз ефективності медіаосвіти як інструменту відповіді на складні гібридні загрози, які включають інформаційну маніпуляцію, дезінформацію, та інші маніпулятивні практики. Розглядаються підходи та стратегії використання медіаосвіти для підвищення інформаційної грамотності та розвитку критичного мислення серед громадян, що є ключовим для збереження демократичних цінностей та стійкості суспільства перед гібридними загрозами.

Робота відстежує вплив медіаосвіти на формування відповідальної громадянської позиції та активної участі у демократичних процесах, спрямованих на протидію гібридним загрозам. Автори статті звертають увагу на значення партнерства між урядовими та громадськими організаціями у впровадженні програм медіаосвіти, які сприяють не лише інформаційній грамотності, але й формуванню відповідальності за власні дії в медіапросторі.

А. Головка у праці «Діяльність сучасних ЗМІ в контексті інформаційної безпеки України» [10] розглядає роль сучасних ЗМІ в забезпеченні інформаційної безпеки України в умовах сучасних викликів та загроз. Зокрема, досліджується вплив медіа на формування громадської думки та відносин у суспільстві з урахуванням інформаційно-психологічної війни та дезінформації. Автор статті аналізує різноманітні підходи та стратегії, які використовують ЗМІ для збільшення інформованості громадськості та зміцнення інформаційної безпеки, включаючи розробку професійних стандартів, підвищення інформаційної грамотності, та реагування на маніпулятивні дії.

Робота також висвітлює важливість співпраці між ЗМІ, урядовими структурами та громадськістю у сфері інформаційної безпеки. Особлива увага приділяється ролі ЗМІ у виявленні та розкритті штучно створених інформаційних загроз, а також сприянню висвітленню правдивої інформації та захисту від маніпуляцій. Вчений аналізує проблеми, з якими стикаються сучасні ЗМІ у сфері забезпечення інформаційної безпеки та робить висновки щодо шляхів покращення діяльності медіа для забезпечення національної безпеки.

Стаття К. Захаренка та Є. Міненка на тему «Інститут медіа як суб'єкт інформаційної безпеки» [14] аналізує роль ЗМІ у сфері інформаційної безпеки, зокрема в контексті розвитку інформаційного суспільства та умов воєнного стану. Засоби масової інформації стають ключовим каналом для формування громадських думок та переконань, особливо в умовах гібридних військових конфліктів, де їх вплив може бути вирішальним у передачі правдивої інформації та захисті від дезінформації. Інформаційна війна виявляється важливим аспектом таких конфліктів, підкреслюючи необхідність етичного та правового регулювання діяльності медіа в кризових ситуаціях.

Основна наукова цінність статті полягає у новому погляді на роль ЗМІ в інформаційному просторі, враховуючи вплив цифрових медіа та соціальних мереж на поширення інформації та її сприйняття. Також важливим є поєднання різних наукових підходів для аналізу взаємодії медіа та інформаційної безпеки, що дає можливість краще розуміти динаміку і вплив цих процесів на сучасне суспільство, особливо в умовах поширення дезінформації та інформаційних маніпуляцій.

Стаття «Регулювання діяльності засобів масової інформації: міжнародні принципи та європейський досвід» [16] Н. Ільченко та Л. Безуглої присвячена аналізу принципів та стратегій координації політики у сфері телерадіомовлення між Європейським Союзом та Радою Європи. Основна увага зосереджена на вивченні ролі цих міжнародних організацій у встановленні стандартів та норм для регулювання мовлення в Європі, зокрема з урахуванням культурної та мовної різноманітності регіонів. Досліджується взаємодія між національними

системами регулювання мовлення та європейськими структурами з метою забезпечення високих стандартів якості та культурного розвитку у сфері медіа.

Досить важливим є і дослідження національних систем регулювання мовлення в Європі. Автори розглядають різноманітні підходи та методики регулювання мовлення в країнах Європейського Союзу, зокрема, культурного різноманіття та мовної політики. Висвітлюються основні проблеми та тенденції у цій сфері з урахуванням сучасних технологічних змін та впливу глобалізації на медіаландшафт Європи.

О. Климчук у роботі «Кіберпростір як нова арена воєнних дій» [20] аналізує роль кіберпростору як нової арени для воєнних дій у сучасному світі. Основна увага приділена вивченню технологічних аспектів кібернетичних загроз та військових стратегій, що використовуються в цьому контексті. Автор розглядає еволюцію кібервійськ та їх вплив на безпеку країн та міжнародні відносини, зокрема у контексті розвитку технологій та кіберзброї.

Дослідник також висвітлює питання захисту кіберпростору та стратегії протидії кібератакам. Автор досліджує методи та засоби кіберзахисту, як-от роль кіберстратегій в національній та міжнародній безпеці. Зокрема, аналізується співробітництво між країнами, міжнародні ініціативи та правові аспекти в цій сфері з метою ефективного захисту кіберпростору від потенційних загроз.

О. Крюков у праці «Інформаційна безпека держави в умовах глобалізації» [22] зосереджується на аналізі питань інформаційної безпеки держави в контексті глобалізації. Автор досліджує сучасні виклики та загрози, що виникають у зв'язку з швидким розвитком технологій та зростанням обсягів обміну інформацією між країнами та регіонами. Особлива увага приділяється аналізу інформаційних загроз: як кібератаки, дезінформація та кібершпигунство, а також їх потенційній шкоді для національної безпеки.

У статті також висвітлюються шляхи подолання інформаційних загроз в сучасних умовах глобалізації. Автор розглядає різні стратегії та підходи до захисту інформаційної безпеки, включаючи розвиток кіберзахисту, підвищення інформаційної грамотності суспільства та міжнародне співробітництво у сфері

кібербезпеки. Також досліджено ефективність інформаційно-правових механізмів регулювання та захисту цінної інформації як одного з ключових ресурсів сучасної держави.

Стаття З. Кукіної «Правове регулювання діяльності засобів масової інформації в Європейському Союзі» [23] присвячена науковому аналізу європейського законодавства, яке визначає правила та умови діяльності засобів масової інформації. Основним об'єктом дослідження є розгляд основних правових механізмів Європейського Союзу, що стосуються регулювання медіа-сфери. Автори звертають увагу на ключові аспекти такого законодавства, як свобода слова, регулювання власності засобів масової інформації, контроль за рекламою та захист інформаційної приватності.

Головна мета статті – аналіз правових норм ЄС у контексті їх подальшої гармонізації з українським законодавством. Авторка аналізує перспективи та можливості впровадження європейських стандартів українськими законодавцями з метою зближення української правової системи з правовими стандартами ЄС у сфері медіа-регулювання.

У статті Г. Нерсесян «Медіаграмотність молоді – запорука протидії інформаційній агресії» [36] зазначено, що у ситуації, коли Росія активно розповсюджує деструктивну інформаційно-психологічну пропаганду щодо України, важливо, щоб суспільство було освіченим і грамотним у питаннях інформаційної культури. Вміння розрізняти правду від брехні стає ключовим, оскільки маніпуляції та спотворення фактів створюють несприятливу атмосферу для формування образу України та маніпулювання громадською думкою.

Особливу увагу слід звернути на молоде покоління, яке є активним учасником суспільних процесів і відіграє важливу роль у формуванні медіапростору. Забезпечення їхньої медіаграмотності, критичного мислення та здатності аналізувати інформацію є ключовим завданням для протистояння інформаційній агресії та маніпуляціям. Соціологічні дослідження підтверджують, що молодь часто звертається до соціальних мереж для

отримання інформації, тому важливо зробити акцент на їхній медіаосвіті та вмінні критично оцінювати отриману інформацію.

У статті І. Новосельського «Політико-правові засади функціонування нових медіа: світовий досвід та Україна» [38] проаналізовано законодавчий досвід у сфері регулювання онлайн-медіа на світовому рівні. Виявлено, що рішення щодо правового забезпечення діяльності медіа включає створення спеціальних норм для електронних медіа та розробку механізмів саморегуляції в Інтернеті. Спостерігається відмінність міжнародних моделей регулювання медіа: «східна» модель передбачає домінантний контроль держави, тоді як «західна» модель ставить акцент на баланс між державним контролем і саморегуляцією. Україна має суперечливе правове середовище для медіа, що потребує узгодження із європейськими стандартами та розвитку механізмів захисту медіапростору та інформаційної безпеки.

О. Панченко у роботі «Засоби масової інформації як джерело інформаційної безпеки» [40] зазначає, що засоби масової інформації, як ключовий елемент масової комунікації, активно впливають на формування громадської думки, культури та світогляду. Цей вплив, що виникає з інформаційного середовища, має як конструктивні, так і деструктивні аспекти. Відтак, оцінка його корисності, нейтральності або шкідливості часто стає предметом суперечок через турбулентність та невизначеність самого середовища. Зони турбулентності відзначаються нестабільністю, яка за умов навіть найменших негативних впливів може призвести до дисбалансу та хаосу, якщо не приймати необхідних заходів протидії.

Особливо важливою є проблема інформаційної безпеки в контексті загальної безпеки держави. Засоби масової інформації повинні виступати як захисниками масово-інформаційної безпеки, забезпечуючи не лише доступ до необхідної інформації для прийняття обґрунтованих рішень, але й захищаючи від маніпулятивної дезінформації. Від їхньої діяльності значною мірою залежать зміни в суспільстві. Таким чином, створення ефективних систем інформаційної безпеки вже є актуальною проблемою, яка вимагає комплексного підходу і

взаємодії з органами державної влади для забезпечення стабільного розвитку та захисту прав і інтересів суб'єктів інформації.

Є. Перегуда у праці «Медіаосвіта в умовах суспільної стабільності та в умовах війни» [41] розглядає роль медіаосвіти як важливого чинника у забезпеченні суспільної стабільності і в умовах конфлікту та війни. Основна мета дослідження полягає в аналізі ефективності освітніх програм у галузі розвитку критичного мислення та інформаційної грамотності серед громадян. Автор дослідження розглядає динаміку та вплив медіаосвіти на формування відповідального сприйняття інформації та здатність аналізувати та розрізняти факти в умовах психологічних загроз, характерних для воєнного часу.

В статті також досліджується вплив медіа на формування суспільних уявлень та стереотипів в умовах війни, а також ефективність медіаосвітніх заходів у запобіганні дезінформації та маніпуляційних впливів на громадян. Аналізується також роль медіаосвіти у підтримці громадського діалогу та сприянні конструктивному розв'язанню конфліктів, спрямований на покращення інформаційної обізнаності та розуміння суспільних процесів, які стають особливо актуальними в умовах соціальної нестабільності та воєнного стану.

