МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Острозька академія»
Навчально-науковий інститут міжнародних відносин та національної безпеки
Кафедра міжнародних відносин

Кваліфікаційна робота

на здобуття освітнього ступеня магістра

на тему: **«Інформаційна безпека України: сучасний стан та перспективи»**

Виконала студентка 2 курсу, групи зММВ-2
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»,
освітньо-професійної програми
«Міжнародні відносини»

Волошина Ольга Миколаївна

Керівник – к.п.н., старший викладач,
Близняк Ольга Анатоліївна

Рецензент – к.н.д.у., старший викладач,
Шершньова Олена Володимирівна

Робота допущена до захисту
(протокол № ____ засідання кафедри міжнародних відносин від
_____20___року
Завідувач кафедри міжнародних відносин: _____
(прізвище ім’я й по батькові)

м. Острог – 2022 р.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

RAND	Research and Development – аналітичний центр у США
АІВ	акцій інформаційного впливу
ЗМІ	засоби масової інформації
ЗМК	засоби масової комунікації
ІВ	інформаційна війна
ІПсО	інформаційно-психологічна операція
СІО	спеціальні інформаційні операції

ВСТУП

Актуальність. На всіх етапах історичного розвитку цивілізації інформація була одним із головних засобів боротьби між народами, державами, військово-політичними блоками і союзниками. Найактивніше інформаційно-психологічне протиборство велося під час світових і локальних війн, національних і релігійних конфліктів. Інформаційна зброя не знищує противника безпосередньо, проте підриває його моральний стан, створюючи передумови до фізичної перемоги.

Інформація стала символом політичного впливу й економічного розвитку, а тому геополітичний авторитет держав на міжнародній арені, його можливості впливати на світові тенденції та події тепер залежать не тільки від економічної й військової могутності. Простежується тенденції, коли усе більшого значення набувають не силові, а інформаційні фактори: можливість ефективно впливати на інтелектуальний потенціал інших країн, поширювати й впроваджувати в суспільну свідомість відповідні духовні й ідейні цінності, трансформувати або підривати традиційні підвалини націй і народів.

Наша держава від 24 лютого 2022 року живе в умовах повномасштабного вторгнення Російської Федерації. До того ж, військова агресія супроводжується постійними спеціальними інформаційними операціями, пропагандою, дезінформацією, інформаційно-психологічними операціями, націленими на підрив обороноздатності держави в умовах воєнного стану та на викривлення загального сприйняття України як суб’єкта на міжнародній арені.

Саме тому важливо дослідити стан інформаційної безпеки держави, щоб визначити, які сьогодні існують найбільші загрози в інформаційному секторі, зрозуміти механізми їх розповсюдження в інформаційному просторі та способи впливу на суспільну свідомість. З огляду на швидкі темпи та динамічність подій, які змінюють реальність в інформаційному просторі, що викликано зокрема і російсько-українською війною, тема дослідження постійно потребуватиме нових аспектів висвітлення та аналізу.

Аналіз стану розробки проблеми. Сфера інформаційної безпеки досить глибоко досліджується як українськими, так і зарубіжними науковцями. Наше дослідження передбачає аналіз законодавчої бази сфери інформаційної безпеки України. Цей аспект глибоко досліджували такі українські науковці, як Баїк О., Коваль Г., Кобко В., Кобко Є.

Різновиди загроз та їх механізми впливу, які постають перед державами в інформаційній сфері на сучасному етапі розвитку, досліджували такі українські науковці: Остроухов В., Присяжнюк М., Хорошко В., Хохлачова Ю.

Не менш важливим аспектом дослідження є перспективи та виклики, які стоять перед цивілізованими суспільствами, які прагнуть до інформатизації та мирного співіснування в загальному інформаційному просторі. Зокрема, перспективи приєднання України до європейського інформаційного простору досліджували Климчук І., Солдатенко О., Солодка О., Сухорольська І., Фролова О., Черненко Т.

Варто зазначити, що недостатньо дослідженими є механізми протидії інформаційним загрозам, зокрема дезінформації, пропаганді, інформаційним спеціальним операціям. На системному державному рівні окреслено, які законодавчі норми повинні охороняти інформаційний простір від подібних атак, утім чітких механізмів протидії, окрім як виявлення і реагування на загрози, немає. Це також може бути пов’язано і з власне природою таких явищ інформаційної агресії. Адже стрімкий розвиток інформаційних технологій робить вразливими до атак навіть найбільш захищені об’єкти, інформаційні простори, наративи та візії держав.

Мета роботи полягає у дослідженні сфери інформаційної безпеки України на сучасному етапі розвитку, щоб зрозуміти перспективи держави у цій сфері.

Головними завданнями дослідження є: дослідити законодавчу базу України та основні нормативні документи, що відповідають за сферу інформаційної безпеки; визначити головні загрози для держави в інформаційному секторі в контексті російсько-української війни; окреслити

перспективи та завдання для держави, які необхідно виконати для успішного формування інформаційного суспільства в Україні.

Об'єктом дослідження є інформаційний простір України

Предметом дослідження є інформаційна безпека України, процеси які формують сучасний стан захищеності та/або незахищеності інформаційної безпеки нашої держави.

Теоретико-методологічна основа дослідження. У роботі використано низку загальнонаукових методів дослідження. Метод аналізу використаний під час вивчення нормативно-правової бази України в інформаційній сфері. За допомогою описового методу був досліджений головний масив документів, які формують законодавчу базу сфери інформаційної безпеки. Також методом аналізу ми з'ясували головні напрямки державної інформаційної політики, які окреслені у стратегічних документах.

Метод спостереження був використаний під час дослідження сектору засобів масової інформації та засобів масової комунікації на предмет наявності та функціонування в інформаційному просторі загроз різного рівня.

Метод порівняння був застосований під час аналізу європейського законодавства у сфері розвитку інформаційного суспільства та співставленні його із українською нормативно-правовою базою.

Хронологічні та географічні рамки. Хронологічні рамки роботи охоплюють період з 1991 по 2022 рік. Вибір цього часового періоду вмотивований тим, що з 1991 року Україна стала незалежним суб'єктом міжнародних відносин, почала активно формувати і провадити власну політику в багатьох сферах життя у тому числі і в контексті захисту свого інформаційного простору, засад інформаційної безпеки тощо. Верхня межа дослідження пов'язана із 2022 роком, коли в умовах повномасштабної війни в Україні триває активна робота у сфері захисту інформаційного простору, протидії гібридним війнам з боку країни-агресора, протидії дезінформаційним впливам на населення.

Географічні межі роботи охоплюють територію України в межах конституційних кордонів.

Джерельна база дослідження складається із законів України, які є основою для нормативно-правового сектору у сфері інформаційної безпеки, це зокрема: Конституція України, Закони України «Про національну безпеку України», «Про Службу безпеки України», «Про державну таємницю», «Про центральні органи виконавчої влади», «Про Раду національної безпеки і оборони України», «Про засади внутрішньої і зовнішньої політики», «Про основні засади забезпечення кібербезпеки України», «Про розвідку» та інші.

Важливими для аналізу також є стратегії та доктрини сектору інформаційної безпеки, це зокрема: Стратегія національної безпеки України, Воєнна доктрина України, Стратегія інформаційної безпеки, Доктрина інформаційної безпеки, Стратегія публічної дипломатії, Комунікаційна стратегія МЗС України, Директива ЄС про аудіовізуальні медіапослуги та інші.

Джерельна нормативно-правова база наукової роботи є досить широкою, відповідає меті та завданням нашої роботи.

Практичне значення і практична апробація. Практичні результати дослідження можна використовувати при розробці тематичних курсів, лекційних матеріалів, під час підготовки до семінарських занять з тематики інформаційної безпеки.

Структура роботи. Наукова робота складається із вступу, трьох розділів, поділених на підрозділи, висновків і списку використаних джерел та літератури. Загальна кількості сторінок – 75, обсяг роботи – 65 сторінок.

РОЗДІЛ 1. ІНФОРМАЦІЙНА БЕЗПЕКА В СИСТЕМІ ДЕРЖАВНОЇ ПОЛІТИКИ

1.1 Нормативно-правова база інформаційної безпеки в системі нацбезпеки держави

До повномасштабного вторгнення Росії в Україну 24 лютого 2022 року та подальшого застосування агресором ядерного шантажу, націленого проти всього континенту, у військовій справі довгий час простежувався постядерний етап – від стратегій ядерного стримування до високоточної контрсилової інформаційної зброї, що не загрожує людству глобальною катастрофою. За таких умов важливо з'ясувати місце та роль інформаційної безпеки в системі національної безпеки України.

Національна безпека охоплює оборону країни та всі види безпеки, передбачені Конституцією України та законодавством України, насамперед, державну, громадську, інформаційну, екологічну, економічну, транспортну, енергетичну безпеку, а також безпеку особи [19; с.30].

Інформаційна безпека є складовою національної безпеки, а тому регулюється Законом України «Про національну безпеку України» від 21 червня 2018 року. Основними термінами цього Закону є *«національна безпека України», «національні інтереси України», «загрози національній безпеці України».*

Відповідно до цього Закону розробляються і затверджуються Президентом України Стратегія національної безпеки України і Воєнна доктрина України, інші доктрини, концепції, стратегії і програми, якими визначаються напрями діяльності органів державної влади в конкретних умовах з метою своєчасного виявлення, запобігання та нейтралізації реальних і потенційних загроз національним інтересам України. Стратегія національної безпеки України і Воєнна доктрина України є документами, обов'язковими для

виконання, а також основою для розробки конкретних програм за складовими державної політики національної безпеки.

Рівень розвитку та безпека інформаційного середовища, які є одними з найвагоміших факторів у всіх сферах національної безпеки, активно впливають на стан політичної, економічної та інших складових національної безпеки України. А тому доцільно розглядати інформаційну безпеку як складову інших сфер національної безпеки, спрямовану на забезпечення національних інтересів у цих сферах. Разом з цим, інформаційна безпека є самостійно складовою національної безпеки, і в цьому проявляється її подвійний характер. [19; с.30]

Інформаційна безпека держави – це стан її захищеності та інформаційного розвитку, при якому акції інформаційного впливу, спеціальні інформаційні операції, інформаційні війни, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів та комп'ютерна злочинність не завдають суттєвої шкоди національним інтересам. [19; с.11]

Необхідний рівень інформаційної безпеки держави забезпечується створенням умов для гармонійного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод людини в інтересах держави: зміцнення конституційного ладу, суверенітету і територіальної цілісності країни, встановлення політичної і соціальної стабільності, економічного розвитку, безумовного виконання законів та міжнародного співробітництва.

Щоб зрозуміти, які є об'єкти інформаційної безпеки та загрози цим об'єктам в інформаційній сфері, доцільно розглянути сфери національної безпеки України.

Об'єктами інформаційної безпеки у *сфері державної безпеки* є інформаційні ресурси, що містять державну таємницю та іншу інформацію обмеженого доступу; засоби та системи інформатизації. Програмне забезпечення, автоматизовані системи управління, системи зв'язку та передачі даних, в яких циркулює інформація обмеженого доступу; технічні засоби та систем, що оброблять відкриту інформацію, але розміщені в приміщеннях, де

обробляється інформація обмеженого доступу; приміщення для закритих переговорів, під час яких озвучується інформація обмеженого доступу.

Загрозами інформаційній безпеці у цій сфері є протизаконна діяльність спецслужб іноземних держав й окремих осіб; порушення встановленого регламенту збору, обробки і передачі інформації; використання засобів і систем, які не сертифіковані відповідно до вимог щодо захисту інформації; залучення до робіт фірм, що не мають державних ліцензій. [19; с.32]

У *воєнній сфері* об'єктами інформаційної безпеки є інформаційна інфраструктура органів воєнного управління; інформаційні ресурси підприємств оборонного комплексу та науково-дослідних установ; програмно-технічні засоби автоматизованих і автоматичних систем воєнної сфери [19; с.32].

Загрози інформаційній безпеці у воєнній сфері поділяються на зовнішні та внутрішні. Зовнішніми загрозами є розвідувальна діяльність зарубіжних держав та інформаційно-технічний вплив з боку ймовірного противника. До внутрішніх загроз зараховують порушеного встановленого регламенту збору, обробки, зберігання та передачі інформації; навмисні дії а також помилки персоналу; невирішені питання захисту інтелектуальної власності. [19; с.32].

У зовнішньополітичній сфері об'єктами інформаційної безпеки є інформаційні ресурси, до яких входять органи державної влади, які реалізують зовнішню політику України, представництв і організацій за кордоном, представництв при міжнародних організаціях; а також ЗМІ, які роз'яснюють закордонній громадськості мету та основні напрями державної політики України, її погляди на соціально значимі події державного і міжнародного життя [19; с.33].

Загрозами у цій сфері є також як зовнішні, так і внутрішні фактори. До зовнішніх зараховують інформаційний вплив іноземних структур на зовнішню політику України; розповсюдження за кордоном дезінформації про зовнішню політику; порушення прав українських громадян та юридичних осіб в

інформаційній сфері за кордоном; спроби несанкціонованого доступу до інформації та впливу на інформаційні ресурси зовнішньої політики.

Внутрішніми загрозами для цієї сфери є пропагандистська діяльність, що спотворює стратегію і тактику зовнішньої політики України; недостатня поінформованість населення про зовнішню політику; порушення порядку збору, обробки, зберігання та передачі інформації в державних органах влади, зо реалізують зовнішню політику [19; с.33].

У *економічній сфері* об'єктами інформаційної безпеки є система державної статистики; кредитно-фінансова система; інформаційні та обчислювальні автоматизовані системи; системи бухгалтерського обліку; системи збору, обробки, зберігання та передачі інформації [19; 33].

Загрозами у цій сфері є безконтрольна діяльність виробників і споживачів інформації, засобів інформатизації та захисту інформації; безконтрольне залучення іноземних фірм до створення засобів інформатизації та захисту інформації; комп'ютерні злочини: проникнення кримінальних елементів у комп'ютерні системи і мережі банків та інших кредитних організацій.

У *екологічній сфері* об'єктами інформаційної безпеки є система прийняття рішень з надзвичайних ситуацій і ліквідації їх наслідків; система збору інформації про можливі надзвичайні ситуації [19; с.33].

Загрозами у цій сфері є приховування, несвоєчасне надання чи надання недостовірної інформації населенню про надзвичайні екологічні ситуації техногенного чи природного походження; недостатня надійність інформаційно-комунікаційних систем щодо збору, обробки, та передачі інформації в умовах надзвичайних ситуацій; низький рівень інформатизації органів влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпечних об'єктів і завчасного прогнозування та реагування на надзвичайні ситуації.

У *кіберсфері* об'єктами інформаційної безпеки є інформаційні ресурси фінансових установ, підприємств, транспорту та енергозбереження, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій.

Загрозами у цій сфері є невідповідність інфраструктури електронних комунікацій держави; недостатній рівень захищеності критичної інфраструктури; безсистемність заходів кіберзахисту; недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального та іншого характеру; недостатній рівень координації між суб'єктами забезпечення кібербезпеки [19; с.34]

У *інформаційній сфері* об'єктами інформаційної безпеки є засоби масової інформації, засоби масової комунікації, інформаційно-телекомунікаційні системи, автоматизовані системи управління, інформаційні ресурси.

