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: **«Інформаційний фронт України в умовах російсько-української війни»**

Виконала студентка 5 курсу, групи ЗММВ-21
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»
освітньо-професійної програми
«Міжнародні відносини»

Гуда Аліна Олегівна

Керівник – кандидат політичних наук, старший викладач
Близняк Ольга Анатоліївна

Робота допущена до захисту

(протокол №___засідання кафедри міжнародних відносин від
_____20___року

Завідувач кафедри міжнародних відносин: Сидорук Тетяна Віталіївна

м. Острог – 2023 р.

ЗМІСТ

ВСТУП

Актуальність теми дослідження

В останні десятиліття розпочався новий етап у розвитку цивілізації – епоха інформаційного суспільства, яка характеризується посиленням ролі знань у будь-якому формі вираження. Розвинені країни рухаються до інформаційного суспільства, де якість життя та соціальні зміни залежать від використання інформації. Тому людині неминуче доводиться весь час перебувати в інформаційному середовищі і формувати світогляд під впливом інформаційного середовища.

Слід зазначити, що використання інформаційних технологій для впливу на свідомість є дуже актуальним для України, країни, яка перебуває у стані війни. Російська Федерація проводить агресивну інформаційну політику проти нашої держави на окупованих територіях України та на міжнародній арені. Крім того, варто зазначити, що інформаційний елемент сучасного асиметричного протистояння між Росією та Україною є окремою складовою цього протистояння, і в більшості випадків не менш важливим, ніж військовий елемент.

У висвітленні військових конфліктів ЗМІ є одним із основних джерел інформації про перебіг подій. Ця інформація може бути об’єктивною, неупередженою та придатною до маніпулювання. Порядок денний новин і те, як вони представлені, можуть сприяти вирішенню конфліктів або, навпаки, сприяти їх ескалації. Розвиток соціальних мереж он-лайн та глобалізація міжнародного суспільства активно використовується у військовій промисловості не лише для реалізації процесів управління, а й для ведення віртуальних бойових дій та забезпечення реалістичних військових протистоянь. Технології 2.0 органічно вписалися в інформаційну та психологічну парадигми так званої гібридної війни, значення якої зростало з арифметичною прогресією кожного наступного міжнародного військового конфлікту.

У війні, яка сьогодні йде в Україні, провідне місце займають інформаційні баталії. Постріли та вибухи, репортажі та коментарі стали знаряддям гібридної війни. Репортер на війні – це той же боєць, в якого головна його зброя – слово.

Інформаційний фронт не менш важливий, ніж військові і тактичні заходи на передовій.

Аналіз стану наукової розробки проблеми. Різним аспектам поняття інформаційна війна, інформаційна безпека, протидії гібридним та інформаційним впливам присвячена значна увага широкого кола дослідників. Зокрема, над питанням правового забезпечення інформаційної безпеки зосереджуються такі дослідники, як: Довгань О. Д., Кунєв Ю. Д., Сливка М. М., Хорошко В.

Вони вказують що, забезпечення інформаційної безпеки – це комплекс заходів, спрямованих на недопущення інформації та інформаційної інфраструктури завдати шкоди властивостям об’єктів безпеки, а також засобам і суб’єктам цієї діяльності. Загалом правові норми національної інформаційної безпеки є невід’ємною частиною основного закону про адміністрування інформації.Як галузь інформаційного права, структура правових норм національної інформаційної безпеки складається з органів конфіденційності, захисту інформації, відповідальності за порушення в цій сфері і т.д. Справді, вдосконалення правового забезпечення інформаційної безпеки в Україні потребує комплексного перегляду вітчизняного інформаційного законодавства.

Концепцію інформаційної безпеки досліджували наступні вчені: Антонова С.Є., Дмитренко М.А., Ільницька У., Сафаров А. Зокрема, Антонова С. Є. зазначає, що інформаційна безпека визначається як: стан безпеки інформаційного простору; стан захищеності національних інтересів України в інформаційному середовищі; правила, встановлені законодавством про захист; суспільні відносини, пов’язані із захистом життєво важливих інтересів людини і громадянина, політичної, економічної, оборонної та інших складових національної безпеки.

Ільницька У. вказує, що інформаційна безпека є невід’ємною частиною національної безпеки і вважається пріоритетною функцією держави. Дослідниця також зазначили, що інформаційна безпека вважається як самостійним

елементом національної безпеки будь-якої країни, так і невід'ємною частиною будь-якої іншої безпеки.

До більш глибоких досліджень інформаційної війни та інформаційних фронтів належать: Корсунський С., Ніколаєнко Н., Герасименко П., Орел В., Сабрі К.Н., Скібіцька Ю. та ін. За визначенням Н. Ніколаєнко, інформаційний фронт складається з низки інформаційно-психологічних прийомів впливу та протидії, спрямованих на зміну стану масової та індивідуальної свідомості.

Сабрі К. Н. описує напрямок, в якому розгортається інформаційний фронт, особливо населення зони конфлікту, громадяни держави-агресора, міжнародна спільнота.

Дослідження Ілюка К зробили вагомий внесок у вивчення інформаційних воєн та інформаційних фронтів. Автор зазначає, що інформаційний фронт під час війни безпосередньо обслуговує бойові дії, а інформаційна війна – це не просто ілюзія. Більше того, фейки є найменшою одиницею такого роду війни. Структура російської інформаційної війни така: наратив, інформація, дезінформація та маніпуляція.

Варто згадати ще одного дослідника А. Шуляка, який досліджує питання інформаційного обміну між Україною та зарубіжними державами. Зокрема, він визначає інформаційну безпеку як набір заходів, призначених для забезпечення безпеки інформації від несанкціонованого доступу, використання, розголошення, знищення, модифікації, перегляду, перевірки, запису або знищення. та її дослідження інформаційної гігієни. Оскільки інформація може водночас сприяти національній стабільності та соціально-економічному розвитку, але водночас становить загрозу національним інтересам, Україні слід уважніше ставитися до інформаційної гігієни.

Серед зарубіжних вчених можна виділити: Patric De Schutter, Mithum Sarkar, Mike Dahm та ін. Вони зазначають, що у сучасній війні інформаційна війна може приймати різні форми, так як сьогодні існує широкий спектр доступний технологій і методів обміну інформацією. Однією із психологічних операцій інформаційної війни є дезінформація, яку дослідники називають

навмисним поширенням неправдивої або частково невірної інформації. Це знамениті «фейкові новини», інформація, створена з повітря або модифікована для впливу на громадську думку.

Попри значний інтерес до теми інформації, інформаційної війни, безпеки в інформаційному просторі, проблему інформаційного фронту в умовах російсько-української війни досліджено не достатньо, а тому ця тема потребує ширшої дослідницької уваги.

Метою кваліфікаційної роботи є вивчення особливостей інформаційного фронту України в умовах російсько-української війни.

Досягнення цієї мети передбачає вирішення наступних **завдань**:

- дослідити основні характеристики інформаційної війни;
- дослідити фактори, які спричинили та підсилюють інформаційну війну РФ проти України;
- визначити роль українського інформаційного фронту та його розвиток;
- визначити проблеми та перспективи інформаційного простору України.

Об'єктом дослідження є інформаційний простір України.

Предметом дослідження інформаційний фронт в умовах російської агресії на Україну.

Методи дослідження. Робота виконана в рамках комплексного підходу та спирається на принципи об'єктивності та узагальнення, порівнянні та аналізі наукової літератури та інтернет-джерел.

Методологічною основою дослідження стала сукупність методів, підходів та прийомів наукового пізнання – як загальнонаукових, так і спеціальних. Серед загальнонаукових методів було використано метод спостереження, порівняння та аналіз. Завдяки яким було розглянуто та проаналізовано інформаційний простір України раніше та зараз.

Основним методом дослідження є системний аналіз, що дозволяє представити суб'єкти дослідження як елементи цілісної системи. При вирішенні

головної мети дослідження загальнонаукові методи поєднуються з методом аналізу документів та кількісного аналізу. У процесі дослідження виникнення та розвитку інформаційної війни був використаний історичний метод та метод спостереження. Системно-функціональний та структурно-функціональний методи дозволяють досліджувати правові основи інформаційного суспільства як єдиний системний механізм, структурні елементи якого функціонують як єдине ціле.

Хронологічні рамки: 2014 рік до сьогодення.

Вибір нижньої хронологічної межі пов'язаний з початком російської агресії на Сході та окупацією о. Крим.

Вибір верхньої хронологічної межі обґрунтовано тим, що повномасштабне вторгнення, та, відповідно, інформаційна війна триває і зараз.

Географічні рамки: Україна та Росія.

Джерельна база дослідження. Джерельну базу дослідження можна умовно поділити на 3 групи. Першу групу джерел складають нормативно-правові документи, договори, доктрини, стратегії, законодавчі акти щодо інформаційного простору та інформаційної безпеки України. Зокрема, Стратегія інформаційної безпеки України, що розкриває відповіді на низку питань щодо того, що є загрозами інформаційній безпеці для нашої держави, проаналізовано механізми протидії тощо. Також, Закон України «Про Інформацію», де визначено такі терміни, як документ, захист інформації, власне сама інформація та її види.

Другу групу джерел складають довідники, монографії, наукові статті де розкривається теоретичні основи поняття інформаційного простору, інформаційного фронту, інформаційної війни та безпеки.

Третьою групою дослідження є інтернет джерела, зокрема російські та українські новини на телебаченні, у соцмережах та на просторах інтернету. Розглянуто міжнародні засоби масової інформації, які дають змогу простежити практичні аспекти функціонування інформаційного простору України в умовах російсько-української війни, а також те як війну в Україні сприймають закордоном.