Медіаграмотність, як важлива складова інформаційної безпеки, є предметом обговорення у статті І. Солдатенко та А. Зінюк «Медіаграмотність як складова інформаційної безпеки» [51]. Досліджено вплив медіаграмотності на забезпечення безпеки інформаційного середовища в умовах суспільної стабільності та війни. Стаття аналізує рівень медіаграмотності населення, його здатність критично оцінювати інформацію, розрізняти факти від маніпуляцій та розпізнавати загрози інформаційної безпеки. Особлива увага приділена ролі медіаграмотності у підвищенні свідомості громадян щодо ризиків інформаційних загроз у сучасному цифровому середовищі.

У контексті суспільної стабільності та війни, стаття розглядає, як медіаграмотність може стати ефективним інструментом запобігання дезінформації, впливу пропаганди та маніпуляційних технік на громадян. Досліджуються основні принципи та методи навчання медіаграмотності,

спрямовані на формування критичного мислення та уміння аналізувати інформацію з різних джерел. Результати дослідження можуть допомогти в розробці стратегій підвищення рівня медіаграмотності серед населення як в умовах мирного часу, так і під час воєнного стану.

О. Фролова у науковому доробку на тему «Міжнародне співробітництво в галузі забезпечення інформаційної безпеки» [55] стверджує, що загрози, що стосуються інформаційної безпеки, є однією з найбільш серйозних проблем у сучасному світі. Ця проблема розглядається як стратегічно важлива через свій транскордонний характер, що вимагає тісної співпраці між країнами. Міжнародні актори визнали, що лише спільними зусиллями, заснованими на міжнародному праві, можна вирішити ці проблеми в різних сферах життя суспільства.

Ефективність співпраці особливо вирізняється в рамках міжнародних організацій, які мають потужний потенціал для протидії загрозам в інформаційній сфері. Міжнародна спільнота через механізми таких організацій формує бажання до масштабного співробітництва, об’єднання зусиль, взаємодії та відповідальності у вирішенні спільних проблем безпеки світу. Детальне обговорення цієї теми розкрите в статті, яка досліджує міжнародне співробітництво в галузі забезпечення інформаційної безпеки через роботу з такими організаціями як Організація Об’єднаних націй, Організація Північноатлантичного Договору та Європейський Союз.

Можна зробити висновок, що дослідження теми безпекового контенту у сучасних ЗМК свідчить про актуальність проблеми та значний інтерес до неї у науковому середовищі. Дослідження у цій галузі зосереджене на вивченні поняття безпекового контенту, його впливу на аудиторію та методах забезпечення безпеки в медіа. Станом на сьогодні було проведено значну кількість досліджень, які демонструють різноманітні аспекти цієї проблематики, зокрема, аналіз ризиків, визначення критеріїв безпеки контенту та розробку методів фільтрації та контролю медіапростору.

РОЗДІЛ 2
БЕЗПЕКА МЕДІЙНОГО КОНТЕНТУ ЯК КЛЮЧОВА УМОВА ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ (на прикладі медіаресурсів «Детектор.медіа» та Центру протидії дезінформації)

2.1. **Характеристика та напрями діяльності медіаресурсів «Детектор.медіа» та Центру протидії дезінформації.**

В сучасному інформаційному середовищі безпека медійного контенту набуває особливого значення, зокрема, і як ключова умова забезпечення інформаційної безпеки держави. Особливу роль у плані забезпечення інформаційної безпеки відіграють медіаресурси, як-от «Детектор.медіа» та Центр протидії дезінформації, які ми обрали для дослідження цієї теми.

В Україні на сьогоднішній день однією з найвпливовіших організацій у сфері медіаосвіти є громадська організація «Детектор Медіа», яка була заснована українськими журналістами на початку 2004 року. Колектив ГО, що включає талановитих, креативних та визначених фахівців, визначає три основні напрямки своєї діяльності: поліпшення якості українських ЗМІ, підвищення рівня медіаграмотності серед громадян та боротьба з дезінформацією та маніпулятивними новинами. «Детектор Медіа» впроваджує різноманітні медіаосвітні ініціативи: проекти «Суспільне мовлення», «Індекс інформаційного впливу Кремля», «Як розпізнати пропаганду в ЗМІ», «Журналістське розслідування: основи», «Новинна грамотність», «Медіадрайвер», «Вибори і ЗМІ», «Телятина», «Приціл», «Донбас: чесно», «MediaSapiens» [43, с. 224].

Починаючи як «Телекритика» і ведучи свою діяльність під цією назвою до квітня 2016 року, ГО та сайт вже з самого початку були присвячені аналізу медійного простору та підвищенню рівня медіаграмотності в Україні. Лідер команди, Наталія Лигачова, гравацький журналіст, взяла на себе відповідальність за керівництво цією ініціативою.

У квітні 2016 року «Телекритика» пройшла ребрендинг та прийняла нову назву – ГО «Детектор медіа». Ця перезміна вказує на посилення їхнього підходу

до виявлення та аналізу медійних тенденцій. Започаткована у лютому 2016 року, платформа «Детектор медіа» є не лише новим сайтом, але і унікальним медійним центром для Східної та Центральної Європи, що об'єднує створення контенту, дослідження медійного простору, модерацію професійної дискусії, адвокацію медійних змін та медіаосвіту.

Заснована на місії покращення якості українських медіа, підвищення медіаграмотності українського суспільства та протидії дезінформації та пропаганді, «Детектор медіа» стала ключовим гравцем у формуванні інформаційного простору в Україні. Отож, розглянемо основні проєкти, ініціатором створення яких є медіаресурс «Детектор. Медіа».

Портал «MediaSapiens» визначається своєю вагомою роллю в медійній сфері. За цей час він став невід'ємною частиною медійної ландшафту та визнаним центром аналізу та обговорення ключових подій в галузі. Ініціатива Інтерньюз-Нетворк виявилася стратегічно важливою, створивши простір для дискусій та обміну ідеями серед професіоналів медіа та суспільства в цілому.

Цільова аудиторія «MediaSapiens» – це не лише журналісти, але і широкий спектр громадських діячів, політиків, державних службовців, а також власників та менеджерів ЗМІ. Такий широкий круг зацікавлених сторін свідчить про розмаїття тем і питань, які портал розглядає, та його важливу роль у формуванні обговорення в сфері медіа та суспільства.

«MediaSapiens» відіграє роль не лише надійного інформаційного ресурсу, але також стає значущою платформою для обговорення та обміну ідеями. Ця ініціатива не тільки забезпечує доступ до актуальної інформації, а й створює сприятливе середовище для підвищення рівня професіоналізму в галузі медіа. Важливою частиною є сприяння взаєморозумінню між різними стейкхолдерами. Шляхом об’єднання інформаційного ресурсу та платформи для взаємодії «MediaSapiens» стає цінним інструментом для тих, хто цікавиться розвитком сучасної медіасфери та пошуку конструктивного обміну думками.

В основному матеріали проєкту стосуються спростування російських фейків на українському інфопросторі, як от, публікація про навчання НАТО як прямий передвісник Третьої світової війни [6].

Досить цікавою є й ініціатива «Медіачек». Громадська організація «Детектор медіа» та Громадська організація «Інститут масової інформації», в рамках ініціативи «Медіачек», приймають звернення щодо матеріалів, що публікуються ЗМІ, з метою перевірки на можливі порушення законодавства («Про телебачення і радіомовлення», «Про пресу», «Про інформаційні агентства», Цивільного кодексу України тощо), а також відповідності базовим професійним стандартам журналістики, таким як достовірність, баланс точок зору, розділення фактів і коментарів, повнота і відповідність журналістській етиці [28].

Громадські організації «Детектор медіа» та «Інститут масової інформації» запровадили ініціативу «Медіачек» для сприяння професійному діалогу та підвищення довіри до ЗМІ. Ця ініціатива спрямована на розгляд скарг щодо можливих порушень законодавства і професійних стандартів журналістики, які мають велике значення для забезпечення якості інформаційного простору.

Для надання скарги особа повинна заповнити спеціальну форму на веб-сайтах організацій, вказавши свої особисті дані та інформацію про матеріал, який вона оскаржує. Організації перевіряють ці скарги на відповідність критеріям та проводять аналіз зазначених матеріалів з точки зору їхньої справедливості та відповідності професійним стандартам.

Після аналізу матеріалів організації готують висновок і в разі виявлення порушень відправляють його відповідним ЗМІ чи журналістам. Відкритість цього процесу сприяє підвищенню відповідальності ЗМІ перед громадськістю та вдосконаленню медійного середовища [30].

Ще одна ініціатива досліджуваного медіаресурсу, проєкт аналізу соціальних мереж «Детектор медіа» використовує елементи штучного інтелекту для обробки великих обсягів даних українського сегмента платформ Facebook, YouTube, Telegram та Twitter. Цей підхід дозволяє систематично вивчати та

аналізувати поведінку користувачів, тренди та динаміку інформаційного взаємодії в онлайн середовищі. Результати аналізу надають важливі висновки щодо популярності та впливу різноманітного медійного контенту, а також допомагають ліквідовувати потенційні проблеми, пов’язані з дезінформацією та маніпулятивними технологіями.

Крім того, цей проєкт сприяє розумінню динаміки та тенденцій українського інтернет-простору, допомагаючи розкривати певні закономірності в поширенні контенту та реакції аудиторії. Аналіз соціальних мереж української аудиторії стає важливим інструментом для формування стратегій медійної діяльності, пошуку ефективних способів взаємодії із суспільством [1].

Проєкт «Детектор маніпуляцій» представляє собою ініціативу журналістів медіаресурсу «Детектор медіа», спрямовану на дослідження та спростування фейків держави-агресора. Цей проєкт базується на аналізі інформації з авторитетних джерел та проведенні ретельної перевірки фактів.

Журналісти «Детектор медіа» використовують різноманітні методи та техніки, аби відшукати та аналізувати маніпуляції в інформаційному просторі, зокрема в соціальних мережах та ЗМІ. Їхня робота спрямована на розкриття неправдивої чи спотвореної інформації, яка може використовуватися для маніпуляцій та впливу на громадську думку [11].

«Дошка ганьби» є проєктом, де медійники розкривають та публікують інформацію про впливових осіб, які співпрацювали з державою-агресором або вчиняли протизаконні дії. Цей проєкт має на меті привернення уваги до негативних аспектів співпраці з ворожими структурами чи протиправної поведінки осіб, які мають значний авторитет у суспільстві. Шляхом публікації інформації на «Дошці ганьби», медійники сприяють розкриттю та обговоренню суспільно важливих ситуацій, спонукаючи до дотримання принципу відповідальності та перегляду ставлення до дій впливових осіб у громадському просторі [12].