Загрозами у цій сфері є прояви обмеження свободи слова і доступу до публічної інформації; поширення у ЗМІ, ЗМК культу насильства, жорстокості, порнографі; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, що становить державну таємницю, іншої інформації з обмеженим доступом; намагання маніпулювати суспільною свідомістю, зокрема через поширення недостовірної, неповної або упередженої інформації [19; с.34].

Основою безпеки України в секторі інформації є нормативно-правова база, яка регулює відносини в цій сфері, формує державну політику інформаційного безпекового сектора та забезпечує її реалізацію. Така законодавча база складається із великої кількість документів, серед яких головний – Конституція України, а також низки законів, підзаконних актів, державних програм, стратегій тощо.

Безпековий сектор, зокрема і у інформаційній сфері, базується на таких нормативних документах як Закони України «Про національну безпеку України» від 21 червня 2018 року, «Про Службу безпеки України» від 25 березня 1992 року, «Про державну таємницю» від 21 січня 1994 року України «Про центральні органи виконавчої влади», «Про Раду національної безпеки і оборони України» від 5 березня 1998 року, «Про засади внутрішньої і зовнішньої політики» від 1 липня 2010 року, «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року, «Про оборонні закупівлі» від 17

липня 2020 року, «Про розвідку» від 17 вересня 2020 року. тощо. Окрім цього, діє велика кількість підзаконних актів [27; с.167].

Розглянемо окремі документи детальніше. Відповідно до ст. 7 Закону України «Про центральні органи виконавчої влади» одним із завдань міністерств *є інформування та надання роз'яснень щодо здійснення державної політики* [17]. Основними засадами внутрішньої політики України у сфері національної безпеки і оборони, відповідно до ст. 6 Закону України «Про засади внутрішньої і зовнішньої політики», є *забезпечення життєво важливих інтересів людини і громадянина у сфері інформації* [10]. У Законі України «Про запобігання корупції» серед повноважень Національного агентства ст. 11 передбачає *інформування громадськості про здійснювані ним заходи щодо запобігання корупції,* ст. 31 – *обмеження доступу до певної інформації*, ст. 43 – *нерозголошення інформації*, ст. 46 – *встановлює перелік інформації, яка зазначається в декларації осіб, уповноважених на виконання функцій держави або місцевого самоврядування*, а ст. 60 *встановлює вимоги щодо прозорості та доступу до інформації* [7].

У Законі України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їх символіки» у ст. 5 йдеться, що *держава вживає заходів, спрямованих на підвищення інформованості громадськості про злочини, вчинені представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів* [8]. Окрім того, у Законі України «Про Державне бюро розслідувань» у п. 16 ст. 6 йдеться *про забезпечення відповідно до законодавства й додержання режиму захищеної законом таємниці та іншої інформації з обмеженим доступом, а також визначеного законом порядку оприлюднення та надання доступу до публічної інформації* [18]. Рішенням Ради національної безпеки і оборони від 11 березня 2021 року створено Центр протидії дезінформації, основним призначенням якого є *протидія загрозам національної безпеки та національних інтересів України в інформаційній сфері, боротьба з пропагандою, деструктивними інформаційними впливами та*

компаніями, недопущення маніпулювання громадською думкою [35]. Відповідно до ст. 11 Кодексу адміністративного судочинства України, одним із принципів адміністративного судочинства в Україні є відкритість інформації щодо справи, що закріплює право громадян на отримання в адміністративному суді як усної, так і письмової інформації щодо результатів розгляду справи: «*..ніхто не може бути обмежений у праві на отримання в адміністративному суді інформації про дату, час і місце розгляду своєї справи та ухвалені в ній судові рішення*» [22].

Окрім низки законів, обов'язковими до виконання є стратегії, які формують напрямок політики держави у відповідній сфері. Для сектору національної безпеки, зокрема в інформаційному аспекті, важливими є Стратегія воєнної безпеки та Стратегія інформаційної безпеки, які є складовими Стратегії національної безпеки.

Зокрема, Стратегія воєнної безпеки «Воєнна безпека – всеохоплююча оборона» 2021 року в інформаційній сфері передбачає комплекс заходів, до яких належать:

– протидія Української держави в кіберпросторі та нав'язування своєї волі в інформаційному просторові;

– налагодження публічними органами управління надійних каналів комунікації з населенням;

– конкуренція України з іншими державами у створенні сучасних інформаційних технологій (систем) з метою отримання повної та достовірної інформації для своєчасного ухвалення рішень щодо забезпечення воєнної безпеки держави;

– розгортання захищеної мережі обміну інформацією між органами управління сил оборони, яка відповідає вимогам до захисту інформації [43].

Стратегія інформаційної безпеки України є більше предметною для нашого дослідження, тому її варто розглянути детальніше у наступному підрозділі.

Отже, інформаційна безпека є не тільки самостійною складовою національної безпеки, а й складовою інших сфер національної безпеки держави. Прогресивний розвиток України як сучасної правової держави можливий тільки за умови забезпечення інформаційної безпеки всіх суб'єктів інформаційних відносин.

Основою безпеки України в секторі інформації є нормативно-правова база, яка регулює відносини в цій сфері, формує державну політику інформаційного безпекового сектора та забезпечує її реалізацію. Така законодавча база складається із великої кількість документів, серед яких головний – Конституція України, а також низки законів, підзаконних актів, державних програм, стратегій.

1.2 Реалізація цілей Стратегії інформаційної безпеки України в умовах воєнного стану.

Стратегія інформаційної безпеки є одним із низки документів, які розробляються для реалізації Стратегії національної безпеки України. Її метою є створення умов для забезпечення інформаційної безпеки України, спрямованої на захист важливих інтересів громадянина, суспільства та держави у протидії внутрішнім та зовнішнім загрозам, забезпечення захисту державного суверенітету і територіальної цілісності України, підтримка соціальної та політичної стабільності, оборони держави, забезпечення прав та свобод кожного громадянина. Реалізація Стратегії розрахована на період до 2025 року.

Варто зазначити, що Стратегія є програмним документом, що формує основи для майбутньої політики держави. Відповідні документи зазвичай не передбачають детальний перелік заходів, який згодом встановлюється конкретним планом дій. Однак, Стратегія вказує на майбутні тренди державної політики, тому більшість застережень мають практичний характер і повинні бути реалізовані.

Стратегія складається із 5 частин: Загальні положення, Аналіз загроз та викликів інформаційній безпеці, Стратегічні цілі та напрями реалізації Стратегії, Механізми реалізації мети та завдань, Очікувані результати. [46]

Серед ключових загроз, які автори Стратегії вбачають для інформаційної безпеки, визначені збільшення кількості дезінформаційних кампаній, інформаційна політика Російської Федерації, низький рівень медіаграмотності громадян у поєднанні зі стрімким поширенням цифрових технологій [46].

Стратегія також визначили 7 основних цілей, які власне і відображають плани уряду у сфері інформаційної безпеки:

- протидія дезінформації та інформаційним операціям;
- забезпечення всебічного розвитку української культури та утвердження загальнонаціональної ідентичності;
- підвищення рівня медіакультури та медіаграмотності;
- забезпечення дотримання конституційних прав особи на свободу вираження та захист приватного життя, захист прав журналістів і протидія поширенню незаконного контенту;
- створення ефективної системи стратегічних комунікацій;
- інформаційна реінтеграція тимчасово окупованих територіях;
- розвиток інформаційного суспільства та підвищення рівня культури діалогу.[46]

Розглянемо детальніше пункти Стратегії, щоб зрозуміти мету та завдання кожного напрямку.

1.Протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованих на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету та територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, проведення терористичних актів, посягання на права та свободи людини [46].

Серед головних завдань цього пункту Стратегії – створення системи протидії інформаційним операціям та атакам, створення системи раннього виявлення загроз, протидія заходам країни-агресора. Серед ключових планів – перегляд та вдосконалення законодавства щодо:

– відповідальності за поширення дезінформації *«для збільшення ефективності впливу на державу-агресора та мінімізації шкоди для своїх національних інформаційних інтересів»*;

– виявлення, фіксації, обмеження доступу та/або видалення з українського сегменту Інтернету інформації, розміщення якої заборонено законом;

– взаємодії у сфері інформаційної політики силових структур України з органами державної влади, органами місцевого самоврядування та громадськими інституціями [46].

В умовах воєнного стану, для країни особливо актуальним постало питання необхідності єдиної інформаційної політики. Так, Президент України підписав Указ про введення в дію рішення Ради національної безпеки і оборони України *«Щодо реалізації єдиної інформаційної політики в умовах воєнного стану».* Згідно з Указом, головним інструментом боротьби України проти російської дезінформації під час воєнного стану є правда, яку потрібно доносити не тільки до внутрішньої, а й до закордонної аудиторії: *«..в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об'єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації - цілодобовому інформаційному марафоні «Єдині новини #UAразом»* [46].

Наступним не менш важливим напрямком Стратегія визначає розвиток української культури та збереження української ідентичності.

2. Забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності. Однією із головних цілей російських окупантів протягом століть було знищення української

культури та української ідентичності. Уряд України ухвалив цілком виважене рішення, дозволивши установам культури та мистецтв відновити роботу в умовах воєнного стану. Про важливість культурного виміру говорив класик світової політики Вінстон Черчилль: *«Якщо ми економимо на культурі, то за що ми воюємо?»*.

Сьогодні Українська культура формує імідж країни на міжнародній арені, розповідає світу, ким дійсно є українці, якщо забрати російську призму формування меншовартості. У цьому аспекті важливим є спільний проект Міністерства культури та інформаційної політики України, Державного агентства України з питань мистецтв та мистецької освіти а також їх партнерів «Ukraine Now and Forever». Головна мета проекту – привернути увагу світу до української культури і мистецтва, а також поглибити консолідацію міжнародної спільноти у боротьбі проти російської агресії. [46].

Окрім цього, Стратегія наголошує на важливості медіакультури та медіаграмотності українського суспільства.

3. Підвищення рівня медіакультури та медіаграмотності суспільства. В умовах інформаційної війни, яка є складовою широкомасштабної війни Росії проти України, поширюється масив фейкових новин, дезінформації, пропаганди та різного роду маніпуляцій. Тому важливо, щоб суспільство могло виокремлювати сере всього інформаційного потоку саме правдиві повідомлення. Для цього необхідно отримувати інформацію тільки з перевірених джерел, а також послуговуватися провідними українськими ресурсами, робота яких полягає у викритті російських інформаційних атак, – *Детектор медіа, StopFake, Центр протидії дезінформації при РНБО, Центр стратегічних комунікацій.*

4. Забезпечення дотримання конституційних прав особи на свободу вираження та захист приватного життя, захист прав журналістів і протидія поширенню незаконного контенту [46]. Враховуючи, що доступ до інформації є одним із основних прав громадянина, яке захищає ст. 34 Конституції України, влада має забезпечити необхідні умови, щоб таке право

не порушувалося. Окремо варто зазначити про права журналістів. Важливо, що їхня діяльність згадана у Стратегії, оскільки через викривлене виконання пункту 1 цього документу, влада може цензурувати роботу окремих ЗМІ та журналістів. Тому важливо розрізняти, де є інформація, поширення якої шкідливе для держави в умовах воєнного стану, а де протидія роботі журналістів. Фаховий аналіз роботи журналістів проводить *Детектор медіа* та *Інститут масової інформації.*

5. *Інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та прилеглих до них територіях України, до загальноукраїнського інформаційного простору* [46].Досягнення цієї мети було досить складним завданням ще до повномасштабного вторгнення Росії в Україну. Засоби масової інформації, насамперед телеканали, є особливо ефективними інструментами як для просування ворожої пропаганди, так і для формування українського інформаційного простору, який би відповідав вимогам європейської спільноти. Саме тому цьому питанню варто приділити особливу увагу одразу після перемоги України. Але вже зараз можна напрацьовувати орієнтовний план дій, продумувати програми та проекти, які пришвидшать процес інформаційної реінтеграції в майбутньому.

6. Створення ефективної системи стратегічних комунікацій, метою якої є гарантування ефективної інформаційної взаємодії між органами державної влади, органами місцевого самоврядування та суспільством з питань кризових ситуацій. Зміцнення позитивного іміджу України [46]. Якщо стратегічні комунікації це система внутрішніх і зовнішніх комунікацій, то зв’язки з громадськістю – одна зі складових стратегічних комунікацій. В умовах війни органи державної влади, органи місцевого самоврядування продемонстрували досить високий рівень інформаційної взаємодії із суспільством. Міністерства та відомства систематично оприлюднюють актуальну інформацію, а щоденні виступи Президента України та Голів обласних військових адміністрацій інформують про поточну ситуацію в державі, на міжнародній арені та успіхи наших військових на фронті.

7. Розвиток інформаційного суспільства та підвищення рівня культури діалогу. Завдяки сучасним інформаційним технологіям Україна швидко та ефективно отримувала інформацію про наміри ворога, зокрема і від іноземних партнерів. Застосування інформаційних технологій у військовій сфері відкрило нові можливості щодо забезпечення оборони держави, які дозволяють попереджати нові атаки агресора, оперативно проводити дипломатичний діалог та діалог на найвищих щаблях влади, консолідуючи позицію та зусилля міжнародної спільноти проти країни-агресора. Об'єднання українського інформаційного простору з міжнародним дозволило зламати одновекторність російської пропаганди, націленої проти України. Найбільшим досягнення у цьому аспекті є те, що Кремль вперше за багато років програв світове інформаційне поле [46].

Розділ Стратегії *«Механізми реалізації визначеної мети та завдань»* передбачає розподіл обов'язків між органами влади в процесі імплементації документу. РНБО виконуватиме координуючу роль, Кабінет Міністрів відповідатиме за формування та реалізацію інформаційної політики, фінансування та розробку і прийняття плану заходів з реалізації Стратегії. Серед завдань СБУ визначається необхідність моніторингу спеціальними методами, каналами ЗМІ та Інтернету з метою виявлення загроз національній безпеці в інформаційній сфері, що може становити загрозу для цифрових прав. Водночас, проект Стратегії не визначає головного органу влади, відповідального за звітування щодо впровадження Стратегії.

Отже, Стратегія є важливим рамковим документом, який визначає пріоритетний напрямки в реалізації політики держави щодо інформаційної безпеки. Аналізуючи головні меседжі Стратегії, важливо також зазначити, що будь-які законодавчі заходи, спрямовані на протидію дезінформації та обмеження доступу до шкідливого контенту в Інтернеті, можуть обмежувати і право на свободу вираження поглядів, доступу до інформації, право на журналістську діяльність. Тому диференціація термінів, дій та прав громадян у цьому вимірі має бути дуже чіткою. Також діяльність державних органів, що

залучені до імплементації Стратегії, має бути прозорою та з чітким розподілом повноважень.

Висновок до розділу 1

Інформаційна безпека як окрема сфера є важливою складовою національної безпеки України. Окрім цього, питання інформаційної безпеки розглядаються і в контексті інших сфер національної безпеки держави. Адже розвиток України як сучасної правової держави можливий тільки за умови забезпечення інформаційної безпеки всіх суб'єктів інформаційних відносин.

Нормативно-правова база є основою безпеки для інформаційного простору України. Вона забезпечує державну політику інформаційного безпекового сектора та гарантує її реалізацію. Така законодавча база складається із великої кількість документів, серед яких головний – Конституція України, а також низки законів, підзаконних актів, державних програм, стратегій. Варто зазначити, що українське законодавство має достатньо документів для регулювання інформаційної сфери. Утім, не досить повно реалізована практична сторона головних стратегій та доктрин, тобто чітких планів дій, з урахуванням останніх викликів.