Структура роботи: вступ, 3 розділи, висновки, список використаних джерел та літератури.

Апробація результатів: опублікована стаття на тему «Інструментарій російських інформаційних війн в умовах російської агресії в Україні» студентсько-аспірантському збірнику наукових праць, випуск 8. Публікація статті на науковому блозі НаУОА, на тему «Висвітлення російсько-української війни у міжнародних ЗМІ».

РОЗДІЛ 1. СУТНІСТЬ ТА ЗНАЧЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В ІНФОРМАЦІЙНІЙ ВІЙНІ РФ ПРОТИ УКРАЇНИ

1.1. Основні характеристики поняття інформаційної війни

Інформаційні технології дедалі більше визначають характер часу і мають сильний вплив на всі сфери сучасного суспільного життя. Вони стали важливою частиною соціальної реальності. Крім того, на відміну від енергетичних, транспортних і хімічних технологій, вони не мають жорстких ресурсних і екологічних обмежень, що надає процесу специфіку. Інформаційні технології відновлюються набагато швидше за інші технології: інформаційні технології оновлюються кожні 3-5 років. Інформаційне поле дедалі більше стає ареною міжнародної конкуренції, створюючи загрозу національним інтересам. Розвиток глобальної інформатизації та Інтернету зробили інформаційну інфраструктуру та національні ресурси різних країн уразливими об’єктами для впливу іноземних держав, терористичних організацій, злочинних груп та окремих злочинців. Невід’ємним геополітичним фактором стала загроза міжнародного інформаційного тероризму та інформаційної війни [6].

Сьогодні інформаційна війна має багато визначень. За визначеннях багатьох науковців, інформаційна війна – це форма ведення інформаційного протиборства між різними суб’єктами (державами, неурядовими, економічними та іншими структурами), що передбачає комплексне ураження інформаційної сфери конкуруючих сторін та захисту власного інформаційного простору [28]. Інформаційна війна – це концепція яка передбачає використання в бойовому просторі та управління інформаційно-комунікаційними технологіями для досягнення конкурентної переваги над супротивником [75]. Значна проблема, пов’язана з будь-яким обговоренням інформаційної війни, полягає в тому, що цей термін залишається невизначеним Міністерством оборони, що призводить до великої кількості тлумачень. Серед більш проблематичних ознак інформаційної війни є ті, які описують її безкровну спробу, яка має все спільне з інформацією,

але, здається, не має нічого спільного з війною. Так наприклад, втручання у вибори може становити загрозу національній безпеці, але це не війна.

Томас Рона ввів термін «інформаційна війна» в 1976 році. Він оцінив, що інформаційна війна виникає з інформаційно-залежних систем зброї та військових операцій, контрольованих у величезному просторі в режимі реального часу. У дослідженні Томаса Рони «Управління оцінки мережі, систем озброєння та інформаційної війни Міністерства оборони» зазначається: «Необхідність систематичного визнання та використання цієї інформаційної війни як накладеної та переплетеної з більш видимим фізичним аспектом військової готовності та бойових операцій» – це є, мабуть, найважливішим повідомленням цього дослідження. Прогнози Томаса Рони щодо інформаційної війни 47 років тому стали реальністю. Інформаційні технології, які визначають та інтерпретують простір бою, переплетені та нерозривно пов'язані з фізичним простором. Інтелектуальна зброя харчується інформацією, щоб орієнтуватися у світі та шукати цілі. Інформаційні змагання в бойовому просторі перетинаються з операціями в наземній, морській, повітряній та космічній сферах, так само як ці області накладаються одна на одну [67].

Під час війни інформаційний фронт безпосередньо обслуговує бойові дії. Саме різними інструментами країна допомагає собі вести інформаційну війну. Якщо провести аналогію між кінетичною та інформаційною війною, то територію можна порівняти з увагою. Тобто воюють в інформаційній війні і привертають увагу. Як територію, вона може бути окупована або завойована. У динамічній війні є багато способів завоювати територію: атакувати артилерією, оточити місто або розпочати штурм амфібії. Схоже на увагу. Тож у цій метафорі фейки — це солдати інформаційної армії. Вони мають чітку місію. У порівнянні з технікою їх дуже багато. Над фейком є повідомлення – чітке та зрозуміле повідомлення. Вони схожі на ракети, запущені до конкретної цілі. Інформація може бути правдивою, маніпулятивною або просто неправильною. Може бути кілька повідомлень, іноді навіть суперечливих. Збірка повідомлень об'єднана в розповідь. Завдання наративу — сформувати певний світогляд. Стратегічно

наратив є найважливішим, оскільки інформацію можна змінювати, тоді як наратив є постійною історією. [14].

Інформаційна війна поділяється на сім категорій: командно-контрольна, хакерська, економічна, психологічна, розвідувальна, електронна та кібервійна. Багато визначень інформаційної війни можуть бути пов’язані зі складністю та багатогранністю цього явища та складністю проведення аналогій із традиційною війною. Для інформаційної війни захист зазвичай є чітко визначеним поняттям, де початок та кінець можна застосовувати лише до певних інформаційних операцій, коли лінії фронту не визначені, а атаки описуються різними моделями. Успішні виконані інформаційні операції не мають прямого відношення до співвідношення військового потенціалу обох сторін. Забезпечити інформаційну безпеку на місці національних та муніципальних рішень ґрунтуються на ретельному аналізі структур та змісту управління, а також обробка інформаційних процесів і використання під управлінням відповідних технологій [57].

Щоб не означало поняття «інформаційна війна», воно народилося в сфері військової промисловості і означає, перш за все, вираження напруженої, рішучої та небезпечної діяльності, пов’язаної з реалістичними бойовими діями. Важливо розуміти, що потрібно ефективно використовувати зброю і вміти захищатися від неї для забезпечення національної безпеки країни. Бажання вплинути на громадську дискусію в неправдивих інформаційно-психологічних операціях закордоном не є новиною, це вже давно інструмент в арсеналі націй. Змінюється рівень безпосередності, бізнесу та масштаби зусиль цих підприємств, що стають можливими завдяки зростаючій популярності Інтернету та все більшій актуальності для суспільства формування думки [31].

Військові розглядають інформаційну війну як електронну війну (наприклад, глушіння каналів зв’язку), системи спостереження, точні удари (наприклад, якщо розбомбити телекомунікаційні системи, це вважатиметься інформаційною війною) та вдосконалене управління на полі бою (використання

інформації та інформаційні системи для надання інформації, на якій базуються військові рішення приведенні війни) [75].

Інформаційна війна – це зброя. Це зброї, основними елементами якої є інформація, інформаційні технології (особливо технології інформаційного впливу), інформаційний процес і технічні засоби, для інформаційної боротьби. Методи управління інформаційною війною охоплюють багато сфер діяльності людини. Можна виділити такі: пропаганда, корупція у зовнішніх відносинах, підміна понять, міфологізація історичних фактів, використання підробок та альтернативних фантазій, тощо. Вони створюють негативне враження на внутріполітичне становище країни, тобто послаблюють опір, та протидію країні агресору [48].

У сучасну інформаційну епоху, військова конкурентоспроможність має здатність обробляти інформацію та інтегрувати її у військові дії, тим самим забезпечуючи їхній успіх. Зазвичай інформаційні технології мають вирішальний вплив на розвиток і розгортання конфлікту. Від процесу глобалізації та його відображенню на розвиток людства, використання інформації виходить далеко за межі ЗМІ. Сьогодні інформація має три способи впливу:

1. Посилання власного населення країни на тему протистояння – заміна прийнятих стандартів добробуту політичними цілями, такими як побудова світлого майбутнього, підготовка населення до «неминучої» війни чи військового конфлікту, зміщення фокусу з внутрішніх проблем на зовнішні, експлуатуючи суспільний пафос.
2. Масштабна пропаганда, інформаційна обробка людей в інших країнах і регіонах для забезпечення підтримки власних цілей, з використанням для цього окремих політиків, мігрантів, різноманітних об’єднань тощо.
3. Поширення неправдивої та спотвореної інформації, щоб ввести в оману інші уряди та міжнародні організації. Існує також створення, використання та підтримка маріонеткових урядів і квазіурядів, які

прямо чи опосередковано впливають на надання підтримки основним органам. [36].

Можна виділити так звану зброю інформаційної війни. Це збір інформації; передача інформації; захист інформації; маніпулювання інформацією; порушення, погіршення та заперечення інформації. Варто розглянути детальніше кожну «зброю». Збір інформації: інформаційна революція означає появу парадигми конфлікту, в якій сторона, яка знає більше, матиме вирішальну перевагу; тому збір інформації входить до складу інформаційної війни. Передумова полягає в тому, що наявність більшої кількості інформації підвищує обізнаність людини про ситуацію, що призводить до кращої підготовки до бою та, імовірно, кращих результатів. Технологія точного визначення місця розташування, така як навігація за допомогою глобальної системи позиціонування (GPS), значно пом'якшила ці проблеми. Технології розвідки та спостереження також певною мірою зробили можливим дізнатися про місцезнаходження ворога. Функції розвідки та спостереження також переходять до використання датчиків із такими спектрами, як інфрачервоний, ультрафіолетовий, нюховий, слуховий, оптичний, сейсмічний тощо, та інтеграції даних з них для створення цілісної картини. Оскільки ці технології можуть проникати в ситуації та отримувати точну інформацію з мінімальною втратою точності, збір інформації в інформаційній війні значно менш ризикований і набагато повніший. Передача інформації: інструментами на цій арені є не зброя, а цивільні технології, які застосовувалися у військових ситуаціях. Комунікаційна інфраструктура включає мережі комп'ютерів, маршрутизаторів, телефонних ліній, волоконно-оптичних кабелів, телефонів, телевізорів, радіо та інших технологій і протоколів передачі даних. Без цих технологій було б важко передавати інформацію в режимі реального часу, якого вимагають сучасні стандарти. Тут військовим потрібна мережева інфраструктура для передачі інформації.