Варто зазначити, що це лише декілька прикладів проєктів «Детектор. Медіа». На сьогодні медіаресурс має 18 активних ініціатив, спрямованих

переважно на фактчекінг та підвищення рівня медіаграмотності читачів онлайн-видання. Серед цих ініціатив є проекти, що вивчають джерела інформації, виявляють маніпулятивні технології, аналізують та коментують новинні матеріали. Крім того, «Детектор медіа» проводить та організовує навчальні курси чи інші заходи для підвищення медіаграмотності громадськості та розвитку критичного мислення в інформаційному просторі [52].

Розглянемо наступний медіаресурс, який ми обрали для дослідження – Центр протидії дезінформації.

Центр протидії дезінформації є органом Ради національної безпеки і оборони України, утвореним відповідно до рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації» [48], яке набуло чинності за Указом Президента України від 19 березня 2021 року № 106.

Центр забезпечує проведення заходів щодо протидії поточним і передбачуваним загрозам національній безпеці та інтересам України в інформаційній сфері. Ці заходи включають забезпечення інформаційної безпеки, виявлення та протидію дезінформації, ефективну протидію пропаганді, деструктивним інформаційним впливам та кампаніям, запобігання спробам маніпулювання громадською думкою.

Центр активно висвітлює тенденції у сфері військових питань, оборонно-промислового комплексу, боротьби зі злочинністю та корупцією, зовнішньої та внутрішньої політики, економіки, критичної інфраструктури, екології, охорони здоров'я, соціальної сфери, формування суспільної свідомості, науково-технологічного напряму тощо. Основний акцент зроблено на боротьбі з поширенням неправдивої інформації та інформаційним тероризмом.

Центр діє в рамках законів України, міжнародних договорів, актів Президента та Кабінету Міністрів України, а також розпоряджень Секретаря Ради національної безпеки і оборони України.

Основними завданнями Центру є:

– проведення аналізу та моніторингу подій і явищ в інформаційному просторі України, стану інформаційної безпеки та присутності України у світовому інформаційному просторі;

– виявлення та вивчення поточних і прогнозованих загроз інформаційній безпеці України, чинників, які впливають на їх формування, прогнозування та оцінка наслідків для безпеки національних інтересів України;

– забезпечення Ради національної безпеки і оборони України, Голови Ради національної безпеки і оборони України інформаційно-аналітичними матеріалами з питань забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою;

– підготовка та внесення Раді національної безпеки і оборони України, Голові Ради національної безпеки і оборони України пропозицій щодо: визначення концептуальних підходів у сфері протидії дезінформації та деструктивним інформаційним впливам і кампаніям; координації діяльності та взаємодії органів виконавчої влади з питань національної безпеки в інформаційній сфері, забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою; здійснення системних заходів, спрямованих на посилення спроможностей суб’єктів сектору безпеки та оборони, інших державних органів задля забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою, розвитку національної інфраструктури у відповідній сфері; удосконалення системи правового та наукового забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою;

– участь у розбудові системи стратегічних комунікацій, організації та координації заходів щодо її розвитку;

– участь у розробленні та реалізації Стратегії інформаційної безпеки України, здійсненні аналізу стану її реалізації, зокрема з питань ефективності заходів щодо протидії дезінформації;

– участь у створенні інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

– розроблення методології виявлення загрозливих інформаційних матеріалів маніпулятивного та дезінформаційного характеру;

– сприяння взаємодії держави та інституцій громадянського суспільства щодо протидії дезінформації та деструктивним інформаційним впливам і кампаніям, організація та участь в інформаційно-просвітницьких заходах з питань підвищення медіа-грамотності суспільства;

– вивчення, узагальнення й аналіз досвіду інших держав і міжнародних організацій з протидії дезінформації та підготовка пропозицій щодо його використання в Україні;

– бере участь у визначенні пріоритетів залучення міжнародної технічної допомоги з питань забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.

Сьогодні Центр активно залучений до протидії російській агресії [49].

Можна підсумувати, що основним завданням медіаресурсів «Детектор.медіа» та Центр протидії дезінформації є боротьба з фейками та маніпуляціями в медіа за допомогою різноманітних проєктів та стратегій для підвищення рівня медіаграмотності та забезпечення інформаційної безпеки. Робота журналістів «Детектор.медіа» орієнтована на виявлення та спростування фейків, аналіз новин з точки зору достовірності та підвищення рівня медіаграмотності аудиторії. У свою чергу, Центр протидії дезінформації

зосереджується на комплексному підході до боротьби з дезінформацією. Його діяльність спрямована на використання сучасних технологій та методів аналізу великих масивів даних для виявлення та аналізу явища дезінформації в онлайн-середовищі.

2.2. **Методи та прийоми забезпечення якості та безпеки контенту у досліджуваних ЗМІ.**

У сучасному інформаційному просторі забезпечення якості та безпеки контенту у ЗМІ відіграє важливу роль у формуванні об’єктивного медійного середовища. Методи та прийоми, які використовуються для досягнення цієї мети, стають ключовими факторами у підтримці довіри громадськості до медійних ресурсів.

Насамперед, важливою умовою підтримки якості медійного контенту є редакційна перевірка та процес контролю якості опублікованого матеріалу.

Організація «Детектор медіа» з 2003 року проводить моніторинг якості щоденних телевізійних новин головних центральних телеканалів. Серед телеканалів, що перевірялися у 2018 році, були «Інтер», «1+1», «Україна», СТБ, ICTV, 5 канал, «UA: Перший» та «112 Україна», і цей перелік з часом лише розширюється.

Моніторинг охоплює проблеми дотримання стандартів інформаційної журналістики, виявлення маніпуляцій, «паркету» (офіційних повідомлень без новинної цінності) та матеріалів з ознаками замовності. Результатом цього дослідження є аналітичний огляд, що публікується на сайті MediaSapiens у розділі «Моніторинг щоденних новин».

Крім виявлення порушень стандартів та ознак замовності, комплексний моніторинг фіксує тематику та географію новин, дотримання стандартів журналістики, загальну тональність матеріалів, присутність експертних думок та гостей у студіях, а також згадки про інститути влади та політичні сили.

Методологія дослідження передбачає аналіз текстових матеріалів головних випусків телевізійних новин та звіряння розшифрувань з

відеоматеріалами за потреби. Всі дані вносяться в базу даних, що забезпечує повний доступ до інформації для подальшого аналізу та огляду [32].

Центр протидії дезінформації активно використовує методи та прийоми для забезпечення якості та об'єктивності контенту. Фахівці Центру проводять систематичний аналіз і перевірку інформації, що розміщується у ЗМІ та соціальних мережах, ідентифікуючи можливі фактичні помилки та маніпуляції. Аналіз контенту базується на дотриманні принципів інформаційної журналістики, зокрема, принципу достовірності, об'єктивності, балансу та перевірки джерел.

Наступним прийомом є аналіз змісту публікації на рівень дотримання журналістської етики.

Медіаресурс «Детектор. Медіа» у рамках моніторингу дотримання телеканалами стандартів інформаційної журналістики проводить оцінку відповідності телеканалів цим вимогам на рівні аналізу текстових версій ефірів. Оцінюються такі фактори, як оперативність подачі інформації, точність та достовірність її подання, повнота інформації, баланс думок, відокремлення фактів від думок та доступність подачі інформації.

Центр моніторингу враховує ряд критеріїв, зокрема, чи відповідає коментар журналіста тій картинці, яку показують, чи не спотворено картинку графічними ефектами, чи є повноцінні розкадровки та інтершум, чи є баланс думок учасників подій та чи є достовірність використаних джерел інформації.

У моніторингу враховуються важливі події та аналізуються матеріали про ці події з погляду дотримання стандартів журналістики. Для аналізу обираються підсумкові вечірні випуски новин на загальнонаціональних каналах та випуски о 19-й годині на інформаційних каналах [31].

Що ж до діяльності Центру протидії дезінформації, то варто зазначити, що працівники цього медіаресурсу розробили посібник з протидії дезінформації розроблено працівниками Центру протидії дезінформації робочого органу Ради національної безпеки і оборони України за підтримки Консультативної місії Європейського Союзу в Україні.

У рекомендаціях до посібника журналістам радять дотримуватись високих професійних стандартів та уникати використання маніпулятивних заголовків у своїх медійних публікаціях.

Цей посібник був розроблений у відповідь на негативний вплив противника на інформаційний простір України. Його метою є покращення системи протидії ворожим інформаційним впливам шляхом ознайомлення з тонкощами цієї проблеми та демонстрації тактик, технік і процедур противника. Центр протидії дезінформації узяв до уваги весь наявний досвід в цій сфері та узагальнив його у даному посібнику, що дозволяє ефективніше протистояти дезінформації та зміцнювати інформаційну безпеку [45].

Медіаресурси також можуть залучати експертів та консультантів для оцінки матеріалів, особливо з тематики, яка вимагає спеціалізованих знань або досвіду, що в підсумку допомагає підтвердити достовірність та об’єктивність інформації.

Яскравим прикладом цього є ініціатива «Детектор. Медіа» щодо перевірки якості журналістських розслідувань.

Для моніторингу залучені два досвідчених експерти з журналістських розслідувань, які проходили міжнародні тренінги у цій галузі та брали участь у міжнародних конференціях або конкурсах. Вони переглядають програми шести проектів розслідувань: «Гроші» на 1+1, «Народна прокуратура» на 112, «Наші Гроші» на 24 каналі та UA: Перший, «Слідство.Інфо» на Громадському ТБ, 24 каналі та UA: Перший, «Стоп корупції» на 5-му каналі та «Схеми» на Радіо Свобода та UA: Перший.

Для аналізу обирається два тижні на місяць, під час яких оцінюються всі програми, що вийшли в ефір у ці періоди. За перші 14 місяців моніторингу було оцінено 26 випусків кожного проекту розслідувань і здійснено регулярний аналіз. Кількісний аналіз проводиться за 6 маркерами з оцінкою за трибальною системою. Оцінки заносяться в таблицю Excel, що доповнює методологію моніторингу. Такі заходи дозволяють експертам порівнювати програми за шістьма критеріями та виводити рекомендації для подальшого удосконалення

розслідувань [33]. Критерії аналізу якості журналістських розслідувань експертами ініціативи подано на рис. 2.1.

Рис. 2.1 – Критерії для аналізу якості журналістських розслідувань (медіаресурс «Детектор. Медіа»)

Центр протидії дезінформації також активно залучає експертів задля перевірки достовірності фактів та мінімізації проявів дезінформації в українському інформаційному просторі.