Особливо важливою для інформаційного сектору є Стратегія інформаційної безпеки. Це рамковий документом, який визначає пріоритетні напрямки в реалізації політики держави щодо інформаційної безпеки. Аналізуючи головні її меседжі, важливо вказати на диференціацію термінів, дій та прав громадян, які прописані в цьому документів. Адже за відсутності чіткого плану реалізації цієї Стратегії деякі її положення, зокрема про дезінформацію, можуть трактуватися двозначно на користь заангажованих осіб.

РОЗДІЛ 2. ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ НА СУЧАСНОМУ ЕТАПІ РОЗВИТКУ ДЕРЖАВИ

2.1 ЗМІ та спеціальні інформаційні операції як основний інструмент інформаційного протиборства

Основні тенденції зміни характеру геополітичної боротьби держав, розвиток процесу глобалізації на початку XXI століття свідчать про те, що разом із традиційними силовими методами та засобами вирішення завдань у цій сфері все частіше використовуються інформаційні.

Основним засобом ведення інформаційного протиборства є національні й транснаціональні ЗМІ, а також будь-які інші інформаційні мережі, здатні впливати на світогляд, політичні погляди, правову свідомість, менталітет, духовні ідеали та ціннісні орієнтири як окремої людини, так суспільства в цілому.

Американські фахівці вважають інформаційне протиборство не просто видом забезпечення операцій збройних сил через порушення процесів контролю та управління військами, алей таким, що виходить далеко за межі цих проблеми. Згідно із результатами досліджень, які проводили фахівці американського стратегічного дослідного центру RAND наприкінці 90-х років вперше застосовано термін *«стратегічне інформаційне протиборство».* Згідно із дослідженням, таке протиборство передбачає використання державами глобального інформаційного простору та інфраструктури для проведення стратегічних військових операцій і зменшення впливу на власний інформаційний ресурс. Дослідження дозволили виділити ключові особливості такого виду протиборства: відносно низька вартість створення засобів інформаційного протистояння і крах статусу традиційних державних кордонів під час підготовки й проведенні інформаційних операцій.

Наступні дослідження проблеми запропонували введення поняття *«стратегічне інформаційне протиборство другого покоління».* У звіті воно

визначається як принципово новий тип стратегічного протиборства, породжений інформаційною революцією, що зараховує інформаційний простір до низки можливих сфер протиборства. Наголошується, що розвиток і вдосконалення підходів до ведення стратегічного інформаційного протистояння другого покоління в перспективі може призвести до повної відмови від використання військової сили. По суті, інформаційне протиборство другого покоління зводиться до зусиль із видозміни противника: до знищення його традиційного змісту на наповнення новим.

Сьогодні інформаційний простір фактично стає театром воєнних дій, де кожна протиборча сторона прагне отримати перевагу. Таким чином поява єдиного глобального інформаційного простору, що є природним результатом розвитку світової науково-технічної думки й удосконалення комп'ютерних та інформаційних технологій, створює передумови до розробки і застосування нових засобів ведення інформаційного протиборства– інформаційну зброю.

Інформаційна зброя – це комплекс специфічних програмно-інформаційних засобів, створених для ураження інформаційного ресурсу противника. Як свідчить досвід локальних війн і збройних конфліктів кінця XX –початку XXI століття, на відміну від ударної високоточної зброї, яка точково вражає визначені об'єкти, інформаційна зброя є системоруйнівною. Тобто, вона виводить з ладу бойові, економічні й соціальні системи. За результатами впливу інформаційну зброю можна прирівняти до зброї масового ураження. [19; с.114].

Окрім військової галузі, інформаційна зброя може використовуватися в економічній, банківській, соціальній та інших сферах з такою метою:

– дезорганізація діяльності управлінських структур, транспортних потоків і засобів комунікації;

– блокування діяльності окремих підприємств та банків, а також цілих галузей промисловості через порушення багатоланкових технологічних зав'язків і системи взаєморозрахунків, проведення валютно-фінансових махінацій тощо;

– ініціювання великих техногенних катастроф на території супротивника внаслідок порушення штатного управління технологічними процесами та об’єктами, що мають справу з великими об’ємами небезпечних речовин і високих концентрацій енергії;

– масового поширення і впровадження у свідомість людей визначених уявлень, звичок і поведінкових стереотипів;

– спричинення невдоволення чи паніки серед населення, а також провокування деструктивних дій різних соціальних груп. [19; с.114].

Інформаційній зброї притаманні такі характеристики як цілеспрямованість, вибірковість, розосередженість, масштабність впливу, досяжність, швидкість доставки, комплексність впливу на людей, технічні засоби й системи, можливість регулювання (дозування) «потужності» впливу, що визначає її як зброю масового ураження. [19; с.120].

До *видів інформаційної зброї* науковці умовно зараховують 6 груп засобів, які застосовують для деструктивних інформаційних впливів:

- засоби масової інформації (радіо, преса, телебачення) і агітаційно-пропагандистські засоби (відеокасети, електронні підручники, енциклопедії;
- психологічні засоби (спеціальні генератори, спеціальна відеографічна і телевізійна інформація, відеозасоби типу віртуальної реальності);
- електронні засоби (оптико-та радіоелектронні засоби, спеціальні передавач, випромінювачі електромагнітних хвиль та імпульсів);
- засоби спецального програмно-математичного впливу (комп’ютерні віруси)
- лінгвістичні засоби (мовні одиниці, спеціальна термінологія, мовні звороти, що мають семантичну неоднозначність після перекладу на інші мови)
- психотропні засоби (спеціально структуровані ліки, транквілізатори, анти депресанти, галюциногени, наркотики, алкоголь тощо) [19;с.123].

Відтак, володіння інформаційною зброєю і ефективними засобами захисту від неї стає однією з головних умов забезпечення національної безпеки держави в XXI столітті.

В сучасних умовах глобалізації відбувається інтенсивне використання ЗМІ для ведення інформаційних війн з метою забезпечення власних інтересів світовими лідерами. Беззаперечним є факт нарощування інтенсивності використання інформаційних маніпуляцій як інформаційної зброї і окремими державами, і зарубіжними організаціями, подекуди терористичними. До того ж, із глобалізацією та тотальною інформатизацією світу, тероризму як явищу вдається швидше та ефективніше досягати своїх головних цілей, серед яких масове залякування населення, шантаж влади та дезінформація супротивника.

Раніше терористична діяльність обмежувалася усуненням конкурентів у боротьбі за владу або для досягнення інших обмежених цілей. Зараз же тероризм вийшов на державний рівень – у вигляді прямої або опосередкованої підтримки відповідних організацій *(Наприклад, підтримка Росією терористичних організацій Близького Сходу, Африки).*

Ідеологи і керівники терору розуміють важливість інформаційної складової. Адже теракт, особливо успішний, що не має широкої інформаційної складової, наполовину, або навіть більше, вважається девальвованим. Ось чому поряд з технічними, організаційними, фінансовими та іншими аспектами теракту сучасні терористичні організації ретельно підходять до відпрацювання інформаційного забезпечення.

Так, дослідники виділяють головні складові пропагандистської (інформаційної) роботи терористичних організацій.

По-перше, створення спеціалізованих ЗМІ, їхнє матеріальне, організаційне, технічне забезпечення. Для таких ЗМІ формуються журналістські колективи, склад яких дуже різний і часто специфічний, з урахуванням покладених завдань і національних особливостей. Їхня мета в тому, щоб простими лінійними гаслами залучити нестійких, позбавлених

аналітичного мислення, малоосвічених людей для виконання потрібної ролі [33; с. 67].

По-друге, у мобілізації новобранців в терористичні організації не останню роль відіграє матеріальний фактор. Наприклад, досвід боротьби з тероризмом в Латинській Америці показує, що як тільки підвищується життєвий рівень населення, підтримка бойовиків згасає. На терористичних сайтах питання матеріальної винагороди подається завуальовано, але охочі завжди можуть знайти відповідь на запитання, які їх цікавлять [33; с.67].

По-третє, досить важливим для терористичних організацій є проблема пошуку форм співпраці із засобами масової інформації, журналістами, не пов'язаними безпосередньо з тероризмом, його організаторами і натхненниками. Для більшості ЗМІ дуже важливими є два фактори: оперативність і ексклюзивність. Саме їх і використовують терористичні організації. Для деяких, переважно відомих і авторитетних журналістів, влаштовуються ексклюзивні інтерв'ю з керівниками, ідеологами терористичних організацій. Зазвичай вони ретельно конспіруються задля безпеки, а також з навіювати утаємниченість щодо місцезнаходження і діяльності [33; с.68].

Утім варто зауважити, що не всі журналісти погоджуються спілкуватися з терористами з етичних міркувань, оскільки розглядають це як пособництво в убивстві людей. Проте бажання поговорити з лідерами терористів, побувати в таборах підготовки бойовиків здебільшого переважують етичні застереження. До того ж, якщо один телеканал відмовиться, то таке інтерв'ю, досить ймовірно, транслюватиме вже інший.

Окрім того, PR-служби терористів підбирають ЗМІ, які погодяться публікувати їхні матеріали. Практично це відбувається з використанням сучасних засобів зв'язку: або ж в редакцію заздалегідь надходять відповідні матеріали, або редакцію попереджають про подію найчастіше за кілька хвилин до теракту, коли перешкодити йому неможливо або надзвичайно важко.

Така реальність загострює проблему інформаційної вразливості країни в епоху глобалізації та потребує розробки й впровадження системи забезпечення

інформаційної безпеки через захист не тільки інформаційного простору держави, а і захисту від інформаційних маніпулювань та інформаційної уразливості громадян і суспільства загалом. Сьогодні технології ІПсО, які зокрема і Росія використовує проти України, спрямовані на утриманні медійної переваги в міжнародному інформаційному просторі. І при цьому не надто важливо, наскільки компетентними та авторитетними є ті, чи ті російські ЗМІ. У цьому випадку працює метод безперервної постійної агресивної пропаганди.

В умовах широкомасштабного вторгнення країни-агресора в Україну, варто розглянути загальні *специфічні ознаки проведення ІПсО*, які направленні на дестабілізацію головних сфер держави:

– посилення зовнішнього інформаційного впливу на декілька окремих верств населення, передусім на національні меншини у місцях їх компактного проживання;

– обмеження доступу країни до світових інформаційних ресурсів;

– наявність фахівців, передусім в системі державного управління, діяльність яких має відкриту підтримку у закордонних ЗМІ;

– зростання кількості національних ЗМІ, що мають іноземних власників;

– велика увага до подій всередині країни з боку іноземних ЗМІ та міжнародних установ, створення різноманітних наглядових, консультаційних та дорадчих органів з боку іноземних держав;

– культурна експансія іноземних держав, перенасиченість ринку інформаційних послуг продукцією іноземного виробництва, нав’язування іноземних інформаційних технологій та перешкоджання створенню та впровадження власних [19; с.269].

З огляду на перелік ознак проведення ІПсО, більшість з них можуть бути виявленні через аналіз кількісно-якісних характеристик змісту повідомлень в українському інформаційному просторі. Також на основі вказаного переліку можна визначити єдиний критерій виявлення ознак ведення інформаційно-психологічних операцій.

Одне з центральних місць у психологічному просторі держави в цілому займає *офіційна позиція* щодо будь-яких подій, явищ та процесів, які відбуваються в державі. Основним носієм інтересів держави є законодавчі та нормативно-правові акти у різних сферах її діяльності. Очевидно, що найбільш небезпечним є ІПсО, які орієнтовані на *збільшення розбіжностей між офіційною позицією держави і поглядами, настроями, думками її соціальних груп*. Інструментами проведення ІПсО у такому випаду є ті ЗМІ, повідомлення яких регулярно переглядає та яким довіряє об'єкт. Сукупність таких ЗМІ і визначає інформаційний простір об'єкта, через який здійснюється вплив на його психологічний простір. Відтак очевидно, що для проведення ІПсО проти соціальної групи будь-якої держави, обов'язковим є залучення ЗМІ всередині країни, навіть якщо замовником операції є зовнішня сила. [19; с.270]

Отже, загальним критерієм виявлення ознак ведення ІПсО проти України може бути розбіжність змісту повідомлення у ЗМІ з офіційною позицією України щодо варіантів вирішення або бачення конкретної проблеми, за умови можливості ознайомлення соціальної групи з цими повідомленнями. Утім слід чітко розрізняти, де є незалежна критика державної політики, громадський контроль та моніторинг процесів у владі, які здійснюються зокрема і через ЗМІ, а де розбіжність у ґрунтовних позиціях держави і провідних ЗМІ, що спричинені впливом ІПсО. Показником ведення ІПсО також може бути *напруженість відносин між соціальною групою та державою*, що відбувається у випадку досягнення ІПсО своєї мети.

Яскравим прикладом ІПсО є історія про нібито контрабандну зброю з України, яку запустила країна-агресор. Розглянемо, як розкручувався її механізм.

У липні 2022 року британська газета Financial Times написала про «контрабанду» зброї з України, а згодом скорегувала заголовок, уточнивши, що є «ризики контрабанди». У матеріалі йшлося про те, що в Україні нібито відсутня система контролю за розподілом зброї, яка надходить із Заходу. У ЄС

на це заявили, що Росія подібними чутками намагається зірвати постачання зброї в Україну.

Голова МЗС України Дмитро Кулеба заявив, що наратив про «контрабанду» зброї з України стовідсотково запустила РФ, а видання Financial Times несвідомо його підхопило. Радник керівника Офісу президента України Михайло Подоляк натомість прокоментував, що намагання зірвати постачання зброї – це ключова мета російських інформаційних операцій сьогодні.

Своєю чергою, секретар РНБО Олексій Данілов доповідав, що іноземним та українським журналістам на закритій зустрічі пояснили, як контролюється розподіл західної зброї в Україні, але поширювати цю інформацію не можна [25].

Отже, хоч причетність України до контрабандної зброї спростована, але сам факт поширення публічного діалогу на цю тему та коментування від офіційних осіб держави підігріває увагу аудиторії. І якщо громадяни України переважно вже розуміють, як працюють такі дискредитаційні кампанії, то, наприклад, у європейського громадянина, або громадянина США все ще можуть виникати сумніви.

Отже, основним засобом ведення інформаційного протиборства є національні й транснаціональні ЗМІ. В сучасних умовах глобалізації відбувається інтенсивне використання ЗМІ для ведення інформаційних війн. Так, глобальні та регіональні системи інформаційної безпеки наразі не повною мірою здатні ефективно реагувати на низку нових загроз в інформаційній сфері. Такими загрозами зокрема є нарощування інтенсивності використання інформаційних маніпуляцій як інформаційної зброї і окремими державами, і зарубіжними організаціями, подекуди терористичними, проведення інформаційно-психологічних операцій. Відтак, із глобалізацією та тотальною інформатизацією світу тероризму як явищу вдається швидше та ефективніше досягати своїх головних цілей. Фактично терористичні держави, такі як Росія, користуючись перевагами повсюдності інформації, проводять інформаційні атаки як на Україну, та і на інших акторів міжнародних відносин.

2.2 Інформаційні війни як джерело загроз безпеці державі в національному

За умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнення і боротьби різновекторних національних інтересів держав стає інформаційний простір. Сучасні інформаційні технології дають змогу державам реалізувати власні інтереси без застосування воєнної сили, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів.

Розвиток глобального процесу інформатизації суспільства, що спостерігається в останнє десятиліття, породило нову глобальну соціо-технологічну проблему – інформаційної безпеки людини і суспільства.