Захист інформації: для захисту даних використовуються два види зброї. По-перше, це технології, які фізично захищають критичні сховища даних,

комп’ютери та транспортні механізми, такі як бомби та куленепробивні гільзи та пристрої запобігання проникненню, такі як замки та сканування відбитків пальців. Другий і, мабуть, більш важливий — це технологія, яка запобігає перегляду та перехопленню бітів опонентом. Це охоплює фундаментальні механізми безпеки комп’ютера, такі як паролі, і більш просунуту технологію, як-от шифрування шляхом шифрування його зв’язку та розкодування зв’язку іншої сторони. Кожна сторона веде фундаментальний акт інформаційної війни, захищаючи свій образ реальності, завдаючи шкоди іншій [83].

Маніпулювання інформацією проводиться з метою викривлення сприйняття реальності опонентом. Це можна зробити за допомогою різних технологій, таких як комп’ютерне програмне забезпечення, для зміни тексту, зображень, відео, аудіо та інших типів передачі даних. Обмежені дані зазвичай створюються вручну, щоб відповідальні особи могли контролювати зображення, надане ворогові. Порушення, деградація та заперечення є останніми аспектами інформаційної війни. Усі три стратегії не дозволяють противнику отримати вичерпну та точну інформацію. Завдяки своїй схожості багато однакових видів зброї використовуються для досягнення однієї чи кількох цілей. Тому є сенс обговорювати їх усі одночасно [83].

Інформаційна війна спрямована на сприйняття супротивника, яке знаходиться в когнітивному вимірі інформаційного середовища. Інформаційна війна зосереджена на знищенні знань, правди та достовірності, а не на фізичних чи цифрових артефактах; перші знаходяться в «мозковому просторі», а не в 3D-просторі чи кіберпросторі. Інформаційна війна спрямована на вселення страху, гніву, тривоги, невпевненості та сумнівів у процес прийняття рішень супротивником. Інформаційна війна спрямована на вплив на окремих осіб, організації, ЗМІ, урядові установи, політичне керівництво та соціальні класи [31].

Інформаційна війна включає в себе декілька прийомів:

- Знищення або порушення роботи комунікаційних та/або інформаційних систем супротивника. Зловмисник може, наприклад,

заглушити військовий зв’язок або системи зв’язку, задіяні в озброєнні противника. Він також може здійснювати атаки (фізичні або кібератаки) на системи зв’язку цивільних служб (аеропорти, фінансові ринки, лікарні), щоб пошкодити ці інфраструктури.

- Збір ключової інформації про супротивника, його стратегії та маневри. Шпигунство та аналіз особистих даних також є частиною цього.
- Нейтралізація певних засобів масової інформації (телебачення, радіо), інтернет-сайтів чи комп’ютерних мереж супротивника. Воююча сторона може глушити телевізійні передачі свого опонента або запускати атаки розподіленої відмови в обслуговуванні (DDoS). Ці DDoS атаки спрямовані на нейтралізацію комп’ютера, мережі чи веб-сайту, переповнюючи його великою кількістю комп’ютерних запитів. Заражений комп’ютер, мережа або веб-сайт переповнюються їх кількістю і стають неефективними.
- І останнє, але не менш важливе, поширення неправдивої інформації чи пропаганди з метою маніпулювання громадською думкою опонента чи його деморалізації. У деяких випадках телевізійні канали чи інтернет-сайти можуть навіть бути зламані для трансляції повідомлень дезінформації [68].

Інформаційна війна поділяється на такі категорії:

1. Війна на основі розвідувальних даних – це сенсорна технологія, яка безпосередньо руйнує технологічні системи, війна яка складається з проектування, захисту.
2. Електронна боротьба використовує радіолелектронні та криптографічні методи для погіршення зв’язку. Радіоелектронні методи атакують фізичні засоби передачі інформації. Тоді як криптографічні методи використовують біти та байти, щоб порушити засоби передачі інформації.

3. Психологічна війна – це використання різноманітних прийомів, таких як пропаганда. Інформаційний терор для деморалізації супротивника в спробі досягти успіху в битві.
4. Хакерська війна, мета якої може варіюватися від вимкнення систем, помилок даних, крадіжки інформації, крадіжки послуг, моніторингу системи, неправдивих повідомлень і доступу до даних. Для здійснення таких атак хакери зазвичай використовують віруси, логічні бомби та сніфери.
5. Економічна війна може вплинути на економіку бізнесу чи країни, блокуючи потік інформації. Це може бути особливо руйнівним для організацій, які ведуть великий бізнес у цифровому світі.
6. Кібервійна - використання інформаційних систем проти віртуальних особистостей окремих осіб або груп. Це найширша з усіх інформаційних війн і включає інформаційний тероризм, семантичні атаки [80].

Чим страшна кібервійна та загалом інформаційна війна для суспільства?

Перш за все, стратегічна кібервійна не розрізняє цивільних і військових: так само, як ядерна зброя під час холодної війни, кіберзброя з такою ж імовірністю буде націлена на цивільні ресурси, як і на військові. Незважаючи на те, що ядерна зброя, очевидно, набагато шкідливіша, ніж зловмисне програмне забезпечення, інформаційна війна або ж кібератака може призвести до жертв і смертей серед цивільного населення. По-друге, важко зрозуміти хто здійснив кібератаки, у тому уряди повинні нести відповідальність за свої дії. Однією із сфер де кіберзброя є набагато гіршою за ядерну, є визначення авторства – з’ясування того, хто запустив зброю в перше місце. Дуже легко приховати, звідки ви зламуєте комп’ютер, тому що ви можете пройти через проксі маску, звідки надходить ваш трафік. Навіть якщо ви з’ясували, звідки взявся комп’ютер, ще одна величезна проблема – з’ясувати, ким була людина, яка сиділа за клавіатурою, а тим більше, чи була вона урядовим агентом. Без вказівки авторства ви не можете бути підзвітними. А без підзвітності такі речі, як

стримування та взаємне гарантоване знищення, не працюють. Якщо уряд не несе відповідальності за свої кібератаки під час кібервійни, він завжди може здійснити шкідливі, начебто терористичні атаки, як-от виведення з ладу електромережі країни або саботування промислових систем, щоб фізично (і небезпечно) пошкодити інфраструктуру або міста. В обох випадках, швидше за все, загинуть невинні цивільні особи [72].

Загалом можна виділити 5 основних речей, які варто знати про інформаційну війну. 1. Дезінформація виникає, коли супротивник свідомо поширює брехню. Деякі супротивники значною мірою покладаються на дезінформацію через перешкоди або плутанину, яку вона створює. Результат заважає або затримує аудиторію вжити правильних дій або спонукає аудиторію вживати впевнених, але необережних дій.

2. Не все, що вам не подобається, є дезінформацією. Це може бути риторична інформація, боротьба ідей і цінностей. Це головний виклик, з яким доводиться стикатися в інформаційній війні — те, що не є брехнею, але може бути не зовсім правдою. Це залежить від поглядів — переконань, упереджень, освіти чи навіть культурних особливостей.

3. Недоброзичливці блокують або видаляють інформацію, щоб вплинути на думку. Відсутня інформація — це коли цільовій аудиторії не вистачає інформації для вжиття обґрунтованих дій.

4. Почуватися добре не означає робити добро. Важливо точно оцінювати інформаційне середовище та зосереджуватися на зміні поведінки, а не лише на тому, як повідомлення викликає у людей почуття.

5. Ніхто не може виграти інформаційну війну, вони можуть лише брати участь. Оскільки це стосується того, як віра та думка виявляють дії у фізичному середовищі, не існує такого поняття, як постійний контроль чи остаточно виграна битва. Це про те, як люди спілкуються один з одним, а ідеї передаються через мільярди мобільних пристроїв. Це лише участь [71].

Тобто, інформаційна війна, яка має безліч визначень, є невід’ємною частиною сьогодення та традиційної війни. Як звичній для нас війні, так і

інформаційній, притаманна зброя. Однак відмінністю є те, що інформаційна війна зосереджується на руйнуванні знань або сприйняття, а не на фізичних поразках.

1.2. Інструментарій російських інформаційних війн в умовах російської агресії в Україні

Під час холодної війни радянські «активні заходи» включали маніпулювання засобами масової інформації – наприклад, втручання у створення законного документального фільму в Західній Німеччині з метою посилення напруженості через нацистське минуле країни. Сучасна ж версія покладається на Інтернет для ширшого, більш адаптованого розповсюдження. Напад Росії на Україну називають першою у світі війною TikTok, оскільки стільки повідомлень як за, так і проти зведено до коротких відео в додатку. Також спотворене контрпрограмування процвітає в додатках для обміну повідомленнями, як-от Telegram, соціальних мережах та інших місцях – рекламуючи уявну логіку «спеціальної військової операції» Росії, пропагуючи різанину та дискредитуючи українських біженців. Натиск Росії породив лише останній приклад боротьби за допомогою пропаганди, яка може бути більш поширеною, ніж багато хто припускає [86].