14 липня 2022 року Представники державних органів, громадських організацій, ЗМІ та міжнародні експерти прийняли участь у круглому столі щодо боротьби з дезінформацією. Учасники обговорили маніпулятивні методи, які застосовуються в Україні та за кордоном, а також правові аспекти та взаємодію громадянського суспільства і державних органів у цьому контексті, зокрема у сфері кібербезпеки.

Під час дискусії в. о. керівник Центру протидії дезінформації при Раді національної безпеки і оборони України Андрій Шаповалов підкреслив, що особи, що свідомо поширюють дезінформацію, мають бути розглянуті як

інформаційні терористи і відповідати перед законом як військові злочинці. Він також зазначив необхідність внесення змін до законодавства для захисту інформаційного простору.

Організаторами заходу були Національна Академія СБУ, Фонд цивільних досліджень та розвитку США (CRDF Global Ukraine) та ГО «Міжнародна академія інформації» [8].

Досліджувані медіаресурси також активно працюють над тим, щоб українці мали доступ до достовірних та перевірених джерел інформації. Вони також забезпечують відкритість процесів перевірки та діляться інформацією про свої стратегії та методи з аудиторією.

Наприклад, у одній із публікацій «Детектор. Медіа» ділиться лайфхаками, як розпізнати дезінформаційний вплив та фейкову інформацію у соціальній мережі Телеграм. У цьому дослідженні «Детектор медіа» зосереджується на наступних аспектах:

1. Виявленні проросійських та окупаційних телеграм-каналів та їх мереж.
2. Встановленні взаємозв'язків між цими каналами та іншими.
3. Відстеженні тактик поширення російської пропаганди та дезінформаційних наративів.
4. Аналізі змін у роботі проросійських каналів після початку конфлікту.
5. Дослідженні впливу подій конфлікту на рейтинг, контент та аудиторію цих телеграм-каналів.

«Детектор медіа» розуміє, що неможливо точно визначити мотивацію журналістів, медіа або інших користувачів соцмереж, які поширюють вміст. Автори моніторингу не стверджують, що канали свідомо займаються російською пропагандою (за винятком окупаційних), але лише вказують на те, що їхні матеріали містять меседжі та контент, які відображають дезінформаційні наративи, аналогічні або близькі до тих, які використовує Кремль [29].

Що ж до діяльності Центру протидії дезінформації у цій галузі, то варто зауважити, що цей медіаресурс розробив Глосарій основних механізмів дезінформаційного впливу, виокремивши ключові риси кожного із них та

надаючи рекомендації щодо протидії цим механізмам. Наведемо декілька прикладів цих механізмів із Глосарію Центру:

1. «Заговорювання» – цей метод використовує пропаганда, коли необхідно знизити актуальність та викликати негативну реакцію до будь-якої події. Мета «заговорювання» – викликати втому в аудиторії від дезінформації з певної «гострої» теми, щоб відбити подальше бажання цікавитися нею.

2. «Ефект первинності» – успіх пропаганди полягає в тому, щоб дезінформація досягла аудиторії раніше, ніж правда. При надходженні суперечливої інформації, перевірити яку швидко неможливо, особа схильна надавати перевагу тій інформації, що надійшла першою.

3. «Буденна розповідь» використовується російськими пропагандистами, щоб «привчити» аудиторію до дезінформації про вчинене насильство, вбивства, терористичні акти, обстріли тощо. «Благородні» телеведучі на ростелеканалах зі спокійними обличчями і рівними голосами щодня повідомляють про вчинення російською армією найтяжчих злочинів.

4. «Удар на випередження» є випереджаючим вкидом дезінформації. Його завдання – викликати зустрічну реакцію «супротивника», щоб використати це у більш вигідному для себе контексті. Цей прийом використовують російські пропагандисти, щоб прискорити нагнітання конфлікту та з поширенням дезінформації створити провокацію, чим «загасити» правдиву інформацію [7].

Можна підсумувати, що методи та прийоми забезпечення якості та безпеки контенту у досліджуваних медіаресурсах містять систему фактчекінгу та перевірку достовірності інформації перед публікацією. Крім того, перевірка дотримання професійних етичних стандартів та принципів, які визначають межі використання необхідної інформації без порушення приватності та безпеки осіб, теж є важливим інструментом підтримки якості та безпеки журналістського контенту. Важливою практикою є також регулярний моніторинг дотримання журналістами стандартів професійної етики, а також впровадження технологій перевірки та пошуку шкідливого контенту, які сприяють вчасному реагуванню на можливі загрози та забезпечують безпеку користувачів.

РОЗДІЛ 3
СТРАТЕГІЇ ЗАХИСТУ КОНТЕНТУ ЗМК В УМОВАХ ГІБРИДНОЇ ВІЙНИ РОСІЇ ТА УКРАЇНИ: ПЕРСПЕКТИВИ ТА РЕКОМЕНДАЦІЇ

3.1. **Медіаосвіта як інструмент захисту населення від дезінформаційного впливу країни-агресора.**

Ідеологія інформаційного суспільства спрямована на створення ноосферної економіки, де основним ресурсом вважається інформація, і на задоволення головних потреб людини у знаннях. Вона визнає пріоритет духовно-інформаційних потреб перед матеріальними. Розвиток соціальних систем розглядається в контексті еволюції інформаційних технологій. У XXI столітті понад половина робочого часу буде витрачена на обробку, зберігання та передачу інформації, що вимагає розробки ідеології інформаційного суспільства. Ця ідеологія прагне забезпечити гідне місце для людини в сучасному світі, акцентуючи на культивуванні розвитку і ускладненні інформаційно-комунікативних технологій.

Ідеологія інформаційного суспільства, розглянута як наукова та освітня парадигма, повинна визнати освіту ключовим компонентом економіки сталого розвитку. Інформаційне суспільство еволюціонує в «суспільство знань», а його ідеологія перетворюється в ідеологію «суспільства знань». Ця ідеологія враховує особливості виробництва та споживання знань у корисній інтелектуальній діяльності людей [18, с. 47].

Зростання кількості цифрового контенту, доступного в Інтернеті, а також зростання впливу соціальних мереж та новинних платформ роблять суспільство вразливим перед великим обсягом дезінформації та медіатероризму. У цьому контексті медіаграмотність, яка охоплює розуміння, аналіз та ефективне використання медійних засобів, є необхідною умовою для забезпечення стійкості та безпеки користувачів у цифровому просторі.

Медіаграмотність визначається не лише здатністю розрізняти правдиву інформацію від дезінформації, але й умінням критично оцінювати та розуміти

різноманіття медійних форматів. У світі, де медіавіруси можуть швидко поширюватися через соціальні мережі та інші канали, важливо виховувати суспільство, яке знає, як ефективно користуватися медійними ресурсами, щоб уникати пасток дезінформації та забезпечити сталість інформаційного простору.

Медіаграмотність – це процес навчання людини, яка володіє розвиненими навичками сприйняття, створення, аналізу та оцінки медіатекстів. Цей процес також включає розуміння соціокультурного та політичного контексту функціонування медіа в сучасному світі, а також знання кодових і репрезентаційних систем, які використовуються в медіа. Людина з розвинутою медіаграмотністю пов’язана з громадянською відповідальністю, і її життя в суспільстві і світі визначається цими здатностями та знаннями [60, с. 9494].

Медіакомпетентність, визначена в документах Ради Європи, охарактеризована як критичне та вдумливе ставлення до медіа з метою формування відповідальних громадян. Ця компетентність дозволяє людям висловлювати власні судження на підставі отриманої інформації, використовувати її, аналізувати, ідентифікувати економічні, політичні, соціальні та/або культурні інтереси, пов’язані з нею. Крім того, медіакомпетентність надає здатність інтерпретувати і створювати повідомлення, вибирати найбільш відповідні для комунікації медіа, а також реалізовувати право на свободу самовираження та інформацію. Це сприяє особистому розвитку, а також збільшує соціальну участь і інтерактивність [57, с. 117].

Згідно з документами ЮНЕСКО, медіаосвіта визначається як навчання теорії та практичних навичок для засвоєння сучасних мас-медіа. Ця галузь розглядається як частина специфічної та автономної області знань у педагогічній теорії та практиці. Важливо відрізняти медіаосвіту від використання медіа як допоміжного засобу у викладанні інших предметів, як от, математика, фізика чи географія [61, с. 203]. Так, документи ЮНЕСКО наголошують на чіткому розрізненні між медіаосвітою та використанням медіа як засобу підтримки в інших галузях знань.

Медіаосвіта розглядається як навчання, що включає в себе розвиток різноманітних навичок та знань, спрямованих на розуміння та використання різних видів медіа і технологій. Вона має надавати людям здатність критично аналізувати, творчо сприймати та створювати медіатексти, а також розуміти соціокультурний контекст та політичні аспекти функціонування медіа в сучасному світі. Медіаосвіта визначається як необхідний елемент основних прав громадян на свободу вираження та інформації, сприяючи демократії, і рекомендується включати до навчальних планів національних систем освіти [63, с. 273]. Особливий акцент робиться на переконанні, що медіаосвіта є фундаментальним правом людини і має продовжуватися та удосконалюватися протягом усього життя [15, с. 22].

У сучасному світі важлива освіта в медіа, оскільки умови інформаційного суспільства та глобалізації мас-медіа призводять до впливу, який вони мають на сприйняття людиною світу. Часто засоби масової інформації не об’єктивно інформують про події та факти дійсності. Тому медіаосвіта навчає людину критично оцінювати медіаінформацію та робити обґрунтовані висновки, що сприяє її самозахисту [46, с. 80].

Фахівцеві інформаційної епохи, за думкою Г. Онковича, поставлено завдання розвивати критичне мислення та вміння аналізувати та вибирати особисто значущу інформацію. Це означає бути медіа- та інформаційно грамотною особистістю, а також вміти структурувати, узагальнювати та осмислено використовувати медіапродукти. Досягнути цього можна завдяки медіаосвіті [39, с. 82]. О. Федоров визначає медіаосвіту як процес розвитку особистості з використанням мас-медіа для формування культури спілкування з медіа, творчих і комунікативних здібностей, критичного мислення та вмінь повноцінно сприймати, інтерпретувати, аналізувати й оцінювати медіатексти. Медіаосвіта також включає навчання різних форм самовираження за допомогою медіатехніки [27, с. 122].

Деякі науковці вважають медіаграмотність рівнем медіакультури, за допомогою якого журналіст здатний використовувати інформаційно-

комунікативну техніку, спілкуватися за допомогою медіазасобів, презентувати себе, свідомо «прочитувати», сприймати і критично аналізувати інформацію, розрізняючи віртуальні та реальні медіа тексти [39, с. 83].