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на одну з головних арен протиборства. РФ використовує проти України найефективніші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом та порушення суверенітету і територіальної цілісності України.

Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації [19; с.90].

Увага до проблем гарантування інформаційної безпеки України зумовлена антиукраїнськими впливами, які пропагують ідеї сепаратизму, насильства, національної ворожнечі і є спробою руйнування національної ідентичності українців, знищення міжнаціональної злагоди, посягання на конституційний лад України, територіальну цілісність держави.

Кожна інформаційна агресія в комунікаційно-контентному просторі глобального світу передбачає три вектори:

- вектор атаки – дії, спрямовані на знищення або нав'язування власного трактування фактів чи міфів, які становлять світоглядні підвалини супротивника;
- вектор оборони – дії, спрямовані на захист власних ідеологічно-ментальних підвалин від атак супротивника;
- внутрішній вектор – це дії, спрямовані на побудову і модернізацію власних ідеологічних підвалин [46; с.77].

Якщо розглядати зокрема інформаційне протистоянні між Росією та Україною до повномасштабного вторгнення, то варто зазначити про певні особливості, які, відповідно, зумовлювали характер інформаційної агресії.

Основною особливістю є те, що Росія має потужний *внутрішній вектор імперських традицій*, які визначили існування масивних ідеологічних підвалин так званого *«рускогo міра».* Україна через історичні обставин таких підвалин не могла створити. Утім, наша держава і не намагається розвивати такий напрям. Тобто путінська Росія воює за парадигму «рускогo міра», концентруючи державні, бізнесові та громадські зусилля, а українці протистоять цьому із власним бачення мирної незалежної України.

Відсутність загальної для всієї України ідеології як базового рушія державництва призвела до того, що всю новітню історію наша держава жодного разу не мала суспільного консенсусу з будь-яких суспільно-політичних питань. Відповідно, не був сформований і вектор історичного розвитку. Тому Україні необхідно в період реальної війни сформулювати декілька рівнів стратегій проти політичного режиму Росії і почати справжню інформаційну агресію. Дослідники пропонують кілька тез для формування можливої стратегії цієї кампанії. Розглянемо детальніше вектор атаки України в контексті інформаційної агресії Росії.

Вектор атаки. Об'єктом інформаційної атаки проти Росії має бути комплекс ідей, які звикли називати «рускій мір». Ось основні положення російської концепції:

- Росія є наддержавою, яка за власним статусом є рівною США і більшою за всі інші країни, тому має право впливу на половину всього світу.
- Росія перемогла у Великій Вітчизняній війни, саме росіяни були основною силою перемоги.
- Росія – найбільша слов'янська країна світу, що дає їй надзвичайне/виняткове право на вплив інших слов'янських країнах будь-де.
- Росія є найбільшою православною країною світу, що дає їй право на духовне верховенство серед інших православних країн.
- Росія – славетна древня імперія, тому має право впливати на держави, що входили колись до її складу, і де живуть громадяни, які самоідентифікуються як «рускіє» [46; с.78].

Пропонується таке трактування ідей «руского міра» Україною в контексті інформаційних ініціатив для публічного домінування:

- Так, Росія була наддержавою до 2014 року, але після захоплення Криму втратила цей статус. Наддержавою вважається така країна, яка сама, без союзників, здатна вести успішну війну з будь-якою країною світу. Війна із Україною позбавила Росію такої можливості. Наразі Росія не в змозі протидіяти ані США, ані Китаю.
- Так, Радянський Союз переміг у Великій Вітчизняній війні, яка була частиною Другої світової війни. Але перемогли всі республіки разом, а не одна Росія, яка ніколи не змогла б цього зробити самотужки. У цій війні Росія справді є рекордсменом, але рекордсменом за кількістю зрадників-колаборантів. Так, за офіційними російськими даними на боці нацистів воювали 600 тисяч росіян, а за оцінкою фахівців до 1,5 мільйона.
- Найбільшою слов'янською державою можна вважати колишній Радянський Союз, але після його розпаду такою державою стала Україна. Якщо спиратись на офіційні російські дослідження, то слов'янська складова в

сучасній Росії становить не більше ЗО мільйонів осіб. Більшість тих, хто в Росії вважає себе слов'янами, за даними Російської академії наук, генетично є фінотатарами.

- Так, Радянський Союз міг вважатися найбільшою християнською православною державою, але після його розпаду такою державою стала Україна. В Росії налічується близько 15 500 парафій російської православної церкви, а в Україні сумарно – до 22 000 парафій церков візантійського обряду, а це навіть більше, ніж у російській православній церкві разом із білоруським екзархатом.

Так, Росія свого часу була імперією де-факто, але ніколи не могла бути імперією легітимною, оскільки імператора мав висвячувати на царство або Папа Римський, або Вселенський патріарх. Тобто Росія є країною із привласненою чужою історією і дуже сумнівною владою щодо легітимності [46; с.78].

Проблема забезпечення інформаційної безпеки України актуалізувалася ще більше в умовах широкомасштабного вторгнення Росії в Україну. Відтак, інформаційна експансія, упереджене та тенденційне висвітлення фактів та явищ з боку Росії про Україну, які тривали десятиліттями і більш інтенсивно від початку війни на Сході України, в умовах повномасштабного вторгнення перейшли у щоденний потік інформаційно-психологічних операцій (ІПсО), дезінформування та пропаганди. Російські пропагандистські інформаційно-психологічні кампанії, акції та загалом інформаційна війна проти України спрямовані на домінування і просування російських наративів як в українському, так і в глобальному інформаційному просторі.

Інформаційна війна є всеосяжною цілісною стратегією, війною за знання, які дають можливість керувати масами. Інформаційні війни сьогодні на рівні зі збройними конфліктами становлять велику небезпеку нормальному функціонуванню системи органів державного управління.

Наприкінці 1996 року експерт Пентагону Роберт Банкер представив доповідь, присвячену новій військовій доктрині Збройних сил США XXI

століття (Концепція XXI). У її основі лежало розділення всього театру військових дій на дві складових – традиційний простір і кіберпростір. І саме кіберпростору надавали більшого значення. Таким чином простір ведення бойових дій розширився – до землі, моря, повітря та космосу почали зараховувати й інфосферу.

У жовтні 1998 року міністр оборони США вводить в дію «Об'єднану доктрину інформаційних операцій», де було розтлумачено співвідношення понять інформаційних війн та інформаційних операцій.

За цією Доктриною *інформаційною операцією* є комплекс дії, що проводять з метою перешкоджання збору, обробки, передачі і зберігання інформації інформаційними системами противника під час захисту власної інформації та інформаційних систем.

Натомість *інформаційна війна* – це сукупність інформаційних операцій, всебічний валив на систему державного і військового управління противника, на її військово-політичне керівництво. Метою інформаційної війни за мирного часу є ухвалення противником сприятливих рішень для сторони-ініціатора, тоді як в умовах збройного конфлікту завдання ІВ повністю паралізувати функціонування інфраструктури управління противника. [19; с.93].

У науковій літературі також часто використовують термін *інформаційне протиборство*, що характеризуєтесь боротьбою сторін в інформаційному просторі з використанням політичних, економічних, дипломатичних, військових та інших методів , способів та засобів для впливу на інформаційне поле в інтересах досягнення поставлених цілей.

Основне завдання ІВ – здійснення безпосереднього негативного руйнівного впливу на сукупну політичну могутність держави через послаблення її реальних та потенційних можливостей щодо забезпечення власної безпеки; створення труднощів у внутрішньому розвитку й проведення активної зовнішньої діяльності, а також підтриманні міжнародних зав'язків. [19; с.95].

Основними об'єктами деструктивного впливу ІВ є:

- ідеологічно-психологічне середовище суспільства, пов'язане з використання інформації, інформаційних ресурсів та інформаційної інфраструктури для здійснення впливу на психіку й поведінку людей;
- інформаційні ресурси, які розкривають духовні, культурні, історичні національні цінності, традиції, надбання держави, нації в різних сферах життя суспільства;
- інформаційна інфраструктура – всі проміжні ланки між інформацією та людиною;
- система формування суспільної свідомості (світогляд, політичні погляди, загальноприйняті правила поведінки тощо);
- система формування громадської думки;
- система розробки та прийняття політичних рішень;
- свідомість і поведінка людини [19; с.96].

На сьогодні вже напрацьована велика кількість технологій здійснення негативного впливу на духовно-ідеологічну сферу життя суспільства. Їх можуть застосовувати спецслужби іноземних держав, терористичні організації, політизовані радикальні угрупування, кримінальні структури, транснаціональні корпорації та інші формальні й неформальні учасники сучасно міжнародно-правових відносин.

В умовах активного розвитку міжнародних відкритих мереж типу Інтернет і приєднанні до них більшості країн кардинально змінюється ідеологія ведення війни і розвідки, де основний акцент тепер роблять на використанні новітніх інформаційних технологій. Окрім цього, *характер деструктивних впливів на інформаційний простір*, тобто на процеси отримання, обробки та поширення інформацій, *визначає три форми ІВ*:

по-перше, вплив на форму повідомлень, механізми їх передачі, зберігання, обробку даних тощо;

по-друге, блокування передачі повідомлень;

по-третє, вплив на зміст повідомлень через проведення СІО та АІВ. [19; с.97]

Інститут національно-стратегічних досліджень США виділяє *сім складових ІВ:*

- стратегія й тактика нейтралізації органів управління противника;
- розвідувальна війна;
- електронна війна;
- психологічна війна;
- комп'ютерна війна (кібервійна);
- ІВ у економічній сфер;
- інформаційний тероризм [19; с.98].

Якщо розглянути для аналізу інформаційну війну, яку проводить країна-агресор Російська Федерація проти України, то ми зможемо простежити усі її складові.

Інформаційна війна Росії проти України довгі роки була самостійною агресивною кампанією проти нашої держави. Та вже зараз, після того як агресор наважився на повномасштабне вторгнення, можна переконливо стверджувати, що завдання і мета цієї ІВ мали б полегшити для Росії повну окупацію Україна та повернення її під тотальний контроль зразка часів СРСР.

Стратегія й тактика нейтралізації органів управління противника. Протягом десятиліть Росія успішно вбудовувала в українську політичну систему своїх агентів. Так звана 5-та колона в українському політикумі, яку представляли в різні періоди різні політичні партії, протягом останніх років перед повномасштабним вторгненням не приховувала своїх намірів і відверто щодня транслювала проросійські наративи. Таким чином, в усіх гілках влади були люди, які працювали на користь Росії, і їхньою кінцевою метою було повне домінування Росії над Україно. Після початку повномасштабного вторгнення російське керівництво відверто заявило про намір ліквідації політичного керівництва України та повалення «режиму», який нібито панує в Україні. Агресор сподівався, що його інкорпоровані агенти швидко займуть місце усунутої влади, утім прогнози виявилися помилковими.

Розвідувальна війна. Розвідка Росії активно працювала по всьому світу ще від розпаду СРСР. Фактично, мережа радянської розвідки нікуди не зникла, а тільки змінила назву. Небезпека розвідувальної війни в тому, що вона є прихованою, непублічною. Ніколи наперед неможливо спрогнозувати до яких саме наслідків може призвести витік секретної інформації. Від початку широкомасштабної війни Росії проти України розвідка агресора активізувалася не тільки в Україні, а й по всій Європі. Так, наприклад, Голландська розвідувальна служба викрила російського військового агента, який намагався проникнути у Міжнародний кримінальний суд, який розслідує звинувачення у воєнних злочинах в Україні. Шпигун намагався отримати дозвіл на проходження стажування у Гаазькому трибуналі.

Електронна війна. У своєму звіті американська неурядова організація C4ADS заявила, що Росія активно використовує технології дезорієнтації системи супутникової навігації GPS в окупованому Криму та в Чорному морі. Технології з дезорієнтації системи супутникової навігації GPS/GNSS були використані загалом близько 10 тис. разів російським устаткуванням електронної війни від лютого 2016-го до квітня 2019 року [3].

Психологічна війна. Під поняттям «психологічна війна» слід розуміти передусім підрив бойового духу та мотивації до спротиву противника. Інструменти цього типу протиборства зараз активно використовує українська розвідка та контррозвідка, суттєво послаблюючи моральний дух ворожої армії. Головний наратив, які українські розвідслужби доносять до російських солдат полягає у тому, що їхня країна не переймається життям свої військових після того, як відправила їх на фронт. Вони для керівництва – прийнятні втрати.

Комп'ютерна війна (кібервійна). Більше ніж за місяць до повномасштабного вторгнення в Україну, Росія почала низку кібератак на Україну. Вже згодом ці дії експерти класифікували як першу у світі кібервійну. Кібератаки почалися в ніч з 13 на 14 січня 2022 року, під час якої хакери вивели з ладу понад 70 урядових сайтів; 17 січня 2022 року хакери атакували форум Prozorro Infobox; 15 лютого 2022 року відбулась наймасштабніша DDoS-атака

на державні та банківські сайти України; 23 лютого 2022 року , напередодні вторгнення російських військ, було ушкоджено сайти Верховної Ради, Кабінету Міністрів України та Міністерства закордонних справ; 24 лютого 2022 року був атакований сайт Київської ОДА, а деякі ресурси були відключенні для збереження даних.

Інформаційна війна в економічній сфер. Яскравим прикладом такої боротьби є рішення РНБО України 2017 року *«Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». Рішення* забороняє інтернет-провайдерам надавати послуги з доступу користувачам мережі інтернет до низки російських інформаційних ресурсів та порталів. На думку аналітиків, російські інтернет-сервіси, які перебували в російському тилу, після виходу на український ринок суттєво демпінгували ціни, зокрема на надання рекламних послуг, що призвело до занепаду українських компаній-конкурентів у цій сфері [34].

Інформаційний тероризм. Яскравим прикладом інформаційного тероризму Росії проти України в контексті широкомасштабного вторгнення можна вважати інформаційний супровід російських пропагандистських і псевдо ліберальних ЗМІ ракетних ударів Росії по українській критичній інфраструктурі, які відбулися 10, 17 та 31 жовтня 2022 року. Протягом місяця, від моменту коли були завдані перші масштабні руйнування, фактично всі російські ЗМІ «розкручували» тезу про критичний переломний момент, цитуючи виступ президента РФ: *«Путін попередив Україну про нові удари, якщо Київ не припинить теракти: головне з виступу 10 жовтня 2022»* [2].

Однією із загроз національній безпеці України є зовнішня інформаційна експансія, яка призводить до таких наслідків, як втрата національної ідеї, духовних цінностей, порушення суспільного строю, зміни політичного устрою, розвалу економіки, держави, армії тощо. Інформаційна експансія здійснюється у формі СІО та АІВ.

СІО – це сплановані дії, направлені на ворожу, дружню або нейтральну аудиторію з метою схилення до ухвалення управлінських рішень або (та)

вчинення дій, вигідних для суб'єкта інформаційного впливу. СІО здійснюються в кілька етапів і можуть бути довгостроковими (більше місяця), середньостроковими (два-чотири тижні) й короткостроковими (один-два тижні). Натомість акції інформаційного впливу тривають один-три дні. Варто зауважити, що СІО складаються з поєднаних між собою часом, метою, завданнями, силами й засобами проведення акцій інформаційного впливу. [19; с.99].