З моменту приходу Володимира Путіна на посаду президента Росії в грудні 1999 року не було єдиної цілісної доктрини інформаційної війни. Натомість російський уряд опублікував серію доктрин інформаційної безпеки, концепцій зовнішньої політики, військових доктрин та інших політичних і стратегічних документів, які встановлюють стратегічні та оперативні пріоритети для російського інформаційного апарату та, у сукупності, викладають, як Кремль думає про інформацію та Інтернет, а також конкуренцію та конфлікти в цьому просторі.

Доктрина інформаційної безпеки Російської Федерації 2000 року проголосила, що «національна безпека Російської Федерації істотно залежить від рівня інформаційної безпеки, і з технічним прогресом ця залежність неминуче посилюватиметься» [8]. Документ визначає інформаційну безпеку як «стан

захищеності своїх національних інтересів в інформаційній сфері, що визначається загальною збалансованістю інтересів на рівні особи, суспільства і держави». Доктрина інформаційної безпеки 2016 року, підписана в грудні того ж року, замінила попередню доктрину 2000 року. У новій редакції документу значно розширено поняття інформаційної безпеки, додаючи пряме згадування про «внутрішні та зовнішні інформаційні загрози» проти Росії. У доктрині зазначалося, що «іноземні країни нарощують свій потенціал інформаційних технологій, щоб впливати на інформаційну інфраструктуру під час проведення військових операцій». Стратегія національної безпеки, яка була прийнята до 2021 року ще більше посилила явну параною Кремля, заявивши, що вороги Росії включають іноземні технологічні компанії, які «поширюють неперевірену інформацію», і що «спотворене уявлення про історичні факти, а також події, що відбуваються в Російській Федерації та у світі, нав'язуються користувачам Інтернету з політичних міркувань» [87]. Відтак, можна зробити висновок, що інформаційна складова є особливо важливою складовою і національної і інформаційної безпеки.

Сучасну російську модель пропаганди можна характеризувати як «пожежний шланг брехні» через дві її відмінні риси: велику кількість каналів і повідомлень і безсоромну готовність поширювати часткову правду чи відверту вигадку. За словами одного спостерігача, Джорджіо Бертолін [64], «нова російська пропаганда розважає, заплутує і переповнює аудиторію». Сучасна російська пропаганда має принаймні ще дві відмінні риси. Вона також швидка, безперервна і повторювана, і їй не вистачає послідовності. Цікаво, що деякі з цих особливостей прямо суперечать загальноприйнятій думці про ефективний вплив і комунікацію з боку уряду чи оборонних джерел, які традиційно наголошують на важливості правди, достовірності та уникнення протиріч. Незважаючи на ігнорування цих традиційних принципів, Росія, схоже, досягла певного успіху в рамках своєї сучасної моделі пропаганди або через більш пряме переконання та вплив, або шляхом заплутування, плутанини та зриву чи зменшення правдивих повідомлень [81].

Інформаційна війна Росії використовується перш за все для встановлення російського домінування в її колишній зоні впливу, яка включає колишні радянські та комуністичні республіки та території, які раніше входили до складу Російської імперії або перебували під її впливом. Зараз Росія веде, те що вона називає «війною нового покоління» (NGW). Ця війна використовує будь-які методи примусу, крім відкритої звичайної війни, включаючи інформаційну війну, політичний та економічний тиск. Ця стратегія використовується в надії на те, що Росія зможе змусити НАТО уповільнити або навіть скасувати свій вплив і експансію на російське «ближнє зарубіжжя». Аналіз відомих російських інформаційних операцій у західних демократіях висвітлює три ключові головні цілі: дискредитувати надійні демократичні інституції, розділити західну коаліцію та підірвати наднаціональні організації, які підтримують і просувають ці демократичні цінності. Медіа, що підтримується російським урядом і російськими тролями та ботами, стали ключовим елементом російської кампанії інформаційної війни. Вони працюють над просуванням версії світових подій, яка відповідає цілям російської зовнішньої політики, підриваючи як міжнародну систему після холодної війни, де домінував Захід, так і глобальні демократичні інституції. Вони сприяли зміцненню екстремізму по обидва боки політичного спектру та працювали цілеспрямовано, щоб допомогти Росії в зовнішніх операціях [65].

Росія має добре розвинену програму наступальних кібератак. Вона розробила тактику та зброю, спрямовану на забезпечення домінування в інформаційному «бойовому просторі», випробувану в Грузії та Україні. Ще від 2014 року Україні мережі стільникового зв’язку та інтернет-з’єднання були порушені та закриті, державні веб-сайти були переповнені DDOS-атаками, соціальні мережі були пошкоджені, а інтернет- і телефонні кабелі були перерізані проросійськими силами. Російські спецназівці, які встановили обладнання для блокування мобільних телефонів для членів українського уряду та депутатів законодавчої гілки влади, атакували базу Укртелекому в Криму. Кіберзброю використовували для зараження державних і неурядових систем комп’ютерними

вірусами, логічними бомбами, троянами та ботнетами для придушення обміну інформацією в телекомунікаційних мережах і передачі необхідної інформації за допомогою DDOS-атак. Для впровадження вірусів, шкідливих програм у державні та корпоративні інформаційні мережі розроблено та придбано/адаптовано у злочинних угруповань методики [76].

Також варто навести приклади російської брехні та правду, що поширювалось у ЗМІ у січні 2022 року. Перше, те що Україна та українські урядовці є агресором у російсько-українських відносинах. Однак усім відомо, що Росія вторглася в Україну в 2014 році, окупувала Крим, контролює збройні сили на Донбасі і вже починала накопичувати понад 100 000 військових на кордоні з Україною, а Володимир Путін погрожував «військово-технічними» заходами у відповідь, якщо його вимоги не будуть виконані. Друге, це те що Захід штовхав Україну до конфлікту і розведення Росією бойових сил є звичайним передислокуванням військ на власній території. Однак, Росія першою спровокувала нинішню кризу, розмістивши військових на кордоні з Україною, без жодної подібної військової діяльності з українського боку кордону. Ну і звичайно, те що Росія захищає етнічних росіян в Україні. Однак, немає жодних достовірних повідомлень про те, що етнічні росіяни або російськомовні люди перебували під загрозою з боку українського уряду (або ж як люблять говорити росіяни, що українці 8 років самі бомбили Донбас) [70].

Напередодні вторгнення Росії в Україну та під час триваючого конфлікту, соціальні медіа стали полем битви, де державні і недержавні актори пошрюють конкуруючі наративи про війну та зображують поточний конфлікт у своїх власних термінах. Оскільки війна триває, ці цифрові екосистеми заповнені дезінформацією. Стратегічні пропагандистські кампанії, включаючи дезінформацію, аж ніяк не є чимось новим у воєнний час, але перехід до соціальних медіа як основного каналу комунікації змінює тих, хто може брати участь у поточних розмовах для формування нових наративів [82].

23 лютого 2022 року, за день до вторгнення, Служба військової розвідки Росії (ГРУ) здійснила кілька деструктивних кібератак зі знищенням даних проти

українського уряду та інших ІТ, енергетичних і фінансових організацій. Ці атаки призначені для підтримки майбутніх наземних і повітряних ударів. Видаляючи дані з державних системи, Росія, можливо, намагається уповільнити координацію сил оборони України та державних служб. Очікувалося, що кіберможливості можна буде використовувати таким чином напередодні війни, але це використання дуже руйнівного зловмисного програмного забезпечення в кількох ітераціях має нові якості [55].

24 лютого Україна прокинулася від вибухів. Окупанти разом із ракетами атакують нас фейками, маніпуляціями, чутками та всіляким інформаційним мотлохом. Навіть ті, хто вважав себе захищеним від демпінгу, поширюють сумнівні новини. Теми змінюються щогодини. Ніхто не готовий до такого потоку інформації. Ні влада, ні ЗМІ, ні навіть громадяни. Після вторгнення Росії в Україну ЄС заблокував RT (Russia Today) і Sputnik, два головні канали Кремля для поширення пропаганди та дезінформації про війну. Через майже шість місяців кількість веб-сайтів, які рекламують той самий контент, різко зросла, оскільки Росія знайшла способи уникнути заборони. Вони перейменували та змінили свою роботу, щоб приховати її. Частину пропагандистських обов'язків вони переклали на дипломатів. Вони вирізали та вставили більшу частину вмісту на нові веб-сайти, які поки що не мають жодних очевидних зв'язків з Росією. NewsGuard, нью-йоркська компанія, яка спеціалізується на дослідженні та моніторингу дезінформації в Інтернеті, наразі виявила 250 веб-сайтів, які активно поширюють російську дезінформацію про війну, а за останні місяці додано десятки інших. Заяви на цих сайтах включають звинувачення в тому, що українські військові здійснили кілька смертоносних атак на Росію, щоб заручитися глобальною підтримкою, що президент України Володимир Зеленський підробив публічні виступи або що українські біженці скоюють злочини в Німеччині та Польщі. [77].

Багато з них також були створені задовго до війни і не мали жодного зв'язку з російським урядом, поки раптом не почали поширювати аргументи Кремля. У NewsGuard їх називають сплячими сайтами. Вони поступово формують

аудиторію, розміщуючи нейтральні матеріали, а потім переходять до пропаганди або надання дезінформації, коли це потрібно Кремлю. Дослідники знайшли кілька статей про українських біженців, опублікованих на офіційному сайті RT. Потім вони використали пошук в Google, щоб знайти ресурси, що публікують матеріали з однаковою назвою – близько 66 ідентичних частин в вмісту німецькою, іспанською англійською та французькою мовами [47].