В основі медіаграмотності лежить вміння критичного мислення, яке визначається як оціночне та рефлексивне, відкрите для нових інформаційних шарів, які наростають на основі особистого життєвого досвіду. Критичне мислення виявляється у послідовних розумових діях, спрямованих на перевірку висловлювань чи систем висловлювань з метою визначення їх відповідності фактам, нормам або цінностям. Це уміння суворо оцінювати свої та інші думки, аналізувати припущення, враховуючи всі аргументи за та проти, розглядаючи припущення як гіпотези, які потребують перевірки. Загалом, критичне мислення представляє собою форму практичної логіки, адаптованої до контексту розмірковувань та індивідуальних особливостей мислителя [36, с. 57].

Останнім часом в Україні стала популярною ідея медіаграмотності, яка визнає необхідність володіння цим навичками як професійними комунікаторами, так і споживачами інформації. Професіонали звертають увагу на важливість ефективного володіння медіаграмотністю, а також на усвідомлення можливих небезпек, якими вони можуть свідомо чи несвідомо наражати суспільство. Одночасно висвітлюється, що споживачі масової інформації також повинні мати знання теорії комунікації, щоб уникнути потенційних маніпуляцій і не стати жертвами недостовірної інформації [17, с. 78]. Завдяки стрімкому поширенню та впливові масових комунікацій в суспільстві, медіаграмотність здобула значну увагу дослідників. Останні роки визначили різні рівні медіаграмотності: ті, що характерні та достатні для осіб, які мають професійні або опосередковані зв'язки з масовими комунікаціями. Таким чином, крім загальної медіаграмотності, з’явився термін «критична медіаграмотність», який використовується для оцінювання більш ретельного впливу засобів масових комунікацій на різні суспільні явища. Розвиток цієї грамотності базується на здатності індивіда критично мислити й формулювати власну позицію, відмінну від загальноприйнятих [51, с. 139].

Загальні завдання медіаосвіти в Україні відповідають концепціям медіаосвіти, розробленим ЮНЕСКО. Основні положення включають:

1. Суспільство повинно критично використовувати інформацію, комунікації та технології, а також критично оцінювати інтернет-середовище.

2. Кожна особа може створювати інформацію і мати право на самовираження, і медіаграмотність є необхідною для всіх.

3. Інформаційні повідомлення не завжди є об'єктивними і можуть бути упередженими чи маніпулятивними. Медіаосвітяни мають просувати цю ідею як ключову для розвитку медіаграмотності.

4. Кожна людина має право на інформацію, розуміння її та комунікацію.

5. Медіаграмотність є результатом тривалого навчання, яке вимагає значних зусиль від медіапедагогів. Критичне мислення є компетенцією, яку потрібно постійно розвивати, оскільки технології постійно змінюються [21, с. 4].

Україна планувала завершити другий етап розвитку медіаосвіти у 2022 році, але зміни в умовах, зокрема зростання потоку дезінформації, фейків та маніпулятивного контенту, а також проведення інформаційно-психологічних операцій з боку країни-агресора, змусили зосередитися на формуванні ще більш критичного ставлення до медіа, активніше вивчати методи російської пропаганди для ефективного протистояння їй в гібридній війні.

Медіаосвіта допоможе розпізнавати:

1. Дезінформацію-навмисне розповсюдження інформації, яка є повністю або частково неправдивою.

2. Інформаційні маніпуляції-навмисне та масове розповсюдження неправдивих або упереджених новин у ворожих політичних цілях.

3. Фейкові новини. Поняття фейкових (підроблених, фальшивих) новин включає як спотворення об'єктивних істин, так і оманливі історії [9, с. 56].

Два напрями і якісні характеристики реалізації завдань медіаосвіти в контексті інформаційної безпеки можна сформувати таким чином. Перша характеристика полягає в аналізі медіаосвіти у стабільних умовах суспільного

середовища, де прогрес технологій комунікації призводить до збільшення числа замовників та агентів медіаосвіти, що включають не лише національно-державні, а й приватні суспільні політичні актори, розширюючи спектр форм медіаосвіти. Друга характеристика визначається технологічним прогресом, який розширює коло носіїв інформації, відповідно до атрибутивного підходу до інформації як об’єктивної властивості матеріальних об’єктів [27, с. 127]. Медіаосвіта в умовах архітектурних об’єктів може здійснюватися через спеціальні курси, які здавалося б, на перший погляд, не пов'язані з нею. У разі війни медіаосвіта набуває інших характеристик, оскільки вона відображає роль у забезпеченні інформаційної безпеки в умовах загострення ролі інформаційно-психологічних чинників та воєнної ситуації. Тому важливо, щоб аудиторія медіаосвітніх заходів могла розрізняти між певними фактами та тими, що потребують перевірки, оцінювати надійність джерел інформації, виявляти упередженість суджень, розуміти незрозумілі або двозначні аргументи, а також розпізнавати логічну несумісність у ланцюжку міркувань тощо [27, с. 129]. Відмінність від процесів медіаосвіти в умовах суспільної стабільності полягає, зокрема, в централізації медіаосвітніх процесів. Різко зростає роль держави як ключового їх замовника. Але це не означає, що роль інших суб’єктів нівелюється [41, с. 180].

Можна стверджувати, що медіаосвіта є важливим інструментом захисту населення від дезінформаційного впливу, особливо під час російсько-української війни. медіаграмотність допомагає людям розвинути критичне мислення, необхідне для аналізу інформаційних повідомлень і вміння відрізняти правдиву інформацію від маніпуляцій та пропаганди. Завдяки медіаосвіті громадяни можуть краще розуміти методи та інструменти, які використовуються для дезінформації, тим самим знижуючи рівень вразливості до інформаційних атак. Навчання тому, як перевіряти джерела інформації і оцінювати контекст новин, може зменшити ризик поширення неправдивих новин. Крім того, медіаосвіта сприяє формуванню відповідальної громадянської позиції, що є критично важливим у боротьбі з інформаційними загрозами країни-агресора.

3.2. **Міжнародний досвід захисту медійного контенту від кіберзагроз**.

У сучасному світі медійний контент стає все більш вразливим через розширення кіберзагроз, що формує необхідність міжнародної співпраці та обміну досвідом щодо його захисту. Різні країни розробляють і впроваджують складні стратегії та технології для забезпечення безпеки інформації, яка розповсюджується через медіа.

Загальновизнано, що міжнародна діяльність держав має сприяти соціальному та економічному розвитку і відбуватись у відповідності до завдань підтримки миру та міжнародної безпеки. Вона повинна відповідати загальновизнаним принципам і нормам міжнародного права, включаючи принципи мирного врегулювання спорів та конфліктів, незастосування сили у міжнародних відносинах, невтручання у внутрішні справи інших держав, поваги до суверенітету держав, а також основних прав і свобод людини [13, с. 74].

Міжнародне співробітництво в галузі інформаційної безпеки вимагає пошуку спільних рішень в межах міжнародних організацій для протидії інформаційним та кіберзагрозам. Також необхідно розробляти спільну стратегію інформаційної безпеки для боротьби з кібервійнами, інформаційним тероризмом та інформаційною злочинністю.

Міжнародне співтовариство визнає, що лише спільними зусиллями та відповідно до принципів міжнародного права можливо вирішити проблеми у політичній, економічній, безпековій та інших сферах життєдіяльності суспільства [55, с. 127].

Політичні рішення, прийняті у форматі міжнародних організацій, як-от ООН, НАТО, ОБСЄ, є важливими керівними принципами діяльності багатосторонніх механізмів, оскільки вони враховують позиції та інтереси усіх міжнародних акторів.

Модернізація політики інформаційної безпеки на рівні ООН викликана визначенням нових факторів відповідальної поведінки держав, приватного сектора, наукових установ та громадських організацій у кіберпросторі. Це може сприяти підвищенню ефективності міжнародного співробітництва.

Варто зазначити, що проблеми міжнародної інформаційної безпеки активно обговорювалися на засіданнях Генеральної Асамблеї ООН протягом 1998-2015 років з метою розробки відповідного міжнародного документа. У резолюціях «Роль науки і техніки в контексті міжнародної безпеки і роззброєння» та «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» обговорювалися питання про подвійне використання високих технологій, їх роль у цивільних та військових сферах, модернізація сучасного озброєння, а також про необхідність протидії деструктивному впливу в цих сферах [34, с. 47].

Основним принципом безпеки інформації НАТО є те, що інформація повинна зберігати свій ступінь захисту при всіх її передачах, починаючи з джерела, а контроль за розподілом і поширенням інформації повинний забезпечити відсутність її витоку, а також і те, що правила доступу до інформації повинні дозволяти використання інформації лише особам, яким вона потрібна для виконання службових обов'язків. Присвоєння інформації НАТО того або іншого грифа таємності виробляється відповідно до правил систем безпеки країн-учасниць [3, с. 197].

Організація безпеки та співробітництва в Європі (ОБСЄ) має важливу роль у забезпеченні інформаційної безпеки через дві основні функції. По-перше, вона сприяє державам-учасницям у повному виконанні своїх зобов'язань, визначених ОБСЄ. По-друге, вона контролює виконання цих зобов'язань державами-учасницями. ОБСЄ веде діалог і сприяє політичній взаємодії між країнами-членами з широкого спектру питань безпеки, включаючи раннє попередження конфліктів, запобігання кризам, врегулювання криз та відновлення після конфліктів.

Цікаво, що ОБСЄ розглядає безпеку як комплексне поняття і працює над розв'язанням трьох аспектів безпеки: військово-політичного, економічного, екологічного та людського, аналізуючи їх взаємозв'язок і взаємозалежність. Комплексний підхід ОБСЄ до безпеки включає політико-воєнні аспекти разом з економічно-екологічними та людськими аспектами. Таке багатовимірне

розуміння безпеки вказує на те, що різні виміри безпеки взаємодоповнюються та мають взаємний вплив один на одного [50, с. 115].

Одним із ефективних інструментів захисту медіапростору є й законодавче регулювання діяльності ЗМІ.

Принципи законодавчого регулювання медіа формувалися протягом століть. У 1859 році відомий теоретик свободи преси Джон Стюарт Мілль у своїй роботі «Про свободу» розглядав питання про «властивості і межі влади, яку суспільство може справедливо мати над індивідом» [35, с. 13]. Згідно з поглядами дослідника, ніхто, включаючи сам народ, не має права обмежувати свободу висловлювання думок. Тому проголошене в законодавствах більшості країн світу право на доступ до інформації є одним із фундаментальних прав людини.