Перед здійсненням СІО можуть провести низку акцій інформаційного впливу для «розігріву» цільової аудиторії, крім випадків, коли потрібен фактор несподіванки. Середня тривалість СІО складає від двох тижнів до місяця, оскільки цього часу зазвичай достатньо для ефективної обробки цільової аудиторії. Водночас тривале поширення негативної інформації притупляє її сприйняття людською психікою, що, своєю чергою, призводить до зниження ефективності СІО.

Підготовка СІО передбачає планування операції, визначення форми та способів її здійснення, цілей, завдань, сил і засобів, прийомів та методів впливу, цільової аудиторії. Така інформаційна операція зазвичай здійснюється за однаковим алгоритмом у чотири етапи:

1-ий етап – інформування: створення інформаційного приводу – використання реальної або вигаданої події;

2-ий етап – «розкручування» інформаційного приводу – поступове зростання напруження, наприклад, кількості повідомлень і їх сенсаційності, тенденційності, емоційності, та переважно недостовірності.

3-ій етап – загострення напруження є основною частиною СІО, що полягає у використанні інформаційного приводу для досягнення цілей операцій.

4-ий етап – вихід з операції або етап закріплення – забезпечення плавного завершення СІО після досягнення поставленої мети. Якщо мети не досягнуто зазвичай готується нова інформаційна операція [19; с.99].

Виділяють такі ознаки проведення спеціальних інформаційних операцій:

– збільшення кількості повідомлень негативного змісту з певної соціально-політичної або економічної тематики;

– зростання емоційності повідомлень;

– зростання тенденційності повідомлень;

– збільшення сенсаційності повідомлень;

– лавиноподібність інформаційного потоку;

– скоординованість дій суб'єктів проведення СІО;

– час проведення від одного тижня до двох місяців.

Цілі, які повинні досягнути СІО та АІВ, поділяють відповідно до умов та часу проведення кампаній:

у мирний час: домінування в інформаційному просторі, вплив на соціально-політичну ситуацію в регіоні, формування власного позитивного іміджу;

у воєнний час: інформаційно-психологічний вплив і забезпечення діяльності вищого військово-політичного керівництва;

у післявоєнний час: забезпечення процесу формування лояльної влади, сприяння соціально-економічному розвитку в регіоні, впровадження програм гуманітарної допомоги [19 ;100].

Замовниками СІО та АІВ зазвичай є керівництво іноземних держав. Утім організаторами можуть бути і транснаціональні компанії, і приватні особи з міжнародним рівнем авторитету й капіталу. Такі інформаційні кампанії спрямовані на ідеологічний, ідейно-політичний і соціальний вплив на особу, групу осіб чи суспільство загалом з метою їх переорієнтації на інші цінності й ідеали. Також можуть використовуватися для спонукання до вчинення протиправних дій із підриву державного й суспільно-політичного устрою.

Залежно від спрямованості, СІО та АІВ поділяють на такі види:

- проти суб'єктів, які ухвалюють рішення;
- компрометуючі та такі, що завдають шкоди опонентам;
- дестабілізуючі політичну (економічну) ситуацію.

Основними методами проведення СІО є:

- дезінформування;
- пропаганда;
- диверсифікація громадської думки;
- психологічний тиск;
- поширення чуток [19; с.101].

Зважаючи на реальну загрозу, які ці методи сьогодні становлять для безпеки нашої держави в умовах широкомасштабної війни, що було зазначено і в Стратегії інформаційної безпеки України, розглянемо їх детальніше, щоб зрозуміти механізм їх створення та впливу на свідомість громадян.

Дезінформування – метод, який передбачає обман чи введення об'єкта впливу в оману щодо реальних намірів задля спонукання його до потрібних дій. Найчастіше у світовій практиці застосовуються *5 основних форм дезіфнормування:*

1. *Тенденційне викладення фактів* – полягає в упередженому висвітленні фактів чи іншої інформації щодо подій за допомогою спеціально підібраних правдивих даних. Об'єкту впливу доводять дозовано із постійним зростанням напруження спеціально сформовану інформацію. [19; с.101].

Наприклад, Росія створила подібну дезінформацію про те, що, Україна, так само як і Туреччина, отримавши статус кандидата на вступ до ЄС, ніколи не стане повноправним членом Євросоюзу. Це чи не єдиний тип дезінформації з РФ, що успішно «заходить» в Україні. Тобто чітко сформований наратив Росії, що в Україні «все погано», і вона не має шансів на успіх– перемогу, відновлення, членство в ЄС тощо.

Головний аргумент, яким підживлюють цю зневіру – приклад Туреччини, який переносять на Україну. *Мовляв, нас ніхто не чекає у ЄС, а статус кандидата нічого не означає – подивіться, на Туреччину, яка вже понад 20 років кандидат, тож на Україну очікує та сама історія*. Так, за основу береться реальний факт, у ньому випускають з уваги або деформують ключові елементи, а те, що вийшло у підсумку, «натягують» на українську історію й

роблять з цього висновки, які геть не пов’язані з реальністю, але резонують з тривогами людей.

Насправді ж Туреччина має статус кандидата ще з 1999 року, тобто вже більше 20 років, і справді лишається так само далекою від членства. Але тут головне врахувати те, наскільки відмінним є турецький рух цією процедурою від українського та й від усіх інших держав, що прагнуть вступити до ЄС або вже стали членами. Зрештою, 16 чинних держав-членів ЄС подали заявку на членство пізніше за Туреччину, але вже давно вступили до Євросоюзу [20].

2. Дезінформування «від зворотного» – відбувається через подання правдивих відомостей у спотвореному вигляді чи в такій ситуації, коли вони сприймаються об’єктом впливу як неправдиві. Внаслідок застосування подібних заходів виникає ситуація, коли об’єкт фактично знає правдиву інформацію про наміри чи конкретні дії протилежної сторони, але сприймає її неадекватно та не готовий протистояти негативному впливу. [19; с.102].

Досить часто в зоні бойових дій для обміну інформацією військові використовують незахищений зв’язок, який легко перехвалюється противником. Дезінформування «від зворотного» полягає в тому, що військові спеціально надають противнику інформацію про події, які суперечать одна одній, або події, що фактично неможливі. Внаслідок цього, навіть під час перехоплення правдивих повідомлень, противник не сприймає достовірну інформацію як правдиву.

Наприклад, один із наших бійців пригадував, як українським військовим вдавалося утримувати оборону Маріуполя протягом довгого часу фактично в повному оточенні. Оскільки не було можливості постійно прошивати рації, ворог міг легко прослуховувати зв’язок українських солдат. Так, саме через переговори по радіозв’язку наші захисники вводили противника в оману, після чого він обстрілював дислокацію своїх же підрозділів. Вдалося провести кілька успішних операцій до того, як ворог зрозумів обман. І вже не використовував інформацію, отриману з перехоплень переговорів, як оперативну.

3. Термінологічне «мінування» – полягає у викривленні первинної правильної суті принципово важливих, базових термінів і тлумачень загально-світоглядного та оперативно-прикладного характеру. [19; с.102].

Яскравим прикладом такого дезінформування є підміна термінів «нацизм», «денацифікація», які зараз активно використовує російська пропагандистська машина проти України. Насправді ж нацизмом вони називають патріотизм українців та бажання жити самостійно, без російського впливу. Натомість нав'язування виключно російського наративу в Україні та знищення всього українського вони назвали денацифікацією.

4. «Сіре» дезінформування – передбачає використання синтезу правдивої інформації з дезінформацією. Також дуже часто простежується у інформаційних потоках Росії проти України.

5. «Чорне» дезінформування – використання та поширення переважно неправдивої інформації. [19; с.103]. На зовнішню аудиторію, зокрема українську, з боку Росії застосовується порівняно менше, оскільки є абсолютно недієвим. Натомість є головною формою пропаганди для внутрішнього споживача – громадянина РФ. Саме через механізми «чорного» дезінформування широким масам у Росії, які до того ж мають слабке критичне мислення, нав'язали страшні сценарії про те, що в Україні більшість населення є фашистами і прославляють нацистський режим. Цей наратив Росія почала активно розкручувати із 2015 року, щоб виправдати свої дії в Криму та на Донбасі.

Пропаганда – поширення політичних, філософських, наукових, художніх та інших ідей з метою їх упровадження у громадську думку та активізації використання цих ідей у масовій практичній діяльності населення. Пропагандою є також повідомлення, які поширюються для здійснення вигідного впливу на громадську думку, провокування запрограмованих емоцій та зміни ставлення чи поводження певної групи людей у напрямі, безпосередньо чи опосередковано вигідному організаторам [19; с.104].

Ідеолог та найвідоміший пропагандист фашизму *Й. Геббельс визначив такі головні принципи пропаганди:*

по-перше, пропаганда має бути спланованою та проводитися з однієї інстанції;

по-друге, тільки авторитет може визначити, має бути результат пропаганди істинним чи фальшивим;

по-третє, «чорна» пропаганда використовується тоді, коли «біла» неможлива, або ж не має належного ефекту;

по-четверте, пропаганда має характеризувати події чи людей маркерними фразами чи гаслами;

по-п'яте, для кращого сприйняття пропаганда повинна викликати інтерес в аудиторії й передаватися через привабливе середовище комунікацій [19; с.105].

Виділяють 3 основні форми проведення пропаганди:

- пропаганда способу життя;
- формулювання та створення нових ідей;
- коректування сформованих думок.

Залежно від мети, яку ставить перед собою пропагандист, *пропаганда поділяється на позитивну й негативну.*

Мета позитивної пропаганди – сприяти соціальній гармонії, злагоді, вихованню людей в системі загальноприйнятих цінностей. Позитивна пропаганда виконує виховну та інформаційну функції в суспільстві. Вона здійснюється на користь тих, кому адресована, а не обмеженого кола зацікавлених осіб; не допускає обману та приховування фактів. У цьому її відмінність від негативної. Позитивна пропаганда не містить маніпулятивної мети, тому використовується не для проведення СІО та АІВ, а для захисту населення від них.

Завдання негативної пропаганди – розпалювання соціальної ворожнечі, ескалація соціальних конфліктів, загострення суперечливих поглядів у суспільстві. Це призводить до роз'єднання людей, робить їх більш слабкими та піддатливими до волі пропагандиста. Основна функція негативної пропаганди –

створення ілюзорної паралельної реальності з хибною системою цінностей, переконань та поглядів. Під час цього активно використовується навіювання на широкі маси з метою маніпуляції на користь обмеженої групи осіб [19; с.104].

Диверсифікація громадської думки **–** розпорошення уваги серед різних груп суспільства, часто серед політичної еліти, на різні штучно акцентовані проблеми й відволікання уваги від вирішення нагальних завдань суспільно-політичного та економічного розвитку для нормального функціонування соціуму й країни [19; с.106].

Виділяють такі форми диверсифікації громадської думки:

- дестабілізація ситуації в державі чи окремих її регіонах;
- активізація кампаній проти політичного курсу владної еліти та окремих її лідерів різними міжнародними установами;
- ініціювання антидемпінгових кампаній, скандальних судових процесів, застосування міжнародних санкцій з інших причин [19; с.106].

Метод диверсифікації громадської думки активно застосовувався інкорпорованими до українського політикуму російськими агентами. Вони «розкручували» теми розділення України на Східну та Західну, загострювали вирішення питання законодавчого регулювання державної мови та мови нацменшин, що подекуди ставило під сумнів державну політику.

Психологічний тиск **–** вплив на психіку людини через залякування, погрози з метою реалізації запланованої моделі поведінки. Такими *формами психологічного тиску є:*

- донесення до об’єкта впливу відомостей про реальні чи вигадані загрози та небезпеки;
- прогнози щодо репресій, переслідувань, убивств тощо;
- шантаж;
- здійснення вибухів, підпалів, масових отруєнь, захоплень заручників, інших терористичних акцій;
- «телефонний тероризм» ;
- використання забороненої технології 25-го кадру [19; с.105].

Один із останніх яскравих прикладів психологічного тиску – це погрози у листах, які отримали низка дипломатичних установ, пов'язаних з Україною. Так, із 24 листопада по 2 грудня 2022 року пакунки з вибухівкою отримали прем'єр-міністр Іспанії Педро Санчес, посольство України в Мадриді, урядові установи, супутникова компанія, зброя якої була направлена в Україну, та американське дипломатичне представництво. Після цього українські посольства у 12-ти країнах, зокрема й Іспанії, отримали листи з погрозами, що Міністерство закордонних справ назвало «добре спланованою кампанією терору» [31].

Поширення чуток **–** поширення інформації, переважно неправдивої, серед широких верств населення здебільшого неофіційними каналами з метою дезорганізації суспільства та держави або їхніх установ чи органів.

Чутки класифікують за трьома параметрами: експресивність, інформативність, та ступінь впливу на психіку людини [19; с.107].

Особливість використання чуток у інформаційних операціях полягає в тому, що практично немає ефективних засобів протидії цій формі. Чутки не можна зупинити на офіційному рівні, адже це викликає зворотній ефект. До того ж, за рахунок розголосу досягається головна мета – поширення чутки на всіх рівнях, і навіть найвищому. Єдиний можливий спосіб боротьби із чуткам – це цілковите їх ігнорування. Оскільки через певний час напруга спадає і зайва активність в обговоренні уже неактуальних новин згасає.

Наприклад, на початку широкомасштабного вторгнення російські пропагандисти розповідали про те, що Український Президент виїхав з країни. Спроби поширити цю чутку систематично повторюють, але українське суспільство вже абсолютно не сприймало подібну таку інформацію. До того ж Офіс Президента і сам Володимир Зеленський завжди спростовував цю інформацію [30].

Вже у листопаді 2022 року російська пропаганда намагалася перевести фокус уваги з проблем «спеціальної військової операції» на виправдання невдач окупантів на фронті в Україні. Аналітики Центру протидії дезінформації при

РНБО виокремили 4 основні напрями, на які поширювалася пропаганда агресора.

Перший напрям: спроба розсварити Україну із сусідами-партнерами традиційно посідає важливе місце в наративах російської пропаганди. Ситуація 15 листопада, коли під час масштабних ракетних атак росії в польському прикордонному селі Пшеводув загинули дві людини, стала «подарунком» для російської пропаганди. Хоча розслідування того, чи була це російська ракета, чи це був результат роботи української системи ППО, досі триває, російська пропаганда акцентувала увагу на начебто умисному обстрілі українськими ЗС польської території [49].

Проте чергова спроба посварити дружні народи виявилася невдалою. Польська влада, опозиція та суспільство визнали, що навіть якщо буде доведено, що це українська ракета ППО влучила в польське селище, відповідальність за трагедію несе Росія як терористична держава-агресор, яка напала на Україну.

Другий напрям: щоб перекласти відповідальність і захиститися від гніву президента РФ, російське командування звинувачує у всіх провалах «спецоперації» російських військових, які здаються в полон українським захисникам. Також протягом листопада Росія активно поширювала в соцмережах відео сумнівного походження про страту «вагнерівця» та відео, на якому військовослужбовці ЗСУ начебто розстрілюють російських військовополонених. За допомогою подібних «доказів» пропаганда намагається навіяти російським солдатам, що в полон їм краще не здаватися [49].

Третій напрям: після наймасовішого ракетного удару по українській енергетиці 15 листопада та блекаутів по всій території країни російська пропаганда почала активно створювати у Telegram-каналах картинку невдоволення та стимулювала людей виходити на протести. В Одесі у місцевому проросійському пабліку почали десятками публікувати звернення нібито обурених мешканців, де прослідковувалося нав’язування хибної ідеї, що

Одеса – російське місто, де потрібно перемогти фашизм, а «киевляне» і «львовяне» – абсолютно чужий народ, який не шкода [49].