Дезінформація навколо широкомасштабного вторгнення російських військ в Україну в лютому 2022 року ознаменувала ескалацію тривалої інформаційної кампанії Росії проти України та відкритих демократій. Оскільки обмеження щодо політичної опозиції в Росії продовжують посилюватися, дезінформаційний наратив розвинувся з пропаганди та історичного ревізіонізму — наполягаючи, наприклад, на тому, що Крим «завжди був російським» після його анексії Москвою в 2014 році. Хибні твердження, що неонацисти проникли в Україну. Урядові та теоретичні змови щодо українських/американських лабораторій з біозброї. Ці зусилля представляють багато способів, як російський уряд і союзники використовують дезінформацію як зброю, щоб відвернути, заплутати та послабити своїх супротивників.

Російські наративи дезінформації часто є неправдивими або розпливчастими фактами з напівправдою та «щось про це» (спроба відповісти на запитання, порівнюючи його з іншим запитанням, яке не має нічого спільного з початковим запитанням). Російські актори використовують різні тактики, щоб представити, посилити та поширити неправдиві та спотворені наративи по всьому світу.

Російські пропагандистські та дезінформаційні кампанії проводяться у великому масштабі та поширюються через велику кількість каналів, включаюси онлайн та традиційні ЗМІ. Наприклад, у 2020 році Facebook виявив, що російські військові операції, націлені на Україну, створювали фальшиві профілі Facebook під виглядом журналістів і намагалися поширювати дезінформацію у спосіб, який здавався більш достовірним. Відверто кажучи, російський уряд проводить скоординовану інформаційну (і дезінформаційну) діяльність у власних акаунтах

у соціальних мережах. Наприклад, з 25 лютого по 3 березня 2022 року 75 російських урядових облікових записів у Twitter опублікували 1157 твітів із 7,3 мільйонами підписників, 35,9 мільйонами ретвітів, 29,8 мільйонами лайків і 4 мільйонами відповідей. Близько 75% твітів стосувалися України, багато з яких поширювали дезінформацію. Наративи, які ставлять під сумнів статус України як суверенної держави, привертають увагу до ймовірних військових злочинів інших країн і поширюють теорії змови [69].

У березні 2022 року в Росії був введений закон про доповнення Кримінального кодексу РФ, в якому стаття 207.3 передбачає покарання за поширення «завідомо неправдивої інформації про діяльність збройних сил РФ і за «дискредитацію використання російських військових», у тому числі кваліфікуючи їхні дії як «війну» або «вторгнення». Санкції статті – від штрафу (в розмірі до півтора мільйона рублів) до позбавлення волі на строк до 15 років. Цей же закон передбачає кримінальну відповідальність за заклики до санкцій проти Росії. Для боротьби зі зростаючими візуальними доказами смерті та руйнувань у густонаселених районах України, які суперечили офіційним повідомленням про моральність вторгнення, Кремль запустив кампанії в соціальних мережах та особисті мітинги, «кампанію букв Z» та інші подібні зусилля диверсії/приховування.

Свідки задокументували тортури та вбивства цивільних осіб російськими військами після того, як Росія була змушена вийти з північної України. Москва у відповідь створила численні брехні, щоб заплутати аудиторію вітчизняну та іноземну аудиторію, стверджуючи, що Україна або влаштувала фальшиві масові вбивства, або вчинила справжні. Росія також відкрито використовувала та продовжує використовувати дипломатичні канали для поширення пропаганди та дезінформації, а російські посольства та установи не уникали поширення відверто фейкової інформації. Так, наприклад, у Польщі Росія намагалася використати складну історію двох країн як сусідів. Операція з маніпулювання інформацією інсинували та поширювали дезінформацію про нібито наміри Польщі анексувати українські території, включно з фальсифікацією документів.

У Франції Росія зосередилася на тому, щоб представити Україну як ненадійного партнера, розповсюджуючи історії про те, що зброя, яку постачають європейські партнери, продається третім країнам, з метою затримання постачання зброї [78].

Загальна кількість операцій під час російсько-української війни може бути невідомою, але в серпні 2022 року Група реагування на комп'ютерні надзвичайні ситуації України (CERT-UA) повідомила про понад 1123 кібератаки за першу половину війни. Це означає триразове зростання кіберактивності порівняно з довоєнним періодом. У січні 2023 року CERT-UA повідомляла, що Україна відповіла на понад 2194 атаки. У квітні 2022 року дослідники виявили Industroyer2, зловмисне програмне забезпечення, призначене для впливу на промислові системи управління в енергетичній мережі України.

Незалежно від типу атаки, головною метою російських кібератак було калічити українську державу та суспільство на стратегічному рівні. Замість того, щоб знищити чи перешкодити українським військовим силам чи системам озброєння, російські кібероперації були спрямовані на загальну волю українського народу та його здатність захищати себе. Проте мало доказів того, що ці операції мали стратегічні наслідки, такі як зниження волі українців до опору. Навпаки, дослідження показують, що стратегічні атаки на цивільну інфраструктуру не зменшують бажання противника чинити опір, а радше викликають об'єднання навколо ефекту прапора, який створює потужну підтримку керівництва країни, що захищається [84].

Режим Володимира Путіна має досвід пропагандистських кампаній, і соціальні медіа в Україні здебільшого спрямовані знизу вгору, тоді як російський авторитарний підхід «зверху вниз» відзначений обмеженням вільного потоку інформації та призупиненням доступу до соціальних медіа та вербуванням платних тролів. Російські ЗМІ та діяльність, пов'язана з Кремлем, зображують український уряд як повним сатаністів і терористів. Вони поширюють чутки про те, що Україна продає західну зброю в темній мережі з метою наживи.

Росія все частіше використовує новомову, як засіб пропаганди для контролю та соціальних настроїв. «Новомова» – це варіація та спотворення слів

та словосполучень. Новомову створює режим, але керується пропагандистськими ЗМІ та послідовниками. ЗМІ в тоталітарних державах використовують новомову, бо цього хоче режим Путіна. Якщо керівництво захотіло називати табори смерті «концтаборами», це видання не піддаватиме сумніву таке прохання згори. Причина проста: або на журналістів також впливає ідеологія, або вони занадто залежні від режиму, щоб чинити опір, або і те, і інше. Наприклад, навіть так звані опозиційні російські ЗМІ «Дождь» і «Медуза», що працюють за межами Росії, використовують Новомову у своїх публікаціях. Зокрема, замість слова «війна» вони вживають термін «спецоперація», а замість «вибух» — «хлопок». Основним словосполученням сучасної російської новомови є «спеціальна військова операція», яка вживається державою-агресором замість слова «війна». У Росії люди бояться цього слова і роблять все можливе, щоб його не вживати, тому що називати речі своїми іменами – означає їх впізнавати. Ігнорування слова «війна» допомагає применшити серйозність ситуації та знизити рівень напруги серед населення. Крім того, відкрито оголосити війну означає визнати, що вона є агресором, а Росія стверджує, що першою атакувала не Росія, а Україна, яку захищає НАТО. [30].

У 2022 році вороги найчастіше використовували такі теми для створення і поширення фейків:

- звинувачення Збройних Сил України в обстрілі мирних жителів та обстрілі Запорізької АЕС;
- звинувачували українську владу у небажанні вести переговори з Російською Федерацією;
- твердження про те, що Україна є нацистською державою;
- суб’єкти санкцій проти Російської Федерації;
- погрози Росії застосувати ядерну зброю;
- біологічні лабораторії США, які нібито працюють в Україні;
- енергетична криза в Україні та прогнози, що українці не переживуть темну холодну зиму [59].

Загальний план Російської Федерації щодо гібридної війни в Україні такий. Гібридна війна починається з інформаційної війни та народних заворушень проти чинної влади. На другому етапі агітатори, провокатори та диверсанти під виглядом місцевих жителів підбурюють та нагнітають ситуацію. Поступово організаційну ініціативу перебирають на себе кадри, завербовані спецслужбами Російської Федерації і навіть громадяни РФ. Згодом, у міру ескалації конфлікту та переходу його у збройну фазу, до нього підключаються добровольці та найманці, збройознавці та спецпризначенці з РФ, які діяли приховано від імені місцевих ополченців, або діяли відкрито та відверто, не приховуючи свого російського громадянства.

Новою формою інформаційного впливу стає розкрадання української історії, творчості, мови та ментальності. Тут слід звернути увагу на створення паралельних історій, які повністю або частково змінили та/або відходили від правдивих історичних фактів та поставила під сумнів державність України. Це навіть відрізняється від радянського трактування історії. Було поставлено під сумнів існування Київської Русі, термін Русь трактують як щось, що пов’язане з Росією, національних українських героїв різних часів перетворено на зрадників та ворогів, спекулюють питанням мови та віри. Що стосується української мови, то з одного боку, її намагаються представити як окремий діалект чи сільську мову, а з іншого боку, її намагаються вкрасти.

Так, до початку нового 2022/2023 навчального року Міносвіти РФ підготувало підручник з класичної української мови, підвищило кваліфікацію вчителів. Яскравим прикладом крадіжки творчості та мови є створення якісної української пісні «Пливе кача», яка стала дуже популярною в російськомовному Інтернеті. Спочатку вона нагадувала популярну під час Революції Гідності українську пісню «Пливе кача по Тисині». Але загалом ціль пісні – атакувати українських захисників «Азовсталі». Відео на пісню поєднує кадри боїв в Маріуполі на заводі «Азовсталь» у 2022 році з кадрами акцій протесту під час Революції Гідності у 2014 році.