Міжнародні стандарти права громадян на доступ до інформації закріплені в статті 19 «Загальної декларації прав людини», ухваленої Генеральною Асамблеєю Організації Об'єднаних Націй (ООН) 10 грудня 1948 року, а також у статті 10 «Європейської конвенції з прав людини», прийнятої 4 листопада 1950 року. У цих документах чітко зазначено, що кожна людина має право на свободу висловлювання своїх поглядів, а також на отримання і поширення інформації та ідей будь-яким законним способом, незалежно від державних кордонів [37, с. 24].

На сьогоднішній день акти Європейського Союзу (ЄС) регулюють три основні галузі в медіа-сфері. По-перше, це створення механізмів підтримки електронних ЗМІ в Європі. По-друге, це захист культурних інтересів Європи у контексті широкого міжнародного обговорення. І по-третє, це розробка правової бази, необхідної для розвитку єдиного внутрішнього європейського ринку медіа.

Ініціатором створення європейської правової системи регулювання медіа-простору була Рада Європи та Європейська Спільнота. Наприкінці квітня 1982 року Комітет міністрів Ради Європи прийняв Рекомендацію, а пізніше План дій стосовно національної та міжнародної медіа-політики, відомий як «Європейська медіа-хартія». У 1984 році Комітет Міністрів прийняв також дві рекомендації з

питань реклами на радіо та телебаченні, а також супутникової спроможності для телебачення та радіо.

У той же час в Європейській Спільноті також розглядалися перші кроки в напрямі медіа-політики. У 1982 році Європейський Парламент висловив пропозицію щодо створення європейського телевізійного каналу разом із Європейською мовною спілкою. Також в цей час Парламент розглядав можливості діяльності Спільноти в напрямі розвитку транснаціонального кабельного та супутникового телебачення, зосереджуючись на потребах технічної стандартизації та виробництва європейських програм. У 1984 році Комісія опублікувала Зелену книгу щодо Директиви «Телебачення без кордонів» [59]. У різних Резолюціях Європейського парламенту того часу була одна загальна мета: розвиток європейської ідентичності можливий лише за умови належного інформування європейців, а також регулювання мас-медіа має відбуватися не тільки на національному рівні, але й на європейському [23, с. 82].

Багато європейських документів стосується суспільного мовлення. У Резолюції про роль суспільного мовлення в мультимедійному суспільстві (жовтень 1996 р.) Європейський парламент підкреслив необхідність підтримки суспільного мовлення як ключового елемента в розвитку інформаційного суспільства. Однак Рада ЄС у своїй Резолюції від 25 січня 1999 р. висловила більш обережний підхід, зазначивши, що хоча суспільне мовлення має важливе значення, його державне фінансування не повинно порушувати ринкову кон'юнктуру та конкуренцію [53, с. 59].

Для більш детального розгляду специфіки регулювання медіа у Європі розглянемо її на прикладі кількох провідних європейських країн.

У Великобританії з 2003 року функціонує єдиний регуляторний орган у сфері телерадіомовлення, зв’язку та телекомунікацій – OFCOM. Ліцензії на мовлення поділяються на три категорії: наземне мовлення (категорія А), супутникове телемовлення та комерційні додаткові послуги (категорія В), кабельне та місцеве мовлення (категорія С). Ліцензування наземного, місцевого кабельного та супутникового телемовлення здійснюється на основі

запропонованої ціни заявки, за умови відповідності «порогу якості» програмних стандартів та фінансової спроможності виконувати зобов'язання протягом усього терміну дії ліцензії. Такий самий підхід застосовується до загальнонаціонального комерційного радіомовлення, з елементами аукціону та «конкурсу краси».

OFCOM має повноваження накладати санкції за порушення законів або програмних кодексів. Ці санкції варіюються від попереджень і вимоги опублікувати вибачення до штрафів, скорочення терміну дії ліцензії або її анулювання [16, с. 67].

В Італії головним регуляторним органом у сфері медіа та телекомунікацій є Орган регулювання зв'язку (AGCOM, або Autorità per le Garanzie nelle Comunicazioni). Його основні функції включають надання ліцензій і контроль за телекомунікаційними послугами, забезпечення конкуренції на ринку, а також регулювання засобів масової інформації з метою гарантування їх нейтральності та об'єктивності. AGCOM відповідає за дотримання правил і стандартів у галузі телекомунікацій та медіа в Італії, здійснюючи нагляд за відповідністю компаній вимогам законодавства [56].

Орган регулювання зв'язку в Італії (AGCOM) також має повноваження здійснювати моніторинг, зокрема аналізувати та збирати дані, стежити за плюралізмом думок, контролювати дотримання авторських і суміжних прав, а також виконувати посередницьку функцію у цих галузях. Моніторинг проводиться, зокрема, для застосування фінансових санкцій. Значне розширення повноважень цього органу відбулося на початку 2000-х років. Наприклад, у 2013 році AGCOM прийняв положення щодо захисту авторських прав, метою якого є боротьба з піратством та підтримка розвитку ринку контенту, зокрема, на електронних комунікаційних мережах.

AGCOM є незалежним адміністративним регуляторним органом, який має головний штаб у Неаполі і допоміжний оперативний офіс у Римі. Заснований у 1997 році, орган передбачав об'єднання функцій публічного адміністрування та різних компетенцій в одній інституції. На AGCOM покладено подвійне завдання:

забезпечення належної конкуренції між операторами на ринку та захист плюралізму й основних свобод громадян у секторах телекомунікацій, видавництва та медіа [42, с. 192].

У Німеччині держава відіграє значну роль у розвитку преси та суспільного мовлення. Хоча в країні немає федерального закону про пресу, кожна з 16 федеральних земель має власне законодавство, що регулює питання друку. Ідея створення єдиного «рамкового» федерального закону про пресу обговорюється ще з 1960-х років, і в 1980-х роках у Бонні розпочали підготовку відповідного законопроекту. Проте, робота над цим законопроектом продовжується в Берліні, і закон досі не прийнятий.

Німецькі журналісти, опираючись на лише одну статтю Конституції, суворо дотримуються рішень Федерального конституційного суду. Система державного управління в Федеративній Республіці Німеччини розподіляє повноваження між федеральним і земельним рівнями, при цьому федеральні землі відповідають за виконання державних повноважень, якщо Основний закон не встановлює інакше. Відповідно до абзацу 1 статті 75 Конституції Німеччини, федеральний уряд може видавати типові розпорядження щодо загальних правовідносин преси, які будуть спрямовані законодавцям у федеральних землях. Однак ці повноваження мають обмежений характер і не можуть надмірно втручатися у справи земель [54, с. 151].

На тлі зростання впливу соціальних медіа, однією з актуальних проблем є боротьба з недостовірною інформацією. У плані заходів, прийнятому країнами Європейського Союзу у 1998 році щодо забезпечення безпечного користування Інтернетом, визначаються методи протидії розповсюдженню протизаконного контенту в мережі.

Однак більш жорстку позицію щодо відповідальності в медійній сфері, закріплену у документі «Рекомендація Комітету міністрів державам-членам про роль та обов’язки інтернет-посередників» у 2018 році, також висловлює Рада Європи.

Для регулювання поширення нелегального контенту, що може підірвати довіру до цифрового середовища та становити загрозу для його подальшого розвитку, країни ЄС та інтернет-платформи активізували свої дії. Наприклад, спільно з Facebook, Twitter, YouTube, Microsoft був розроблений «Кодекс поведінки щодо мови ворожнечі в Інтернеті», який зобов'язує розглядати скарги щодо нелегального контенту протягом 24 годин. [58]. Німецький закон проти висловлювань ворожнечі, відомий як NetzDG, є яскравим прикладом зусиль урядів щодо регулювання пропаганди, що поширюється в соціальних мережах. Цей закон встановлює систему штрафів до 58 мільйонів доларів США для компаній, які ігнорують видалення постів, що порушують авторські права [62].

Установлення спільних медійних правил та законодавчого регулювання інтернету вимагає активне переміщення виборчих кампаній у соціальні мережі. Так, за час парламентської кампанії 2019 р. в сучасній Україні партії лише у Facebook витратили більше мільйона доларів США й опублікували понад 40 тисяч рекламних дописів.

У рамках світових тенденцій ці вибори підтвердили, що проблемою соціальних мереж залишаються маніпуляції та недостовірна реклама через відсутність дієвої системи правового унормування. Для вирішення питання щодо немаркованої реклами деякі фахівці пропонують законодавчо закріплене видання дозволу на рекламу лише верифікованим особам (як у США) або офіційним групам підтримки (як у Чехії та Словаччині). Уважаємо, що для подолання поширення маніпуляцій у Facebook чи Google українська держава повинна ініціювати добровільну співпрацю на основі конкретних законодавчих рішень та налагодження контактів із впливовими мережами та платформами.

Водночас спроби держав протидіяти цим загрозам часто створюють більш серйозні ризики для свободи вираження поглядів онлайн. Ідеться, зокрема, про блокування та фільтрування онлайн-контенту, координовані кампанії з поширення дезінформації, використання тролів і ботів, несанкціонований збір персональних даних, надсилання фішингових листів, злам облікових записів для залякування громадських активістів, практику «блекаутів» (вимкнення

Інтернету в усій країні) під час виборів, для попередження чи припинення протестів [38, с. 63].

Отже, міжнародний досвід захисту медійного контенту від кіберзагроз демонструє важливість комплексного підходу, який включає як технологічні, так і організаційні заходи. Значна увага приділяється розробці та імплементації передових методів шифрування та систем автентифікації для забезпечення цілісності та конфіденційності інформації. Законодавчі ініціативи встановлюють строгі вимоги до обробки та зберігання персональних даних, що посилює захист інформації в медіа. Важливу роль відіграє також міжнародна співпраця та обмін інформацією про кіберзагрози, що дозволяє швидко реагувати на нові види атак і розробляти ефективні стратегії захисту.

ВИСНОВКИ

Інформаційна безпека є ключовим аспектом сучасного життя, особливо у плані швидкого розвитку технологій та широкого доступу до інформації через медіа. Поняття інформаційної безпеки охоплює заходи та стратегії, спрямовані на захист конфіденційності, цілісності та доступності інформації в умовах зростаючих загроз кібератак, дезінформації та маніпуляції інформацією. Сьогодні інформаційна безпека набуває особливого значення через широке використання медіа як засобу комунікації та поширення інформації. Медіа не лише надають можливість швидкої та глобальної комунікації, але й впливають на формування громадської думки, світогляду та політичних уподобань. Зв’язок між інформаційною безпекою та медіа полягає в необхідності забезпечити безпеку та надійність інформації, яка поширюється через медіа, а також в усвідомленні загроз, які можуть виникнути внаслідок недостатньої захищеності інформації та можливого впливу медіа на формування думок та переконань громадськості.