Російський Telegram-канал, де публікують методички для російських інформаційних атак, поширював фейки про продаж української електроенергії за кордон та «мультик» із закликом не оплачувати платіжки. Так, пропагандистська активність, спрямована на розгойдування ситуації всередині суспільства, вилилась в перекриття доріг в місті вночі 18 листопада. Поширення інформації про протести призвело до того, що жителі інших регіонів висловлювали узагальнене упереджене ставлення до всіх одеситів, які нібито не можуть зрозуміти, що в Україні триває війна. Згодом «картинки» з протестами використали для російських пропагандистських каналів, створюючи умови для розбрату та протестів.

Четвертий напрям: фабрикування фейкових новин про утиснення вимушених переселенців в Європі, нестачу Західної зброї для ЗСУ, протести в Європі проти її надання Україні та загальну втому Західних лідерів від українських проблем [49].

Отже, спеціальні інформаційні операції становлять комплекс заходів інформаційно-психологічного характеру, що здійснюють за єдиним планом із метою порушення системи державного і військового управління, впливу на морально-психологічний стан військово-політичного керівництві, населення й особового складу військ визначеного об’єкта, запобігання інформаційному та психологічному впливу на власні сили і засоби. Здійснення СІО й захист від них є невід’ємною передумовою забезпечення національної безпеки держави. Такі операції проводяться як за мирного часу, так і у воєнний період. Основні аспекти СІО – психологічний, культурний, інтелектуальний, технологічний та економічний.

Основними методами проведення спеціальних інформаційних операцій є дезінформування та його підвиди, пропаганда, диверсифікація громадської думки, психологічний тиск та поширення чуток. Усі ці методи активно застосовуються під час проведення інформаційних атак на український

інформаційний простір державою-агресором, зокрема і під час широкомасштабного вторгнення Росії.

Висновок до розділу 2

Отже, основним засобом ведення інформаційного протиборства є національні й транснаціональні ЗМІ. Системи інформаційної безпеки, зокрема і національні, наразі не повною мірою здатні ефективно реагувати на низку нових загроз в інформаційній сфері. Такими загрозами зокрема є використання інформаційних маніпуляцій як інформаційної зброї, проведення інформаційно-психологічних операцій. Терористичні держави, зокрема і Росія, користуються перевагами повсюдності інформації, проводячи інформаційні атаки як на Україну, та і на інших акторів міжнародних відносин.

Україна також є об’єктом перманентних інформаційно-психологічних впливів, операцій, війн, відтак її інформаційна безпека перебуває під постійним тиском. Проти України широко використовують сучасні технології негативних інформаційно-психологічних впливів, які становлять загрозу як українському національному інформаційному простору, так і суверенітету держави.

Основними методами проведення спеціальних інформаційних операцій, які Росія активно використовує проти України, є дезінформування та його підвиди, пропаганда, диверсифікація громадської думки, психологічний тиск та поширення чуток. Усі ці методи постійно застосовуються під час проведення інформаційних атак на український інформаційний простір державою-агресором, зокрема і під час широкомасштабного вторгнення Росії.

РОЗДІЛ 3. ПЕРСПЕКТИВИ ТА ВИКЛИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Євроінтеграційний вимір формування та розвитку єдиного інформаційного простору України

Третє тисячоліття відзначається стрімким глобальним розвитком комп'ютерних інформаційних технологій, засобів електронної телекомунікації, масовим упровадженням їх у всі сфери суспільної діяльності. Стрімкі теми розвитку комп'ютеризації та інформатизації суспільства неминуче ведуть до створення єдиного світового інформаційного простору, у якому будуть акумульовані всі засоби збору, накопичення, обробки, обміну і збереження інформації.

Виокремлюють такі *геополітичні особливості сучасного інформаційного простору:*

– відсутність звичних географічних і державних кордонів;

– зниження значимості фактору відстані в політичних процесах та відносинах;

– складність здійснення національної і державної ідентифікації суб'єктів і об'єктів інформаційного простору;

– можливість вирішувати задачі у всьому геополітичному просторі в єдиному масштабі часу;

– - можливість забезпечення воєнно-політичних комунікацій з будь-якими державами і територіями без посередників;

– можливість здійснення анонімного доступу до інформаційних, зокрема конфіденційних ресурсів інших держав [19; с.110].

Інформаційний простір – це територія поширення інформації за допомогою конкретних компонентів системи інформації та зв'язку, діяльність якої має гарантоване правове забезпечення. Спеціальними вимірами інформаційного простору можуть стати: загальна кількість засобів масової комунікації, загальний обсяг її продукції, що поширюється і приймається на

певній території; опосередкована фіксація тих або інших результатів контакту з продукцією засобів масової комунікації реципієнтів [37; с.135].

Для України важливо співпрацювати та інтегрувати свій інформаційний простір до європейського особливо зараз, під час повномасштабної війни. Це дасть можливість сформувати єдиний інформаційний фронт проти агресора як серед європейської спільноти, так і на широкій міжнародній арені. Також державі доведеться через зміни у законодавстві ухвалити низку умов та адаптувати процеси до формату ЄС.

Європейський інформаційний простір має стійку основу для функціонування й розвитку. На сучасному етапі поточний стан інформаційного простору України відрізняється від європейського, тому потребує законодавчого регулювання. Стратегія розвитку інформаційного суспільства України була схвалена 15 травня 2013 року і розрахована на період до 2020 року. Очевидно, що інформаційна сфера розвивається дуже стрімкими темпами, а отже держава потребує впровадження вже нової стратегії розвитку.

До того ж, протягом останнього десятиліття національне інформаційне законодавство суттєво змінилося, були запушені процеси інформатизації й діджиталізації в усіх сферах. Натомість законодавче забезпечення процесів помітно відстає в цій сфері, а тому не відповідає вимогам європейських конвенцій. Відтак, задля інтеграції в європейський інформаційний простір важливо успішно пройти адаптацію та гармонізацію українського законодавства в інформаційній сфері з відповідними нормативно-правовими актами ЄС.

Наприклад, європейське законодавство ставить високі вимоги до достовірності інформації й протидії дезінформації. У квітні 2018 року *Єврокомісія представила європейський підхід до боротьби з дезінформацією в мережі Інтернет*, що декларує такі цілі:

– підвищити можливість відслідковувати походження інформації та спосіб її створення, рекламування й розповсюдження;

– сприяти різноманітності інформації, щоб громадяни могли ухвалювати обґрунтовані рішення на основі критичного мислення;

– підвищувати довіру до інформації, акцентуючи увагу на її походженні з перевірених джерел;

– оновити підхід до ухвалення довгострокових рішень, які потребують підвищення поінформованості, медіаграмотності, широкого залучення зацікавлених сторін та співпраці органів державної влади, онлайн-платформ, рекламодавців, журналістів і медіагруп [1].

Підтвердженням того, що ЄС досить серйозно ставиться до регулювання відносин у своєму інформаційному просторі, є вимога, яку поставили перед Україною в межах виконання 7-ми пунктів задля збереження статусу кандидата на вступ до ЄС, отриманого 23 червня 2022 року.

Цей пункт передбачає «*..подолати вплив корисливих інтересів через узгодження закону про ЗМІ з Директивою ЄС про аудіовізуальні медіапослуги та передавши повноваження незалежному регулятору ЗМІ»* [5].

Україна мала зобов’язання гармонізувати медійне законодавство відповідно до стандартів Ради Європи як країна-член організації та імплементувати Директиву ЄС про аудіовізуальні медіапослуги згідно з Угодою про асоціацію. Очевидно, якщо така вимога досі існує перед Україно, і про яку ще раз нагадали в переліку вимог щодо збереження статусу кандидата, то українське законодавство досі не імплементувало усі необхідні вимоги Директиви.

Положення Директиви передбачають:

- обмеження поширення шкідливого контенту, зокрема щодо дітей;
- поступове підвищення доступності медіасервісів для осіб із інвалідністю за допомогою пропорційних заходів;
- регулювання платформ спільного доступу до відео;
- гарантування доступу суспільства до трансляції подій значного суспільного інтересу;
- вимоги до поширення комерційних повідомлень;

- гарантування права на відповідь у разі поширення про особу недостовірних фактів;
- посилення незалежності та автономності регуляторного органу у сфері аудіовізуальних медіа;
- зобов'язання держави просувати та вживати заходів із розвитку навичок медіаграмотності;
- заохочення співрегулювання та сприяння саморегулюванню через кодекси поведінки [5].

Для успішної інтеграції вирішальне значення має політика міжнародної співпраці України та її участь у розвитку глобального інформаційного суспільства. Така співпраця має здійснюватися з метою узгодження стратегій розвитку та сприяння в реалізації універсального підходу до спільних дій, зменшення цифрової та інформаційної нерівності.

Для вирішення зазначених завдань необхідно:

- розширити співпрацю з провідними міжнародним організаціями з розвитку інформаційного суспільства в межах міжнародних договорів України щодо науково-технічного співробітництва та міжнародної технічної допомоги;
- забезпечити інтеграцію освіти, науки, і культури України в глобальний культурний, освітній, науково-технічний інформаційний простір;
- реалізувати в межах міжнародних договорів України спільні проекти, які забезпечують інтеграцію України в глобальний інформаційний простір;
- сприяти розвитку партнерських відносин між державним і приватним секторами економіки в контексті розбудови інформаційного суспільства відповідно до Декларації тисячоліття ООН. [19; с. 60].

Окремо варто зауважити про регулювання відносин в українському інформаційному просторі в умовах воєнного стану, який був введений Указом Президента України 24 лютого 2022 року. Так, Національна рада України з питань телебачення і радіомовлення у серпні 2022 року отримала повноваження для регулювання інформаційного простору в умовах війни.

Механізми контролю і нагляду визначені в новому *Законі України «Про внесення змін до деяких законів України щодо особливостей здійснення окремих повноважень Національною радою України з питань телебачення і радіомовлення в умовах воєнного стану»* від 16 серпня 2022 року. Закон вносить положення, які визначають нові механізми реагування медіарегулятора і є необхідними для забезпечення захисту інформаційної сфери держави. Так передбачено, що рішенням Національної ради буде затверджене положення про особливості процедури ліцензування в період дії воєнного стану.

Окрім цього, Національна рада зможе реагувати на порушення на підставі моніторингу без проведення перевірки. Зокрема, прописана особлива процедура застосування санкцій за виявлені порушення законодавства. Вона передбачає оприлюднення повідомлення про початок розгляду питання щодо можливого порушення, надання ліцензіатом пояснень і ухвалення рішення регулятором.

Санкції за особливою процедурою воєнного часу будуть накладатися за конкретно визначені серйозні (грубі) порушення. Для всіх інших випадків залишиться звичне регулювання мирного часу. Крім того, якщо ліцензіат повторно протягом дії воєнного стану допускає серйозне порушення, Національна рада звертатиметься до військового командування. Такими грубими порушеннями є:

– заклики до насильницької зміни конституційного ладу України;

– пропаганда російського нацистського тоталітарного режиму, збройної агресії російської федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну;

– виправдовування, визнання правомірною, заперечення збройної агресії російської федерації проти України;

– глорифікація осіб, які здійснювали збройну агресію російської федерації проти України тощо [6].

Отже, наразі українське законодавство у секторі сприяння та розвитку спільного інформаційного простору ще не достатньо узгоджене із законодавством ЄС.

Для успішної інтеграції національного інформаційного простору до європейського, Україні доведеться зробити ще низку необхідних кроків. Зокрема, пройти адаптацію та гармонізацію українського законодавства в інформаційній сфері з відповідними нормативно-правовими актами ЄС; подолати вплив корисливих інтересів через узгодження закону про ЗМІ з Директивою ЄС про аудіовізуальні медіапослуги та передавши повноваження незалежному регулятору ЗМІ, чого вимагає ЄС; реалізувати в межах міжнародних договорів спільні проекти, які забезпечують інтеграцію України в глобальний інформаційний простір.

3.2 Публічна дипломатія як складова системи стратегічних комунікацій в умовах російсько-української війни

Широкомасштабна війна Росії проти України спонукає нас до пошуку іноземних союзників та партнерів. Держава-агресор уже протягом багатьох років формувала своє іноземне лобі, використовуючи при цьому переважно заборонені методи, такі як тиск, залякування, підкуп, шантаж через енергоресурси, щоб схилити на свою сторону якомога більше політичних акторів у різних країнах світу.

Сьогодні питання стратегічних комунікацій та публічної дипломатії для України є особливо актуальними, адже в умовах війни кожен чинник може виявитися вирішальним. До того ж, у наслідок російсько-української війни, глобальної пандемії та інших потрясінь міжнародної системи, відбувається суттєва зміна її структури, що супроводжується швидкою еволюцією міжнародних комунікацій. Усі ці процеси потрібно враховувати для того, щоб український вплив на іноземну аудиторію був ефективним та допоміг у досягненні зовнішньополітичних цілей.

Згідно із Доктриною інформаційної безпеки України стратегічні комунікації – це скоординоване і належне використання комунікативних можливостей держави, зокрема публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави [41].

У п. 20 Стратегії національної безпеки України зазначається, що *«деструктивна пропаганда як ззовні, так і всередині України, використовуючи суспільні протиріччя, розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність*» Відсутність цілісної інформаційної політики держави, слабкість системи стратегічних комунікацій ускладнюють нейтралізацію цієї загрози. Відтак поставлено завдання щодо активної та ефективної протидії розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам, російській та іншій підривній пропаганді; створення системи стратегічних комунікацій [43].

Отже, дієвість системи стратегічних комунікацій країни залежить від ефективного застосування інструментарію, до переліку якого входять: публічна дипломатія, зв'язки із громадськістю, військові зв'язки з громадськістю, інформаційні та психологічні операції, операції і заходи з метою просування національних інтересів. Особливий акцент при використанні цього інструментарію має бути на гнучкості та адаптивності до швидких змін ситуації, а також важливості зворотного зв'язку з цільовими аудиторіями [48; с.2].

Публічна дипломатія – одна з найвагоміших складових сучасних стратегічних комунікацій, що передбачає комунікативно-інформаційні дії держави для забезпечення реагування на проблеми у міжнародних відносинах. Метою пунічної дипломатії є просування національних інтересів і зміцнення національної безпеки через порозуміння, інформування та вплив на зарубіжні аудиторії, зокрема і через розширення міждержавних громадських зв'язків.

Сучасними інструментами публічної дипломатії можна вважати проекти в галузі культури, програми обмінів, короткострокові інформаційні кампанії з

метою корекції іміджу країни на міжнародній арені, міжнародне мовлення та моніторинг зарубіжної громадської думки. Тобто, одним із головних завдань публічної дипломатії є вивчення позитивних і негативних суджень про країну, що циркулюють серед зарубіжної аудиторії, та налагодження діалогу як на міждержавному рівні, так і на рівні громадянського суспільства.

Слід зауважити, що саме брак об'єктивної інформації про Україну, її історію та культуру власне і створив проблеми з розуміння та адекватного сприйняття українських подій серед світової спільноти. Натомість українська візія у світі довгі роки подавалася крізь призму тлумачення держави-агресора.