Крім того, в Російській Федерації українські артисти, які підтримують Росію та/або не висловлюють свого ставлення, виступають і рекламують себе на телебаченні, радіо, концертах і фестивальних майданчиках. Водночас переслідувалися інші артисти української, російської та інших національностей, заборонялися їхні концерти, створювалися умови, що унеможливлювали творчу та комерційну діяльність у Російській Федерації [39].

Російська пропаганда залишається ефективною зброєю, особливо за межами України. Обсяги фінансування російської пропаганди в рази перевищують контрінформаційні проєкти західних країн. За даними Мінфіну РФ, з січня по березень 2022 року Росія виділила на фінансування державних ЗМІ 17,4 млрд рублів (з них 11,9 млрд рублів —використано під час бойових дій у березні). Це в 3,2 рази більше, ніж за аналогічний період минулого року. На європейському континенті, який зараз покладається на Кремль в енергетичних питаннях, Російська Федерація активно поширює егоїстичні зауваження та заяви на кшталт про те, що «санкції шкодять країнам, які їх запроваджують», про «надання Києву зброї для розпалювання війни», «боротьбу Росії за колективний Захід» тощо [50].

На основі дослідницьких джерел та літератури можна виділити п’ять груп факторів, які впливають на ефективність російської дезінформації: характер дезінформації; особливість комунікації в сучасному інформаційному просторі; вплив пандемії коронавірусу на канали зв'язку, особливості національного становища України, здійснення часткової інформаційної ізоляції на територіях, де ведуться бойові дії, та на окупованих територіях.

Висновок до розділу 1

Тому інформаційна війна є відносно новим явищем, яке трактується як форма інформаційного протиборства між державами з метою завдання шкоди та загрози інформаційному простору конкуруючих сторін. Інформаційна війна є синонімом військових дій, оскільки це жорстока та небезпечна діяльність. Дезінформація, пропаганда, кібератаки та руйнування інформаційних систем противника – все це методи інформаційної війни. Основною зброєю

інформаційної війни Росії є пропаганда та встановлення домінуючої позиції Росії в її первинних зонах впливу. Росія також активно використовувала кібератаки для зараження державних і неурядових систем комп'ютерними вірусами та ботами, причому лише за 10 місяців вторгнення було здійснено майже 3000 атак. Російські актори використовують безліч стратегій та різних тактик, щоб представити світову свої нікчемні наративи.

РОЗДІЛ 2. СТАН ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ В УМОВАХ ПОВНОМАСШТАБНОЇ АГРЕСІЇ РФ

2.1. Характеристика сучасного стану інформаційного простору України

Інформаційний простір – це територія, на якій за допомогою окремих компонентів інформаційно-комунікаційних систем поширюється інформація та здійснюється охоронювана законом інформаційна діяльність. До цих складових слід віднести: матеріальні (технологічні) можливості горизонтального та вертикального поширення інформації, поширення інформації в будь-якому напрямку, а також наявність регіональних та міждержавних домовленостей, заснованих на розумінні того, що жодна інформаційна обробка не може вважатися винятковим явищем національного характеру. Однак слід також зазначити, що сфера інформаційного впливу не обмежується національними кордонами, а закони, що регулюють функціонування інформаційного простору, не завжди підпадають під дію національного законодавства, особливо коли підпорядковуються актори та «творці» інформаційного дискурсу є іноземними або недержавними акторами [32].

Інформаційний простір позначає набір понять і відносин між ними, які підтримує інформаційна система, він описує діапазон можливих знань або значень, які сутність може мати за заданих правил і обставин. Інформаційні простори оточують нас. Простіше кажучи, коли ми отримуємо файл із комп’ютера, ми переглядаємо інформаційний простір; коли ми використовуємо пошукову систему, ми просіюємо інформаційний простір; і коли ми відвідуємо веб-сайт, ми переходимо через інший інформацій простір. Тобто, інформаційний простір відноситься до інформаційного набору, в якому учасники взаємодіють для виконання діяльності [74].

Характеристиками та ознаками інформаційного суспільства є:

- формування єдиного інформаційно-комунікаційного простору, повноцінної участі України в процесі інформаційно-економічної інтеграції регіонів, країн і народів у складі світового інформаційного простору;

- встановлення та подальше домінування позицій у перспективних галузях, таких як інформаційні технології, комп'ютерне обладнання та телекомунікації;
- зростання ролі інформаційної та комунікаційної інфраструктури у виробничих системах суспільства;
- підвищення рівня розвитку освіти, науки та культури шляхом розширення можливостей інформаційних систем на міжнародному, національному та регіональному рівнях;
- створення ефективних систем забезпечення прав громадян і соціальних інститутів на вільне отримання, поширення та використання інформації є найважливішою умовою розвитку демократії [43].

ЗМІ є важливою частиною інформаційного простору. Важливими факторами в цій сфері інформаційного простору є умови, в яких вони функціонують в країні, законодавче забезпечення та статус захисту журналістів. У країнах, що розвиваються, ЗМІ відіграють життєво важливу роль у всьому суспільстві, оскільки маніпулюють громадською думкою та поширюють неправдиву інформацію без правових обмежень, серйозно порушуючи національну інформаційну безпеку. У національних рамках інформаційний простір – це сукупність засобів масової інформації.

Національний інформаційний простір є потужним важелем національної безпеки та побудови сильної країни. Збігнєв Бжезінський сказав: «З соціально-економічної точки зору світ стає єдиним ігровим полем і все більше страждає від трьох динамічних реалій: глобалізації, «інтернетизації» та дерегуляції. Домінування». «Інтернетизація» або глобальний вплив інформаційного простору визначає вплив сучасних країн. У зв'язку з цим було визначено стратегічне завдання інформаційної політики України – це забезпечити перетворення України в інформаційну політику України та сприяти розвитку світової цивілізації. Це потребує ефективного управління різноманітними інформаційними ресурсами та елементами інформаційно-комунікаційної

інфраструктури, а держава підтримує розвиток інформаційного виробництва, інформаційних технологій, засобів, продуктів і послуг. Основою соціально-економічного, політичного розвитку та забезпечення безпеки та інтеграції України є інформаційний простір, який сучасні українські дослідники визначають як «сукупність інформаційних потоків із внутрішніх і зовнішніх джерел, наявних на території країни». Він складається з газет, електронних ЗМІ та інформаційних мереж [24].

Історично формування інформаційного простору залежало від держави. Тому в контексті нашої країни використовується категорія «Національний інформаційний простір України». Його легальне визначення таке: «Національний інформаційний простір України – це сфера (об'ємний простір) обробки інформації та функціонування юрисдикції України» [11].

У формуванні українського національного інформаційного простору, окрім традиційних ЗМІ, активну роль відіграють і новітні електронні ЗМІ сьогодення, найважливішими з яких, на думку сучасних дослідників, є:

1. Кабельне телебачення, яке з'єднує телевізори в певній місцевості (регіоні) з телевізорами, наданими центром передачі, через дротове з'єднання. Кабельне телебачення в основному використовується для передачі розважальних програм, але воно також може передавати суспільно-політичні передачі.
2. Відеомагнітофон — пристрій для запису та відтворення аудіовізуальних програм та інших новинних матеріалів. Їхня інформація поширюється переважно у вигляді стрічок культурно-розважального характеру, що не виключає поширення за допомогою цього ЗМІ всіх інших видів інформації.
3. Телефонна конференція (електричний міст, телефонна конференція тощо) – використання супутникових технологій для встановлення зв'язку між двома точками на землі, без обмежень відстанню чи географією, здійснення спілкування між групами людей, участь у обговоренні важливих соціальних питань , тощо [16].

Важливою ознакою суверенної та незалежної країни є формування єдиного інформаційного простору, яке спрямоване на зміцнення статусу країни, забезпечення інформаційного суверенітету, створення умов для захисту та ефективного використання національних інформаційних ресурсів. До основних характеристик українського інформаційного простору можна віднести:

- єдині принципи та загальні правила взаємодії всіх об'єктів інформаційної діяльності, а також формування національних інформаційних просторів у країнах, що розвиваються, та оптимальне співвідношення регуляторних і саморегулівних ініціатив;
- наявність умов для безпечного обміну інформацією між державами, організаціями та громадянами;
- рівний доступ суб’єктів інформаційної діяльності до відкритих інформаційних ресурсів та їх правова рівність;
- підтримання балансу інтересів національної та міжнародної спільноти та забезпечення національного інформаційного суверенітету України під час її входження у світовий інформаційний простір [15].

Український інформаційний простір є цілісною системою, яка в свою чергу складається з елементів, які взаємодіють між собою та між системами. Ці елементи є регіональним інформаційним простором, який умовно можна розділити на два модулі – прийнято називати західним і східним. Ці модулі складаються з регіональних інформаційних просторів. Вони характеризуються тим, що часто перебувають у конфліктних стосунках і не займають явного домінуючого положення в системі протягом значних періодів часу. Ще однією особливістю є явна залежність одного модуля від інформаційного простору іншої країни. Наприклад, сучасний інформаційний простір Донбасу та Криму можна вважати цілком залежним від російського інформаційного простору та суміжних елементів цих двох систем інформаційного простору. Інформаційний сектор України має стратегічне значення з точки зору економічної та інформаційної взаємодії. За відсутності явного домінування української інфосфери боротьба за домінування між її елементами, враховуючи чинники буферної зони між

країнами Заходу та Росією, визначає курс на необхідність української інфосфери. Домінуюча позиція третіх осіб в українському інформаційному середовищі очевидна [18].