Дослідження теми безпекового контенту у сучасних засобах масової комунікації (ЗМК) є актуальним і викликає великий інтерес у наукових колах через поширення та інтенсифікацію проблем дезінформації, маніпуляцій та негативного впливу інформації на аудиторію. Увага у цій галузі зосереджена на дослідженні концепції безпекового контенту, його ролі та впливу на сприйняття та поведінку аудиторії, а також на способах забезпечення безпеки в медіа, що є важливими аспектами в умовах інформаційної війни та загроз кібербезпеці. На сьогоднішній день проведено значну кількість досліджень, які розкривають різноманітні аспекти цієї проблематики. Серед цих досліджень можна виокремити аналіз ризиків, пов’язаних з поширенням недостовірної інформації та впливом маніпуляцій на громадську думку. Дослідники також вивчають критерії безпеки контенту, зокрема, оцінку достовірності джерел інформації, відстеження шкідливого впливу на аудиторію та розробку стратегій фільтрації

та контролю медіапростору для підвищення якості інформаційного середовища та забезпечення безпеки користувачів.

Основним завданням медіаресурсів «Детектор.медіа» та Центру протидії дезінформації є боротьба з фейками та маніпуляціями в медіа через впровадження різноманітних проєктів та стратегій з метою підвищення рівня медіаграмотності та забезпечення інформаційної безпеки. Журналісти «Детектор.медіа» спрямовують свою діяльність на виявлення та спростування фейків, аналіз новин на достовірність та підвищення медіаграмотності аудиторії. У свою чергу, Центр протидії дезінформації використовує комплексний підхід у боротьбі з дезінформацією, використовуючи сучасні технології та методи аналізу великих обсягів даних для виявлення та аналізу дезінформаційних явищ у онлайн-середовищі.

Методи та стратегії, які використовуються для гарантування якості та безпеки контенту у аналізованих медіаресурсах, включають систему фактчекінгу та перевірку достовірності інформації перед публікацією. Паралельно з цим, перевірка відповідності професійним етичним стандартам і принципам, які регулюють використання інформації без порушення приватності та безпеки осіб, виступає ключовим інструментом для забезпечення якості та безпеки журналістського контенту. Важливою практикою є також постійний моніторинг виконання журналістами професійних етичних стандартів та впровадження технологій для виявлення та фільтрації шкідливого контенту, що сприяє оперативному реагуванню на потенційні загрози й забезпечує безпеку користувачів. В комплексі ці заходи спрямовані на підвищення довіри громадськості до досліджуваних медіаресурсів та забезпечення безпеки та якості інформаційного середовища.

Медіаосвіта стає ключовим інструментом в боротьбі з дезінформаційним впливом країни-агресора на населення. Медіаосвіта сприяє формуванню критичного мислення та аналітичних навичок у громадян, допомагаючи їм відзрізняти об’єктивну інформацію від фейкової. Важливим є інформування громадян про методи та техніки дезінформації, що допомагає їм уникати впливу

маніпулятивних засобів інформації. Крім того, медіаосвіта сприяє підвищенню рівня знань громадян про загрози дезінформації та залучає їх до активної участі в формуванні інформаційного простору, де кожен має змогу висловлювати свою думку та ділитися об’єктивними джерелами інформації.

Міжнародний досвід демонструє, що захист медійного контенту від кіберзагроз є надзвичайно важливим у сучасному інформаційному середовищі. Ефективний захист від кіберзагроз передбачає активну співпрацю міжнародних партнерів та обмін інформацією про нові загрози та методи їх захисту. Технічні засоби є вкрай необхідними для захистумедійного простору від кібератак. Однак також важливими є питання профілактики та розвитку меідакомпетентності користувачів у галузі кібербезпеки, адже свідомість громадськості в цьому плані є ключовою для успішного захисту від кіберзагроз.

У результаті аналізу означеної теми мети дослідження було досягнуто, а завдання були повністю виконані.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналіз соціальних мереж. Детектор. Медіа. URL: https://detector.media/tag/31666/ (дата звернення: 20.04.2024)

2. Бараненко Р. Кібератаки як одна з форм кібертероризму. *Вчені записки ТНУ імені В.І. Вернадського.* 2021. № 1. С. 45–50. URL: https://www.tech.vernadskyjournals.in.ua/journals/2021/1_2021/part_1/9.pdf (дата звернення: 25.04.2024)

3. Бєлоусова Н., Афанасьєва П. Основні вимоги НАТО щодо забезпечення безпеки інформаційного простору. *Актуальні проблеми міжнародних відносин.* 2011. Вип. 102. С. 195–202. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/apmv_2011_102(1)__32.pdf (дата звернення: 27.04.2024)

4. Бєлошевич Я. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету ім. Т. Шевченка*. 2013. Вип. 30. С. 42–46. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/VKNU_vsn_2013_30_13.pdf (дата звернення: 23.04.2024)

5. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства. *Сучасна спеціальна техніка*. 2011. № 3 (26). С. 104–114.

6. «Військові навчання НАТО – репетиція третьої світової»: як російська пропаганда реагує на Steadfast Defender 2024. *Mediasapiens*. 25 січня 2024. URL: https://ms.detector.media/propaganda-ta-vplivi/post/34058/2024-01-25-viyskovi-navchannya-nato-repetytsiya-tretoi-svitovoi-yak-rosiyska-propaganda-reaguie-na-steadfast-defender-2024/ (дата звернення: 20.04.2024)

7. Глосарій. Механізми. Центр протидії дезінформації. URL: https://cpd.gov.ua/category/glossary/mechanisms/ (дата звернення: 20.04.2024)

8. ГО, ЗМІ та міжнародні експерти взяли участь у круглому столі щодо протидії дезінформації. Центр протидії дезінформації. 14 липня 2022. URL: https://cpd.gov.ua/events/3898/ (дата звернення: 02.05.2024)

9. Гой З., Білявська Ю. Медіаосвіта як засіб протистояння гібридним загрозам. *Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці:* Матеріали IV Міжнародної науково-практичної конференції (м. Київ, 22 листопада 2023 року). Київ: ДУІТ, ХНУРЕ, МНТУ. 2023. С. 55–57. URL: https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/12350/3/hybrid-threats-23-11-2023.pdf#page=55 (дата звернення: 03.05.2024)

10. Головка А. А. Діяльність сучасних ЗМІ в контексті інформаційної безпеки України. *Актуальні проблеми гуманітарних та природничих наук* (м. Ужгород, 08-09 квітня 2016 р.). Херсон: Видавничий дім «Гельветика», 2016. С. 85–87.

11. Детектор маніпуляцій. Детектор. Медіа. URL: https://detector.media/tag/2322/ (дата звернення: 04.05.2024)

12. Дошка ганьби. Детектор. Медіа. URL: https://detector.media/tag/31890/ (дата звернення: 06.05.2024)

13. Забара І. Міжнародна інформаційна безпека: сучасні концепції в міжнародному праві. *Theory and practice of jurisprudence*. 2013. Вип. 2.4. С. 74. URL: http://tlaw.nlu.edu.ua/article/view/63695/59192 (дата звернення: 20.04.2024)

14. Захаренко К., Міненко Є. Інститут медіа як суб'єкт інформаційної безпеки. *Науковий часопис УДУ імені Михайла Драгоманова*. 2023. Вип. 34. С. 29–36. URL: https://enpuir.npu.edu.ua/handle/123456789/44664 (дата звернення: 29.04.2024)

15. Іванов В., Волошенюк О. Медіаосвіта та медіаграмотність: короткий огляд. 2012. 58 с. URL: https://www.aup.com.ua/uploads/oglad-web.pdf (дата звернення: 30.04.2024)

16. Ільченко Н., Безугла Л. Регулювання діяльності засобів масової інформації: міжнародні принципи та європейський досвід. *Державне будівництво.* 2010. № 1. С. 67. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/DeBu_2010_1_41.pdf (дата звернення: 27.04.2024)

17. Квіт С.С. Масові комунікації. К. : Києво-Могилянська Академія, 2008. 206 с.

18. Кириченко М. Інформатизація як фактор оптимізації ідеології інформаційного суспільства та забезпечення його сталого розвитку. *ScienceRise: Pedagogical Education.* 2017. Вип. 1 (9). С. 46–50. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/texcped_2017_1_12.pdf (дата звернення: 25.04.2024)

19. Кізима І. Кібертероризм як глобальна проблема людства. *Матеріали Всеукраїнської науково-практичної інтернет-конференції педагогічних та науково-педагогічних працівників, аспірантів, молодих учених «Сучасні тенденції розвитку науки та освіти»:* зб. наук. пр. / Редкол.: Литовченко О.В. (голова) та ін. Ніжин, 2021. С. 392–397. URL: https://natc.org.ua/docs/Conferencia/2021/Conferencia_mat_20213011.pdf#page=392 (дата звернення: 07.05.2024)

20. Климчук О. О. Кіберпростір як нова арена воєнних дій. *Актуальні проблеми управління інформаційною безпекою держави:* зб. мат-лів наук.-практ. конф. (22 берез. 2011 р.): [у 2 ч.]. Ч. 2. К.: Наук.-вид. відділ НА СБ України, 2011. С. 29–33. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/boz_2011_25-26_39.pdf (дата звернення: 06.05.2024)

21. Концепція впровадження медіаосвіти в Україні : нова редакція / за ред. Л. А. Найдьонової, М. М. Слюсаревського. Київ, 2016. 16 с.

22. Крюков О. Інформаційна безпека держави в умовах глобалізації. *Державне будівництво*. 2007. Вип. 2. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/DeBu_2007_2_12.pdf (дата звернення: 23.04.2024)

23. Кукіна З. Правове регулювання діяльності засобів масової інформації в Європейському Союзі. *Міжнародне право*. 2012. Вип. 7. С. 81–85. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/urykr_2012_7_17.pdf (дата звернення: 06.05.2024)

24. Лисенко О. Кібертероризм як нова форма тероризму. *Соціальні та гуманітарні технології: філософсько-освітній аспект:* матеріали IV науково-практичної конференції (22-23 березня 2018 року, м. Черкаси) / Упор. Т. О. Дроздова. Черкаси : ФОП Гордієнко Є.І., 2018. С. 22–26. URL: https://er.chdtu.edu.ua/bitstream/ChSTU/842/1/%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D1%96%D1%8F%2C%202018.pdf#page=22 (дата звернення: 25.04.2024)

25. Ліпкан В., Максименко Ю. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006. 280 с. URL: https://duikt.edu.ua/uploads/l_1350_59375830.pdf (дата звернення: 28.04.2024)

26. Марущак А., Панченко В. До визначення поняття «інформаційна безпека». *Правничий вісник Університету «КРОК».* 2010. Вип. 1. С. 125. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Pvuk_2010_5(1)__18.pdf (дата звернення: 03.05.2024)

27. Медіаосвіта та медіаграмотність : підручник / ред.-упор. В. Іванов, О. Волошенюк; за наук. ред. В. Різуна. Київ : Центр вільної преси, 2012. 352 с.