Метою росіян упродовж останніх десятиліть є переконати усіх, що Україна є яскравим прикладом неспроможної держави (failed state), де панує хаос, відбуваються постійні неконтрольовані кризи, розкол серед населення досягнув критичної точки, а демократичний проект повністю провалився. Водночас російська пропаганда зображає західну демократію «гнилою», неефективною та фасадною, а західний істеблішмент – маніпуляторами й агресивними авантюристами, які створили кризу в Україні. Величезні фінансові ресурси, які виділяють на російську інформаційно-пропагандистську діяльність, дозволяють задіяти практично весь відомий арсенал засобів та інструментів для взаємодії з широким переліком цільових аудиторій за кордоном [41;324].

Комунікація із закордонною аудиторією стала особливо актуальною для України після російського вторгнення 2014 року. На жаль, тільки тоді для більшості стало очевидним, що поширення російської пропаганди є передумовою до тотальної ліквідації українського суверенітету і незалежності.

Фактично процес інституалізації публічної дипломатії в Україні почався у грудні 2015 року зі створення Департаменту публічної дипломатії у складі МЗС України. Також почав роботу Український інститут, який запрацював у 2019 році.

Сьогодні ж протистояння російському впливу залишається провідною темою політики України. Цей чинник враховано у *Стратегії публічної дипломатії МЗС України на 2021-2025 роки,* де протидію гібридним загрозам,

дезінформації та фейкам з боку РФ визначено як одну з трьох головних цілей [39;19]. Так само у *Комунікаційній стратегії МЗС України* у переліку стратегічних цілей МЗС перше місце *займає «протидія агресії РФ політико-дипломатичними засобами»*, яка охоплює боротьбу з дезінформацією та маніпулятивною інформацією [23; 11].

Стратегія публічної дипломатії Міністерства закордонних справ України 2021-2025 визначає:

• основні підходи та поняття публічної дипломатії;

• внутрішнє та зовнішнє середовище;

• мету, стратегічні цілі та завдання публічної дипломатії МЗС;

• позиціювання України: бренд Ukraine NOW та ключові повідомлення;

• цільові аудиторії, інструменти та канали публічної дипломатії;

• географічні пріоритети;

• ресурси;

• співпрацю та координацію з іншими державними органами України [48; с.3].

Зазначається, що для успішного виконання Стратегії потрібна ефективна координація та взаємодія Міністерства, закордонних дипломатичних установ України та Українського інституту, а також міжвідомча взаємодія з іншими міністерствами та державними установами й неурядовими організаціями. Стратегічні комунікації держави, частиною яких є публічна дипломатія, не обмежуються лише зусиллями МЗС, а потребують скоординованих дій всіх дотичних державних інституцій.

Своєю чергою, Український інститут у 2020 році презентував та ввів у дію середньострокову стратегію, що визначає місію, візію, стратегічні цілі та фіксує принципи діяльності цієї інституції до 2024 року.

Отже, сьогодні *ключові повноваження у сфері публічної дипломатії мають такі інституції*:

• Міністерство закордонних справ України, яке фактично є координатором ПД (Директорат публічної дипломатії та комунікацій);

• Український інститут – експертна організація, що «має системотворчу роль у міжнародній репрезентації України через потенціал культури та має на меті зміцнення міжнародної та внутрішньої суб'єктності України засобами культурної дипломатії»;
• Міністерство культури та інформаційної політики України;
• Український культурний фонд;
• Міністерство економіки України;
• Міністерство освіти і науки України;
• Міністерство молоді та спорту України [48; с.4].

Компетенцію центральних органів державної влади щодо сприяння позиціонуванню України у світі закріплено у положеннях про діяльність цих органів та у спеціальних стратегіях/концепціях/програмах. Комітет Верховної Ради України з питань зовнішньої політики та міжпарламентського співробітництва затвердив *пріоритети міжпарламентського співробітництва Верховної Ради України* у 2021 році. [32]. Серед низки напрямків, два пріоритети є визначальними для формування публічної дипломатії, це зокрема «*посилення роботи із просування українських наративів на міжнародних майданчиках»* та *«сприяння у створенні позитивного іміджу України за кордоном та розвитку культурної співпраці»*.

Ще до початку повномасштабного вторгнення лютого 2022 року, над спільними проектами просування у світі бренду Ukraine NOW працюють усі міністерства та відомства. З метою розвінчування міфів і стереотипів про Україну, а також донесення української культури та історії до іноземних аудиторій було започатковано проект «Ukraine in 2 Minutes» (Український інститут та ІнтерньюзУкраїна), серію перекладів історій про Україну польською, чеською та французькою мовами (УІ та Ukraïner), перший англомовний онлайн курс про Україну «Україна: історія, культура та ідентичності» (УІ, Києво-Могилянська академія та студія онлайносвіти EdEra) тощо. МЗС разом із ГО «Вікімедіа Україна» започаткувало кампанію наповнення Вікіпедії інформацією про Україну різними мовами з метою

протидії дезінформації і продовжило практику реалізації інформаційних кампаній, наприклад #CrimeaIsUkraine, #StopRussianPropaganda, #Fight4Truth, #NeverAgain, #ExportNow, #ExploreUkraineNOW, #ДипломатіяРівнихМожливостей тощо. Триває промоція українського кінематографа, книги, запуск нових україномовних аудіогідів у музеях світу [48; с.4].

Утім, враховуючи нерівність стартових можливостей України, навіть за підтримки ЄС та США, було достатньо важко стримувати вплив російської пропаганди і маніпуляцій, не кажучи вже про те, щоб схилити шальки терезів у інформаційному протистоянні на свій бік.

Незважаючи на провальні комунікаційні проекти РФ на кшталт просування вакцини проти коронавірусу «Спутнік V», їй все ж вдавалося підривати довіру до своїх супротивників. Упродовж тривалого часу Росія користувалася значною перевагою у доступі до каналів комунікації зі світом.

Крім її власних медіаструктур, використовувались різні організації та групи впливу за кордоном. До того ж, інтерес світу до Росії був значно більшим, аніж до України. Повсюдною була практика, коли російські представництва західних та інших медіакомпаній займалися, зокрема, і українськими питаннями. (наприклад, російський офіс Youtube відповідав і за укранський сегмент). Росія успадкувала увесь радянський пропагандистсько-маніпуляційний апарат і досвід, натомість Україні було важко протиставити щось дієве російській пропагандистській машині.

Ключові історичні події недалекого українського минулого – Помаранчева революція, Революція гідності, анексія Росією Криму та окупація Донбасу – на певний час привертали увагу світу до нашої країни, але не закріплювало розуміння серед міжнародної аудиторіє, якою насправді є сучасна Україна без російського контексту.

Широкомасштабне вторгнення 2022 року суттєво змінило ситуацію на користь України, тому зараз важливо не втратити цей шанс і остаточно сформувати нову українську візію. Звісно, Росія все ще має переваги серед

мережі міжнародних агентів впливу, проте після низки зухвалих та жорстоких міжнародних злочинів, підтримка РФ є токсичною для будь-якого міжнародного гравця.

Натомість Україна здобула безпрецедентні можливості для донесення своєї позиції, утвердження українських наративів та формування привабливого іміджу країни у світі. Однією з головних причин цього можна вважати те, що до цього моменту вже відбулися глобальні кардинальні зміни у складі учасників міжнародної комунікації і публічної дипломатії.

Від початку широкомасштабної війни представники українського громадянського суспільства проводять активну діяльність із донесення української позиції до урядів, бізнесів і людей у всьому світі. Спочатку, коли були сподівання, що росіяни мають бажання зупинити масштабну агресію своєї держави, ця комунікація велася і щодо російської аудиторії. Але згодом вона сфокусувалася передусім на збільшенні підтримки України у інших країнах світу.

Комунікація проводилася незалежно від урядових зусиль у цій сфері і паралельно з ними. Цікавим зразком такої публічної громадської дипломатії є тиск українців на іноземний бізнес для того, щоб він вийшов із РФ. Цей тиск здійснювався як безпосередньо на компанії через висвітлення їхньої співпраці з державою-агресором,– а таким чином міг постраждати їхній репутаційний імідж, – або ж через бойкот їхніх представництв в Україні. Так і за посередництвом і з залученням іноземної громадськості. Отже, тут можна простежити взаємодію з політичною метою за схемами: «українська громадськість – іноземний бізнес» або «українська громадськість – іноземна громадськість – іноземний бізнес». Важливо, що компанії реагували у відповідь, вступали в діалог і частково залишали російський ринок [40; с.326].

Отже, публічна дипломатія – один із основних інструментів стратегічних комунікацій держави, що працює на створення позитивного міжнародного іміджу країни, її впізнаваність, підвищення репутації у світі. Публічна

дипломатія, окрім піднесення бренду країни на світовій арені, створює умови для резистентності громадян до негативних інформаційних впливів.

Враховуючи нерівний потенціал України та Росії до початку широкомасштабного вторгнення у лютому 2022 року, Україні навіть за підтримки ЄС та США було важко стримувати вплив російської пропаганди.

Утім масштабна російська агресія та її міжнародні злочини суттєво змінили ситуацію. Відтак, зміна ставлення до Росії у світі надали Україні безпрецедентні можливості для донесення своєї позиції, утвердження українських наративів та формування привабливого іміджу країни.

Водночас Росія, як і раніше, використовує традиційні комунікаційні канали і методи впливу – односторонню пропаганду, підкуп, залякування. Крім того, агресія та воєнні злочини РФ є вагомими аргументами на підтвердження того, що ця держава є ворогом цінностей миру та гуманізму. У контексті такої візії Україна сьогодні є головним захисником цих цінностей.

В таких умовах вага української публічної дипломатії значно зростає, а основні її завдання зводяться до збереження і збільшення підтримки України у світі, протидії російським інформаційним спецопераціям, а також налагодження контактів із цільовими аудиторіями у віддалених країнах, де позиції Росії залишаються сильними.

Отже, публічна дипломатія є одним із основних інструментів стратегічних комунікацій держави, що працює на створення позитивного міжнародного іміджу країни, її впізнаваності та підвищення репутації у світі. Широкомасштабне вторгнення Росії в Україну 2022 року суттєво змінило ситуацію у сфері публічної дипломатії, відкривши широке вікно можливостей на користь України. Відтак, зараз важливо не втратити цей шанс і остаточно сформувати нову українську візію. Головними гравцями публічної дипломатії України сьогодні є громадянське суспільство, Міністерство закордонних справ України, Український інститут, Міністерство культури та інформаційної політики України, Український культурний фонд та інші.

Висновок до розділу 3

Майбутнє України тісно пов’язане з євроатлантичним виміром. Свої прагнення в цьому напрямку наша держава не раз підтверджувала, ратифікуючи важливі європейські документи та наближаючи норми законодавства до європейських. Саме тому для України важливо продовжити співпрацю та інтеграцію свого інформаційного простору до європейського особливо зараз, в умовах повномасштабної війни. Утім також потрібно зважати на те, що європейський інформаційний простір має стійку законодавчу основу, натомість українське законодавство у секторі сприяння та розвитку спільного інформаційного простору ще не достатньо узгоджене із законодавством ЄС.

Відтак, для успішної інтеграції Україні доведеться зробити ще низку необхідних кроків. Зокрема, подолати вплив корисливих інтересів через узгодження закону про ЗМІ з Директивою ЄС про аудіовізуальні медіапослуги та передавши повноваження незалежному регулятору ЗМІ, чого вимагає ЄС; реалізувати в межах міжнародних договорів спільні проекти, які забезпечують інтеграцію України в глобальний інформаційний простір.

Інструментами для реалізації таких проектів є публічна дипломатія, що працює на створення позитивного міжнародного іміджу країни, її впізнаваності у світі. Широкомасштабне вторгнення Росії в Україну суттєво змінило ситуацію у сфері публічної дипломатії, відкривши нові міжнародні майданчики для обговорення та бачення майбутнього України в демократичній міжнародній спільності. Тому зараз важливо сформувати нову візію для України, зокрема закріпивши за нею статус головного захисника людських цінностей, гуманізму та демократичних свобод.

ВИСНОВКИ

Дослідивши законодавчу базу України та основні нормативні документи, що відповідають за сферу інформаційної безпеки, ми з'ясували, що інформаційна безпека є не тільки самостійною складовою національної безпеки, а й складовою інших сфер національної безпеки держави. Тому прогресивний розвиток України як сучасної правової держави можливий тільки за умови забезпечення інформаційної безпеки всіх суб'єктів інформаційних відносин.

Аналіз нормативно-правової бази дозволив зробити висновок, що основою безпеки України в секторі інформації є низка документів, серед яких головний – Конституція України, а також підзаконні акти, доктрини та стратегій. Під час аналізу ми зосередили увагу на таких Законах України:

«Про національну безпеку України», «Про Раду національної безпеки і оборони України», «Про засади внутрішньої і зовнішньої політики», «Про основні засади забезпечення кібербезпеки України», «Про розвідку» та інші.

Нам вдалося дослідити такі документи як Стратегія національної безпеки України, Воєнна доктрина України, Стратегія інформаційної безпеки, Доктрина інформаційної безпеки, Стратегія публічної дипломатії, Директива ЄС про аудіовізуальні медіапослуги. На підставі аналізу можна зробити висновки, що такі документи є важливими для українських реалі в контексті загальної безпеки держави, але також, зважаючи на існуючі загрози, повинні постійно доповнюватися і вдосконалюватися. Важливо брати за взірець європейську практику, адже саме наближення українського законодавства до законодавства ЄС дозволить швидше пройти усі процеси інтеграції на шляху до вступу у ЄС.

Також ми з'ясували, що Стратегія інформаційної безпеки є важливим рамковим документом, який визначає пріоритетний напрямки в реалізації політики держави щодо інформаційної безпеки. Аналізуючи головні цілі Стратегії, ми визначили, що будь-які законодавчі заходи, спрямовані на протидію дезінформації та обмеження доступу до шкідливого контенту в

Інтернеті, можуть обмежувати і право на свободу вираження поглядів, доступу до інформації, право на журналістську діяльність.

Аналіз інформаційного простору держави, який почасти формує діяльність ЗМІ та ЗМК, дозволив визначити головні загрози для держави в інформаційному секторі в контексті російсько-української війни.

Наше дослідження доводить тезу, що основними засобом ведення інформаційного протиборства є національні й транснаціональні ЗМІ. Оскільки в сучасних умовах глобалізації відбувається інтенсивне використання ЗМІ для ведення інформаційних війн. Натомість і глобальні, і регіональні системи інформаційної безпеки наразі не повною мірою здатні ефективно реагувати на низку нових загроз в інформаційній сфері. Це підтверджує великий масив дезінформаційних кампаній, спеціальних інформаційних операцій та інших видів інформаційного протиборства в міжнародному інформаційному просторі.

Окрім того, відбувається нарощування інтенсивності використання інформаційних маніпуляцій як інформаційної зброї і окремими державами, і зарубіжними організаціями, подекуди терористичними. Тому ми можемо зробити висновок, що фактично терористичні держави, такі як Росія, користуючись перевагами повсюдності інформації, проводять інформаційні атаки як на Україну, та і на інших акторів міжнародних відносин.

Аналіз медіапростору держави підтверджує, що Україна є об’єктом інформаційно-психологічних впливів, операцій, війн, а тому її інформаційна безпека перебуває під постійною загрозою. Проти України широко використовують сучасні технології негативних інформаційно-психологічних впливів, які створюють небезпеку для українського національного інформаційного простору та суверенітету держави.

Детальне дослідження спеціальних інформаційних операцій дозволило систематизувати комплекс заходів інформаційно-психологічного характеру, що здійснюють за єдиним планом із метою порушення системи державного і військового управління, впливу на морально-психологічний стан військово-політичного керівництві, населення й особового складу військ визначеного

об’єкта. Ми чітко визначили, що здійснення спеціальних інформаційних операцій та захист від них є невід’ємною передумовою забезпечення національної безпеки держави. Адже вони проводяться як за мирного часу, так і у воєнний період.