Специфіка українського контексту вже давно сприяла ефективному засвоєнню кремлівського наративу перед повномасштабним вторгненням до Росії. По-перше, варто враховувати тривалу історію відносин і географічну близькість Росії та України. Зокрема, радянська пропаганда та наративи мали значний вплив на населення Донбасу, важливого промислового регіону. Протягом майже всієї історії Радянського Союзу активно пропагувався наратив про «єдину націю», плекалося почуття меншовартості, заперечувалося існування незалежної української мови, культури та держави. Кремлівський наратив давно перебуває під впливом не лише російських ЗМІ, ботів, інфлюенсерів тощо, а й українських акторів: Це «Партія регіонів» та її ідеологічна спадкоємиця «Програма життя опозиції»; такі знаменитості Віктора, як Медведчук, Ілля Кива, деякі українські «ЗМІ» (Шарія, Страна.ua та закриті «112 Україна», NewsOne», «НАШ») [2].

Основними політико-економічними аспектами створення єдиного інформаційного простору в Україні є подолання інформаційних монополій в управлінських і торгових структурах та прозорість інформаційних ресурсів. Лише тоді, коли інформаційний простір відкритий для суспільства, він може бути ефективним і може повноцінно та системно реалізовуватися спільні інтереси громадян, суспільства та країни. Створення та розвиток єдиного інформаційного простору України, особливо відповідних національних інформаційних ресурсів, є міжвідомчим і міжрегіональним питанням. Воно вимагає виконання складних організаційно-технічних завдань, які є дорогими і не можуть бути вирішені негайно [57].

Намагаючись протистояти російському інформаційному впливу, український уряд у 2014 році заблокував приблизно 14 російських телеканалів. У 2015 році Верховна Рада заборонила українським телеканалам транслювати російську пропаганду. У 2017 році під заборону потрапили найбільші російські соціальні мережі та інтернет-сервіси, зокрема ВК (ВКонтакте) і ОК

(Одноклассники), Яндекс, Mail.ru, а також російські медіакомпанії РБК, Рен-ТВ, ТНТ, НТВ Плюс, Звезда, Москва 24» і Russia Today. У березні 2021 року президент Володимир Зеленський заборонив вісім проросійських теле- та медіакомпаній, зокрема ZIK, NewsOne та 112 український телеканалів [51]. Вітчизняні іноземні експерти вважають ці ЗМІ антиукраїнськими. Прихильники свободи слова розкритикували поведінку Зеленського, але зворотній відлік подій 24 лютого 2022 року змусив усіх усвідомити правильність поведінки глави держави.

Щоб зрозуміти, що змінилося після 24 лютого 2022 року, необхідно подивитися на стан медіаринку раніше. Тенденції медіаринку України у 2021 році були такими:

- соціальні мережі та новинні веб-сайти замінили телебачення як основне джерело новин для українців, особливо для тих, хто молодше 35 років;
- зменшення аудиторії національних телерадіоканалів;
- зростання аудиторії національних друкованих ЗМІ, міжнародних веб-сайтів і регіональних веб-сайтів, хоча й у меншому масштабі;
- інтернет-сайти новин і програмне забезпечення для обміну миттєвими повідомленнями стають все більш важливими на місцевому рівні в усіх регіонах країни;
- медіаграмотність українців та здатність виявляти дезінформацію зросла, але впала довіра до російських ЗМІ [58].

Слід розуміти, що сьогодні жодне джерело не може чітко й переконливо донести повідомлення до всіх. Не варто забувати про розшарування української аудиторії. Це не просто різниця у віці, а й культурна і навіть психологічна різниця. Кожній групі потрібна своя форма для подання інформації. Хтось віддає перевагу збалансованим довгим текстам, а хтось задовольняється кількома реченнями з «емодзі». Особливо це розшарування проявляється в соціальних мережах. Наприклад, Facebook для тих, хто поважає довгі тексти, Telegram для тих, хто читає кілька речень, Instagram для тих, хто любить картинки, а текст взагалі неприйнятний у TikTok. Тобто мова йдеться про способи доставки однієї тієї

самої інформації до різних груп людей через різні платформи. Тобто, щоб донести те саме повідомлення до різних аудиторій, його потрібно представити в кількох різних форматах. Це досить складно, але це також характерно для сучасних інформаційних просторів [49].

Українське суспільство вже другий рік поспіль фактично залежить від новин. Інформація про авіаудари, обстріли, зміни ситуації на передовій та політика – все це стало частиною повсякденного життя багатьох українців. Проте за останні кілька років змінилися не лише звички споживання новин, а й сам інформаційний простір. Україна перебуває в активній фазі інформаційної війни, яка проявляється в розповсюдженні інформації та психологічних спецопераціях, дезінформаційних кампаніях, використанні автоматизованих облікових записів для впливу на громадську думку. Українська влада намагається швидко реагувати на ці виклики, але вдалася до монополізації інформаційного простору, що викликало недовіру в українському суспільстві. Найпопулярнішим джерелом для українців залишаються соціальні мережі, на другому місці – телебачення, на третьому – Інтернет [26].

Після 24 лютого 2022 року разом із відчайдушним героїзмом військових інформаційний простір наповнили історії мужності та людяності українських мирних жителів у надскладних умовах масової агресії та окупації. Ми пам’ятаємо, як мирні жителі голими руками блокували військову техніку окупантів, як окупанти ризикували своїм життям, щоб передати повідомлення нашим воїнам чи врятувати життя інших, як херсонці та енгодальці протестували перед озброєними росіянами.

У серпні 2022 року «Детектор медіа» провів вісім фокус-груп у Києві, Дніпрі, Одесі, Вінниці і Львові, щоб зрозуміти, як аудиторія сприйняла український медіа-простір після повної інвазії, зміни у споживанні медіапродукту, чутливість і ставлення до пропаганди тощо. Серед змін в українському медіа-просторі найчастіше в дискусіях згадували: перехід до формату інформаційного марафону «Єдині новини», «суттєве підвищення якості українського контенту – музичного, розважального, пізнавального та

пізнавального; Занепад російськомовного мовлення та занепад проросійських наративів у ЗМІ. Якщо брати до прикладу синдиковані телемарафони, то відгуки тут неоднаково позитивні. У дискусії зазначалося, що об'єднання телеканалів – це символічна та надихаюча подія, є також символом інформаційної стабільності, але є й негативна сторона, фактично єдиний офіційний погляд на подію транслювався під час марафону, інших думок не було, лише лояльні медіагрупи брали участь у телемарафоні, який раніше був у ЗМІ. Залучення ведучих, які просувають російські пропагандистські наративи в Інтернеті, також викликало обурення серед опитуваних.

Серед змін у вітчизняних ЗМІ з початку війни ті, хто брав участь у дискусії, також зазначили: збільшення патріотичного контенту, спрямованого на формування національної ідентичності; політизацію інформаційного простору; заборону критики дій влади; придушення соціально чутливої інформації [53]. Головним недоліком сьогоднішньої війни є контроль над інформаційним простором України. Цей контроль здійснюється через соціальний марафон та інші мережі. Бо на початку підйому Президента Володимира Зеленського За кілька років нова влада завдала найбільшого удару по контрольованому нею інформаційному простору, викликаючи паніку. Власне, через війну цю проблему вдалося вирішити, фінансуючи і контролюючи багато речей з державного бюджету. Тож після війни взяв під контроль медіапростір і знову отримав повну владу [33].

Після кожної відеопромови очільника Кремля, великих подій в українській армії чи розгрому «Другої великої армії», з українського боку з'являється безліч мемів на ці теми. Основна актуальність інформаційного опору полягає в його популярності, яка набула широкого поширення в Інтернет-просторі. Меми допомагають підняти моральний дух як серед цивільних, так і серед військових. Наприклад, мем «Могилізація» пов'язаний з промовою Володимира Путіна до російського народу про початок часткової мобілізації. Сама назва «Могилізація» пов'язана з використанням слова «мобілізація», що означає «смерть», а не «присягу служити країні». Рух «Весна» використав це слово в пості в Twitter із

закликом взяти участь у всеросійських акціях протесту, які проходять у всіх містах Росії. Так, на українських сторінках у соцмережах почали вживати це слово, створювати та поширювати меми на цю тему. Одна з них розроблена на основі тексту відео, на якому після «вибуху селітри» в Криму житель покинув район і сказав: «Я не хочу їхати з Криму, з Алушти, тут так круто». , відчуваю себе як вдома. Я звик до того, як люди живуть у моєму домі..." Сам рядок став інтернет-жартом. В одному з мемів є аналогія, слова прозвучали з вуст російського солдата, який був змушений воювати на території України, але не хотів залишати військову частину. Цей список можна продовжувати довго, щоб українці могли інформаційно-психологічно впливати на особовий склад російської армії, доводячи до розпачу їх стан і особистість. Використання мемів було потужним інструментом деморалізації ворога та підвищення морального духу українців під час опору [38].