28. Медіачек. Детектор. Медіа. URL: https://detector.media/tag/30052/ (дата звернення: 21.04.2024)

29. Методологія аналізу проросійських і окупаційних телеграм-каналів в українському сегменті телеграма. *Детектор. Медіа*. 14 грудня 2022. URL: https://detector.media/monitorynh-internetu/article/205956/2022-12-14-metodologiya-analizu-prorosiyskykh-i-okupatsiynykh-telegram-kanaliv-v-ukrainskomu-segmenti-telegrama/ (дата звернення: 20.04.2024)

30. Методологія Ініціативи «МедіаЧек» із розгляду скарг щодо порушень у журналістських матеріалах. *Детектор. Медіа*. URL: http://bit.ly/2JCC7Nf (дата звернення: 27.04.2024)

31. Методологія комплексного моніторингу дотримання телеканалами стандартів інформаційної журналістики. *Детектор. Медіа*. 17 квітня 2018. URL: https://detector.media/monitoring/article/136930/2018-04-17-metodologiya-kompleksnogo-monitoryngu-dotrymannya-telekanalamy-standartiv-informatsiynoi-zhurnalistyky/ (дата звернення: 04.05.2024)

32. Методологія комплексного моніторингу щоденних теленовин із використанням бази даних. *Детектор. Медіа*. 30 січня 2019. URL: https://detector.media/monitoring/article/144450/2019-01-30-metodologiya-kompleksnogo-monitoryngu-shchodennykh-telenovyn-iz-vykorystannyam-bazy-danykh/ (дата звернення: 08.05.2024)

33. Методологія оцінювання якості журналістських розслідувань. *Детектор. Медіа*. 4 жовтня 2016. URL: https://detector.media/monitoring/article/119360/2016-10-04-metodologiya-otsinyuvannya-yakosti-zhurnalistskykh-rozsliduvan/ (дата звернення: 08.05.2024)

34. Міжнародна інформаційна безпека: теорія і практика/ Макаренко Є.А., Рижков М.М., Ожеван М.А., Кучмій О.П., Фролова О.М./Підручник. Київ: Центр вільної преси, 2016. 418 с.

35. Мілль Дж. Про свободу: есе/ пер. з англ. Київ, 2001. С. 7–24. URL: http://litopys.org.ua/mill/mill01.htm (дата звернення: 30.04.2024)

36. Нерсесян Г. Медіаграмотність молоді – запорука протидії інформаційній агресії. *Інвестиції: практика та досвід*. 2018. № 6. С. 56–60. URL: http://www.investplan.com.ua/pdf/6_2018/14.pdf (дата звернення: 06.05.2024)

37. Нестеряк Ю. Узагальнення міжнародних принципів законодавчого регулювання медіа. *Аспекти публічного управління*. 2015. Вип. 11-12. С. 21–27. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/aplup_2015_11-12_5.pdf (дата звернення: 30.04.2024)

38. Новосельський І. Політико-правові засади функціонування нових медіа: світовий досвід та Україна. *Актуальні проблеми політики.* 2020. Вип. 65. С. 61–67. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/13f11b56-0f0e-4cee-8b86-1ebb05de77bd/content (дата звернення: 05.05.2024)

39. Онкович Г. Професійно-орієнтована медіаосвіта у вищій школі. *Вища освіта України*. 2014. № 2. С. 80–87.

40. Панченко О. Засоби масової інформації як джерело інформаційної безпеки. *Експерт: парадигми юридичних наук та публічного управління*. 2020. Вип. 2 (8). С. 250–258. URL: https://journals.maup.com.ua/index.php/expert/article/view/1692/2139 (дата звернення: 08.05.2024)

41. Перегуда Є. Медіаосвіта в умовах суспільної стабільності та в умовах війни. *Імідж України: соціально-політичні репрезентації і мовне віддзеркалення воєнних реалій у зарубіжних і вітчизняних мас-медіа*: тези доповідей міжнародної науково-практичної конференції (15-16 червня 2023 р., ОНУ імені І. І. Мечникова) / Ред.-упор. О. Сніговська. Одеса : ОНУ імені І. І. Мечникова, 2023. С. 178–184. URL: https://onu.edu.ua/pub/bank/userfiles/files/news/podii/imidzh_ukrainy_06-11_Print.pdf#page=178 (дата звернення: 30.04.2024)

42. Підберезних І. Порівняльна характеристика регуляторних органів публічного адміністрування телебачення Італії та України. *Вчені записки ТНУ імені В.І. Вернадського.* Серія: Юридичні науки. 2023. № 3. С. 190–194. URL: https://www.juris.vernadskyjournals.in.ua/journals/2023/3_2023/3_2023.pdf#page=196 (дата звернення: 02.05.2024)

43. Підмогильна Н., Дрозд А. Інтернет-проєкти як ресурс медіаосвіти. *Вчені записки ТНУ імені В. І. Вернадського*. Серія: Філологія. Соціальні комунікації. 2020. Том 31 (70). № 3. Ч. 3. С. 222–228. URL: https://philol.vernadskyjournals.in.ua/journals/2020/3_2020/part_3/37.pdf (дата звернення: 03.05.2024)

44. Полевий В.І. Понятійний апарат у сфері забезпечення інформаційної безпеки держави: тематичний збірник, довідкове видання. К.: Вид-во НА СБ України, 2005. 121 с.

45. Посібник з протидії дезінформації розроблено працівниками Центру протидії дезінформації робочого органу Ради національної безпеки і оборони України за підтримки Консультативної місії Європейського Союзу в Україні. Центр протидії дезінформації. URL: https://cpd.gov.ua/announcement/posibnyk-z-protydiyi-dezinformacziyi/ (дата звернення: 30.04.2024)

46. Практична медіаграмотність : посібник для бібліотекарів / Л. Гуменюк, В. Потапова ; ред.-упор. О. Волошенюк. Київ : Академія української преси, 2015. 200 с.

47. Про національну безпеку України: Закон України № 2469-VIII від 21.06.2018. *Відомості Верховної Ради України (ВВР).* 2018. № 31. ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 20.04.2024)

48. Про створення Центру протидії дезінформації: Рішення Ради національної безпеки та оборони № 106 від 19.03.2021. URL: https://zakon.rada.gov.ua/laws/show/n0015525-21#Text (дата звернення: 20.04.2024)

49. Про Центр протидії дезінформації. 22 грудня 2021. URL: https://cpd.gov.ua/documents/%d0%bf%d1%80%d0%be-%d1%86%d0%b5%d0%bd%d1%82%d1%80/ (дата звернення: 20.04.2024)

50. Сацюк В. Особливості інформаційної діяльності ОБСЄ. *Актуальні проблеми міжнародних відносин:* матеріали студентської наук. конференції, м. Київ, 20 травня 2021 р. / Київський університет імені Бориса Грінченка. Київ, 2021. С. 114–117. URL: https://fpmv.kubg.edu.ua/images/stories/Departaments/2021/Navchana_doslidgena/Stud_Konf_20.05.2021_Maalen.pdf#page=114 (дата звернення: 30.04.2024)

51. Солдатенко І., Зінюк А. Медіаграмотність як складова інформаційної безпеки. *Актуальні проблеми філософії та соціології*. 2016. Вип. 10. С. 138–140. URL: http://apfs.nuoua.od.ua/archive/10_2016/40.pdf (дата звернення: 23.04.2024)

52. Спецпроєкти. Детектор. Медіа. URL: https://detector.media/module/specprojects/ (дата звернення: 25.04.2024)

53. Стерлінг Христофор Х. Електронні ЗМІ в США. *Вісник Національної ради України з питань телебачення і радіомовлення.* 2001. № 3. С. 58–61.

54. Теребус О. Законодавче регулювання професійної діяльності журналістів у Німеччині. *Масова комунікація: історія, сьогодення, перспективи*: наук.-практ. журн. / відп. ред. С. І. Кравченко; упоряд. М. А. Рожило. Луцьк : Східноєвроп. нац. ун-т ім. Лесі Українки, 2016. № 9-10 (7). С. 149–153. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/12121/1/Terebus%20O.pdf (дата звернення: 26.04.2024)

55. Фролова О. Міжнародне співробітництво в галузі забезпечення інформаційної безпеки. *Вісник Львівського університету*. Серія міжнародні відносини. 2019. Вип. 46. С. 123–136. URL: https://scholar.archive.org/work/3ylpawilvjfh5nqxfp3gezqxy4/access/wayback/http://publications.lnu.edu.ua/bulletins/index.php/intrel/article/download/10365/10492 (дата звернення: 27.04.2024)

56. Autorità garante della concorrenza, AGCM e del mercato. *AGCM*. 2022. URL: https://www.agcm.it// (дата звернення: 23.04.2024)

57. Council of Europe. Recommendations and Declarations of the Committee of Ministers of the Council of Europe in the field of media and information society. 2015. 352 p. URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44 (дата звернення: 30.04.2024)

58. EU Code of Conduct against online hate speech: latest evaluation shows slowdown in progress. European Commission. 24 November 2022. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7109 (дата звернення: 30.04.2024)

59. European Commission, Television without Frontiers. Green Paper on the Establishment of the Common Market for Broadcasting, especially by Satellite and Cable, COM (84) 300, Brussels 14 June 1984)

60. International Encyclopedia of the Social & Behavioral Sciences. Vol. 14 / Eds. N. J. Smelser & P. B. Baltes. Oxford, 2001. P. 9494.

61. Media education. 1984. 406 p.

62. Network Enforcement Act (Netzdurchsetzunggesetz). digWatch. October 2019. URL: https://dig.watch/resource/network-enforcement-act-netzdurchsetzunggesetz-netzdg (дата звернення: 30.04.2024)

63. Recommendations Addressed to the United Nations Educational Scientific and Cultural Organization UNESCO. Education for the Media and the Digital Age. Vienna: UNESCO, 1999. P. 273–274.

64. Момот Н.М., Шурло А.В. Жанровий контент літературних журналів України. *Міждисциплінарні дослідження науки XXI століття*: матеріали II Всеукраїнської науково-практичної Інтернет-конференції молодих учених та студентів (1 грудня 2022 р., м. Київ). Київ: Університет «КРОК», 2022. С. 222–225.