Глибоке дослідження дозволило диференціювати основні методи проведення спеціальних інформаційних операцій і встановити, що такими є: дезінформування та його підвиди, пропаганда, диверсифікація громадської думки, психологічний тиск та поширення чуток. Проаналізувавши український медіапростір, стало чітко зрозуміло, що усі ці методи активно застосовуються державою-агресором під час проведення інформаційних атак на український сегмент, зокрема і під час широкомасштабного вторгнення.

Вибірковий аналіз європейського законодавства у визначеному сегменті дозволив окреслити перспективи та завдання для держави, які необхідно виконати для успішного формування інформаційного суспільства в Україні та інтеграції до європейського інформаційного простору.

Огляд нормативно-правової бази доводить, що українське законодавство у секторі сприяння та розвитку спільного інформаційного простору ще не достатньо узгоджене із законодавством ЄС. Адже для успішної інтеграції національного інформаційного простору до європейського, Україні доведеться зробити ще низку необхідних кроків. Зокрема, пройти адаптацію та гармонізацію українського законодавства в інформаційній сфері з відповідними нормативно-правовими актами ЄС, систематично реалізовувати межах міжнародних договорів спільні проекти, які забезпечують інтеграцію України в європейський інформаційний простір.

Ми з’ясували, що ефективним інструментом для виконання таких завдань є публічна дипломатія, оскільки націлена на створення позитивного міжнародного іміджу країни, її впізнаваності та підвищення репутації у світі.

Дослідження міжнародних тенденцій в контексті російсько-української війни підтверджує, що Україна здобула безпрецедентні можливості для донесення своєї позиції, утвердження українських наративів та формування

привабливого іміджу країни у світі. Однією з головних причин цього можна вважати те, що до цього моменту вже відбулися глобальні кардинальні зміни у складі учасників міжнародної комунікації і публічної дипломатії.

Враховуючи те, що потенціал України та Росії до початку широкомасштабного вторгнення у лютому 2022 року був абсолютно нерівним, нашій державі навіть за підтримки ЄС та США було важко стримувати вплив російської пропаганди.

Утім вже зараз можна констатувати, що масштабна російська агресія та її міжнародні злочини суттєво вплинули на ситуацію. Відтак, зміна ставлення до Росії у світі надали Україні безпрецедентні можливості для донесення своєї позиції, утвердження українських наративів та формування привабливого іміджу країни.

Проаналізувавши основні державотворчі процеси у сфері публічної дипломатії було встановлено, що головними гравцями публічної дипломатії України сьогодні є громадянське суспільство, Міністерство закордонних справ України, Український інститут, Міністерство культури та інформаційної політики України, Український культурний фонд та інші.

Під час проведення дослідження ми з'ясували, що процес інституалізації публічної дипломатії в Україні почався у грудні 2015 року зі створення Департаменту публічної дипломатії у складі МЗС України. Отже можна зробити висновок, що комунікація із закордонною аудиторією стала особливо актуальною для України після російського вторгнення 2014 року. На жаль, тільки тоді для більшості стало очевидним, що поширення російської пропаганди є передумовою до тотальної ліквідації українського суверенітету і незалежності.

Та вже сьогодні протистояння російському впливу є провідною темою політики України. Це підтверджено Стратегією публічної дипломатії МЗС України на 2021-2025 роки, де протидію гібридним загрозам, дезінформації та фейкам з боку РФ визначено як одну з трьох головних цілей [..; 19]. Так само у *Комунікаційній стратегії МЗС України* у переліку стратегічних цілей МЗС

перше місце посідає «протидія агресії РФ політико-дипломатичними засобами».

Підсумовуючи, можна чітко зазначити, що головною перспективою для України у сфері публічної дипломатії є формування нової візії, яка закріпить за нашою державою статус головного захисника людських цінностей, гуманізму та демократичних свобод.

Водночас можна спрогнозувати, що Росія, як і раніше, буде використовує традиційні комунікаційні канали і методи впливу – односторонню пропаганду, підкуп, залякування. Крім того, агресія та воєнні злочини РФ є вагомими аргументами на підтвердження того, що ця держава є ворогом цінностей миру та гуманізму. Відтак, постійна відсіч російських атак для України також є перспективою найближчих років.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Communication – Tackling online disinformation: a European Approach. 2018. 28 apr. URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236 (date of access : 10.10.2022).

2. Баркар Д. Інформаційний тероризм. Як російська пропаганда закликала «вбомбити Україну в кам'яну добу» і заморозити мирних жителів // Інститут масової інформації. 2022. 15 лист. URL: https://imi.org.ua/monitorings/informatsijnyj-teroryzm-yak-rosijska-propaganda-zaklykala-vbombyty-ukrayinu-u-kam-yanu-dobu-i-i49002 (дата звернення: 25.10.2022).

3. Бедратенко О. Російська електронна війна: як Росія дезорієнтує GPS-навігацію в Криму та в Чорному морі, дослідили американські експерти // Голос Америки. 2019. 22 квіт. URL: https://ukrainian.voanews.com/a/navigatsija-rosija-vijna/4886608.html (дата звернення: 10.10.2022).

4. Декларація тисячоліття ООН. URL: https://edera.gitbook.io/world-2030/znayu-prava-i-zminyuyu-svit/chapter2 (дата звернення: 10.10.2022).

5. Директива ЄС про аудіовізуальні медіасервіси. ред. 2022. 29 серп. URL: https://www.nrada.gov.ua/dyrektyva-yes-pro-audiovizualni-mediaposlugy-v-infografitsi/ (дата звернення: 10.09.2022).

6. Закон України «Про внесення змін до деяких законів України щодо особливостей здійснення окремих повноважень Національною радою України з питань телебачення і радіомовлення в умовах воєнного стану». ред. 2022. 16 серп. URL: https://zakon.rada.gov.ua/laws/show/2534-20#Text (дата звернення:05.09.2022).

7. Закон України «Про запобігання корупції». ред. 2022. 22 жовт. URL: https://zakon.rada.gov.ua/laws/show/1700-18#Text (дата звернення: 09.09.2022).

8. Закон України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їх символіки». ред. 2020. 1 січ. URL: https://zakon.rada.gov.ua/laws/show/317-19#Text (дата звернення: 10.09.2022).

9. Закони України «Про державну таємницю». ред. 2022. 15 берез. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 17.09.2022).

10. Закони України «Про засади внутрішньої і зовнішньої політики». ред. 2018. 8 лип. URL: https://zakon.rada.gov.ua/laws/show/2411-17#Text (дата звернення: 17.09.2022).

11. Закони України «Про національну безпеку України». ред. 2022. 15 чер. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 17.09.2022).

12. Закони України «Про оборонні закупівлі». ред. 2022. 10 жовт. URL: https://zakon.rada.gov.ua/laws/show/808-20#Text (дата звернення: 01.11.2022).

13. Закони України «Про основні засади забезпечення кібербезпеки України». ред. 2022. 17 серп. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 17.09.2022).

14. Закони України «Про Раду національної безпеки і оборони України». Ред. 2022. 29 вер. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text (дата звернення: 15.11.2022).

15. Закони України «Про розвідку». ред. 2022. 30 квіт. URL: https://zakon.rada.gov.ua/laws/show/912-20#Text (дата звернення: 17.09.2022).

16. Закони України «Про Службу безпеки України». ред. 2022. 4 груд. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 17.09.2022).

17. Закони України «Про центральні органи виконавчої влади». ред. 2022. 7 трав. URL: https://zakon.rada.gov.ua/laws/show/3166-17#Text (дата звернення: 05.09.2022).

18. Законі України «Про Державне бюро розслідувань». 2022. 7 трав. URL:https://zakon.rada.gov.ua/laws/show/794-19#Text (дата звернення:10.09.2022).

19. Інформаційна безпека: підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. Київ: Ліра-К, 2021. 412 с.

20. Сидоренко С. Кандидат авансом: 7 вимог, які має виконати Україна, щоб ЄС не скасував її новий статус // Українська правда. 2022. 18 черв. URL: https://www.eurointegration.com.ua/articles/2022/06/18/7141516/ (дата звернення: 15.10.2022).

21. Коваль Г., Кобко Є. Інформаційна безпека в системі національної безпеки: адміністративно-правовий аспект // Вісник ХНТУ № 1(80). Херсон, 2022. С. 103-109. URL:https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/10000/1/%d0%9a%d0%be%d0%b2%d0%b0%d0%bb%d1%8c%20%d0%93._%d0%9a%d0%be%d0%b1%d0%ba%d0%be%20%d0%84._%d0%9a%d0%be%d0%b1%d0%ba%d0%be_%d0%92..pdf (дата звернення: 10.09.2022).

22. Кодекс адміністративного судочинства України. ред. 2022. 6 лист. URL: https://zakon.rada.gov.ua/laws/show/2747-15/ed20170803#Text (дата звернення: 09.11.2022).

23. Комунікаційна стратегія МЗС України. URL: https://mfa.gov.ua/storage/app/sites/1/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%97/communication-strategy.pdf (дата звернення: 15.10.2022).

24. Конституція України. ред. 2020. 1 січ. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 04.09.2022).

25. Маляр: Вуха російської ІПСО стирчать з матеріалів, де Україну звинувачують у контрабанді зброї // Детектор Медіа. 2022. 28 лип. URL: https://detector.media/infospace/article/201387/2022-07-28-malyar-vukha-rosiyskoi-ipso-styrchat-z-materialiv-de-ukrainu-zvynuvachuyut-u-kontrabandi-zbroi/ (дата звернення: 10.10.2022).

26. Національна рада отримала повноваження для регулювання інформаційного простору в умовах війни. 2022. 17 серп. URL: https://www.nrada.gov.ua/natsionalna-rada-otrymala-povnovazhennya-dlya-regulyuvannya-informatsijnogo-prostoru-v-umovah-vijny/ (дата звернення: 10.11.2022).

27. Остапенко О., Баїк О. Адміністративно-правова природа інформаційної безпеки // Вісник Національного університету «Львівська політехніка»: «Юридичні науки» № 3 (31), 2021. С. 167-179. URL:

28. https://science.lpnu.ua/sites/default/files/journal-paper/2021/nov/25402/25.pdf (дата звернення: 10.10.2022).

29. Погорілко М. Російський шпигун намагався влаштуватися на роботу до Гаазького трибуналу: хотів «розслідувати» воєнні злочини РФ // Obozrevatel. 2022. 16 черв. URL: https://news.obozrevatel.com/ukr/abroad/rosijskij-shpigun-namagavsya-vlashtuvatisya-na-robotu-do-gaazkogo-tribunalu-hotiv-rozsliduvati-vijskovi-zlochini-rf.htm (дата звернення: 10.09.2022).

30. Подоляк спростував російський фейк про від'їзд Зеленського з Києва // Слово і Діло. 2022. 4 берез. URL: https://www.slovoidilo.ua/2022/03/04/novyna/suspilstvo/podolyak-sprostuvav-rosijskyj-fejk-pro-vidyizd-zelenskoho-kyyeva (дата звернення: 15.11.2022).

31. Поліція Іспанії встановила, звідки надсилалися пакунки з вибухівкою – ЗМІ // Українська правда. 2022. 4 груд. URL: https://www.eurointegration.com.ua/news/2022/12/4/7151829/ (дата звернення: 04.12.2022).

32. Пріоритети міжпарламентського співробітництва Верховної Ради України у 2021 році. 2021. 5 берез. URL: https://www.rada.gov.ua/news/news_kom/204493.html (дата звернення: 04.09.2022).

33. Райхель Ю. Міжнародні журналістські пули у використанні сучасних терористичних практик // Комунікаційно-контентна безпека: гібридно-

месіанські агресії. Україна: 2014-2017 рр.: Тренінговий посібник для фахівців з питань комунікаційно-контентної (інформаційної) протидії. Київ, 2019. С. 66 - 74.

34. Рішення Ради національної безпеки і оборони України «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». ред. 2022. 25 жовт. URL: https://zakon.rada.gov.ua/laws/show/n0004525-17#Text (дата звернення: 10.09.2022).

35. Рішення Ради національної безпеки і оборони України «Про створення Центру протидії дезінформації». ред. 2021. 23 берез. URL: https://zakon.rada.gov.ua/laws/show/n0015525-21#n2 (дата звернення: 04.09.2022).

36. Солдатенко О. Інформаційний простір у мережі інтернет: правове регулювання та контроль // Підприємництво, господарство і право. 2018 (5). С. 134-140. URL: http://pgp-journal.kiev.ua/archive/2018/5/27.pdf (дата звернення: 10.09.2022).

37. Солодка О. Інформаційний простір держави як сфера реалізації інформаційного суверенітету // Інформація і право. № 4 (35). 2020. С. 39–46. URL: http://il.ippi.org.ua/article/view/221216 (дата звернення: 10.10.2022).

38. Стратегія публічної дипломатії МЗС України на 2021-2025 роки. ред. 2021. 24 берез. URL: https://mfa.gov.ua/storage/app/sites/1/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%97/public-diplomacy-strategy.pdf (дата звернення: 15.10.2022).

39. Стратегія розвитку інформаційного суспільства в Україні: ред. 2013. 15 трав. URL: https://www.kmu.gov.ua/npas/246420577 (дата звернення: 10.10.2022.).

40. Сухорольська І., Климчук І. Громадська (публічна) дипломатія в умовах агресивної війни Росії проти України // Вісник Львівського університету. Серія філос.-політолог. студії. 2022. (43), С. 322–331 URL: http://fps-visnyk.lnu.lviv.ua/archive/43_2022/39.pdf (дата звернення: 10.10.2022).

41. Указ Президента України №47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення: 10.09.2022).

42. Указ Президента України №121/2021 «Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України». URL: https://www.president.gov.ua/documents/1212021-37661 (дата звернення: 04.09.2022).

43. Указ Президента України №392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України». URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 10.10.2022).

44. Указ Президента України №555/2015 «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України». URL: https://www.president.gov.ua/documents/5552015-19443 (дата звернення: 04.09.2022).

45. Указ Президента України №685/2021 «Про рішення Ради національної безпеки і оборони «України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 04.09.2022).

46. Фіщенко Д. Інформаційна агресія в глобальному світі: формування стратегій спротиву як тактичних моделей контентних впливів // Комунікаційно-контентна безпека: гібридно-месіанські агресії. Україна: 2014-2017 рр.: Тренінговий посібник для фахівців з питань комунікаційно-контентної (інформаційної) протидії. Київ, 2019. С.74-81.

47. Хорошко В., Хохлачова Ю., Пірцхалава Т., Іванченко Є. Інформаційно-психологічні впливи та інформаційно-психологічна війна як складові частини

інформаційної боротьби // Український науковий журналі інформаційної безпеки. 2022, (28). С. 26-34.

48. Черненко В. Стан впровадження публічної дипломатії як складової системи стратегічних комунікацій // Національний інститут стратегічних досліджень. URL: https://niss.gov.ua/sites/default/files/2021-12/az-publichna-diplomatiya_chernenko_20122021.pdf (дата звернення: 19.09.2022).

49. Які «темники» пропаганди зараз просуває Кремль // Центр протидії дезінформації при РНБО України. 2022. 25 Лист. URL: https://cpd.gov.ua/articles/4763/ (дата звернення: 10.09.2022).