Музика стала ще однією потужною зброєю повідомлення та жанром для вираження творчого натхнення українців, оскільки з давніх часів вона відігравала катарсисну роль, керувала битвами та допомагала впоратися з емоціями у найважчі часи. До створення нової музичної історії долучилися зірки естради, аматори і навіть наші захисники, воїни ЗСУ. Нині у найвіддаленіших куточках світу добре відома народна пісня Січового Стрілецтва відома в Радянському Союзі «Ой у лузі червона калина», з її виконання Андрієм Хливнюком на початку повномасштабного вторгнення. Пізніше у цій пісні також взяли участь відомі українські поп-співаки, які разом заспівали у флешмобі, додавши кожен свій голос. Мотиви підтримки президента України Володимира Зеленського все частіше зустрічаються в музиці. Автори пісень виражають вдячність і гордість за допомогою текстів і мелодій. Також очолює музичні чарти пісня-переможець щорічного пісенного конкурсу «Стефанія» Kalush Orchestra. Цей хіт, безсумнівно, підкорив серця багатьох українців, а також усіх європейців, які були готові долучитися, щоб надати пісні нових звукових форм. Крім того, «Стефанія» стала також символом вдячності війську за захист українців [28].

Військові фотографи виконують особливу місію під час війни, показуючи світові злочини проти людства та страждання, які шокують суспільство. «Погляньте, кажуть світлини, - як це виглядає. Це витвір війни. І ще це – воно теж витвір. Війна розриває, роздирає. Війна здирає, патрає. Війна випалює. Війна розчленовує. Війна руйнує». Сьогодні українські фотографи ризикують життям, аби задокументувати та показати світові реальність війни та злочини російських військових. Соціальна фотографія, світлини військових фотографів, візуальні сюжети про війну роблять військові злочини російської армії в Україні відомими всьому цивілізованому світу [27].

Отже, інформаційний простір – це все що оточує нас. Важливим елементом інформаційного простору – є засоби масової інформації, кабельне телебачення, відеомагнітофони, газети. Тобто, все те що ми використовуємо у повсякденному житті, звідки ми можемо черпати інформацію.

2.2. Правове забезпечення інформаційної безпеки України.

Інформаційна безпека охоплює інструменти та процеси, які організації використовують для захисту інформації. Це включає параметри політики, які запобігають доступу неавторизованих осіб до ділової чи особистої інформації. Інформаційна безпека захищає конфіденційну інформацію від несанкціонованих дій, включаючи перевірку, модифікацію, записування та будь-яке порушення чи знищення. Мета полягає в тому, щоб забезпечити безпеку та конфіденційність важливих даних, таких як деталі облікових записів клієнтів, фінансові дані чи інтелектуальна власність.

Основними принципами інформаційної безпеки є конфіденційність, цілісність і доступність. Кожен елемент програми інформаційної безпеки повинен бути розроблений для реалізації одного або кількох із цих принципів. Разом вони називаються тріадою ЦРУ. Метою принципу конфіденційності є збереження конфіденційної інформації особистої інформації та забезпечення її видимості та доступу лише для тих осіб, які нею володіють або потребують її для виконання своїх організаційних функцій. Принцип цілісності гарантує, що дані є точними та надійними та не змінюються неправильно, випадково чи зловмисно.

Мета доступності – зробити технологічну інфраструктуру, програми та дані доступними, коли вони потрібні для організаційного процесу або для клієнтів організації [73].

У той час як тріада ЦРУ формує основу політики інформаційної безпеки та прийняття рішень, до повного плану інформаційної безпеки слід додати інші фактори, в тому числі наступні:

- Управління ризиками. Метою тут є максимізація позитивних результатів і мінімізація негативних. Організації використовують принципи управління ризиками, щоб визначити рівень ризику, який вони готові взяти на себе під час виконання системи.
- Класифікація даних. Використовується для того, щоб приділити додаткову увагу інформації, яка повинна залишатися або дуже конфіденційною, або даним, які повинні залишатися легкодоступними.
- ЗМІ та угоди про конфіденційність. Повна політика захисту інформації охоплює фізичну інформацію, друковану інформацію та інші види носіїв.
- Навчання користувачів. Необхідне для того, щоб обмежити ризик того, що аналітик бухгалтерського обліку змінить фінансові дані, організація може запровадити технічний контроль, який обмежує права на зміни та реєструє зміни.
- Безперервність роботи та аварійне відновлення. Дані мають залишатися доступними та незмінними у разі збою програмного чи апаратного забезпечення. Організації можуть досягти цього за допомогою резервних копій або резервних систем [88].

Інформаційна безпека відіграє ключову роль саме під час військових дій та конфліктів. Адже некоректна та неправдива інформація може викликати паніку в суспільстві, вплинути на хід подій, призвести до внутрішнього переміщення людей, погіршити імідж політичних лідерів, створити негативний вплив на політиків та їхні заяви та заклики, які можуть негативно вплинути на бойові дії

та посилити фізичний і психічний вплив на людей. Шкода здоров'ю може також завдати непоправної шкоди загальним результатам бойових дій. Тому запобігання поширенню такої викривленої інформації у військових конфліктах має велике значення для всього процесу військового конфлікту.

Створення сучасної системи забезпечення інформаційної безпеки в Україні розпочалося ще зі створенням у 1992 році Ради національної безпеки України та прийняттям Закону України «Про інформацію», який закріпив основні принципи інформаційного суверенітету України. Перший етап можна охарактеризувати як етап становлення нової системи державного управління незалежними секторами українського інформаційного простору. Цей період тривав шість років, це була не лише спроба органу управління національним інформаційним полем, але й національний інформаційний простір набув нового вигляду. Другий етап характеризується принциповою зміною розуміння поняття «інформаційна безпека», яке набуває надзвичайного значення. На той час найважливішим етапом становлення та розвитку інформаційних систем став третій етап закону України «Про Концепцію державної програми інформатизації». Прийняті в цей період теоретичні та концептуальні документи свідчать про те, що «інформаційна безпека» надовго і серйозно витіснила один із пріоритетних напрямків державного управління національною безпекою. Прийнято Стратегію національної безпеки України, яка уточнює ключові завдання національної політики у сфері інформаційної безпеки. Четвертий етап характеризується вирішенням важливих стратегічних питань національної політики забезпечення інформаційної безпеки в умовах інформаційно-психологічного протистояння і є абсолютно новою віхою в історії інформаційної безпеки України. [1].

Інформаційна інфраструктура є одним із основних змістів реалізації національної інформаційної політики та невід’ємною частиною стратегічних інформаційних ресурсів, має велике значення для обороноздатності країни та інформаційного ринку. Відповідно до Закону України «Про Концепцію Національної програми інформатизації» інформаційна інфраструктура включає: міжнародні та міжміські телекомунікаційні та комп’ютерні мережі; системи

інформаційно-аналітичних центрів; інформатизацію; виробництво та супровід інформаційних технологій; систему підготовки кваліфікованих кадрів, талантів у сфері інформаційних технологій [44].

Зростаюча оцифровка послуг і залежність від Інтернету призвели до еволюції кіберпростору, а також створили серйозні виклики безпеці для урядів у всьому світі з точки зору злочинів проти комп'ютерних систем і через них. В Україні це найбільш яскраво продемонструвала масова кібератака на українські енергетичні компанії в грудні 2015 року після атаки на головний телеканал України в день місцевих виборів двома місяцями раніше. Вплив цих атак може бути значним, оскільки вони можуть пошкодити критичну інфраструктуру та перешкодити ефективній роботі та функціонуванню національних органів влади. Метою інформаційної та психологічної війни є дискредитація державної влади та створення умов для дестабілізації суспільно-політичної ситуації.

Щоб подолати ці виклики Україна прийняла Указом Президента свою Національну стратегію кібербезпеки від 15 лютого 2016 року. Основна увага Стратегії зосереджена на трьох напрямках: розвиток національної системи кібербезпеки; розширення можливостей у секторі безпеки та оборони; забезпечення кібербезпеки критичної інформаційної інфраструктури та державних інформаційних ресурсів [66].

Варто також зазначити, що з метою захисту національного інформаційного простору 14 січня 2015 року Кабінет Міністрів України ухвалив про створення Міністерства інформаційної політики України, першочерговим завданням якого є протидія з боку Російської Федерації; розробка ефективної національної стратегії інформаційної політики держави та Концепції інформаційної безпеки України; узгодженість та координація операцій і діяльності органів державної влади в інформаційній сфері. З метою протидії негативним наслідкам інформаційної пропаганди та ведення інформаційної війни, усунення та запобігання реальним і потенційним загрозам в інформаційному просторі України, Рада національної безпеки і оборони України прийняла рішення «Про

заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [13].

Доктриною інформаційної безпеки України, затвердженою Указом Президента України від 29 грудня 2016 року «Про рішення Ради національної безпеки і оборони України» «Про Доктрину інформаційної безпеки України», покладено функції абезпечення інформаційної безпеки на такі органи, як Рада національної безпеки і оборони України, Кабінет Міністрів України, Міністерство закордонних справ України, Міністерство оборони України, Міністерство культури України, Державна рада телебачення і радіомовлення, Державний комітет України з питань телебачення і радіомовлення, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації [41].

Об'єктами захисту законодавства України про інформаційну безпеку є: людина і громадянин – конституційні права і свободи, фізичне і психічне здоров'я, свобода від негативного впливу інформаційних технологій та інформації; суспільство і держава – захист своїх законних інтересів у сфері інформації; інформаційні ресурси та інформаційна інфраструктура – її цілісність, доступність та безпека. Теорія інформаційної безпеки в Україні лише визначає та змістовно відповідає національним інтересам в інформаційній сфері. Згідно з її аналізом, національні інтереси України в інформаційній сфері можна поділити на чотири основні складові:

1. Дотримуватись конституційних прав і свобод людини і громадянина щодо доступу до інформації та її використання, забезпечувати духовне відродження України, зберігати та зміцнювати науковий потенціал країни у сфері соціально-моральних цінностей, патріотизму, гуманізму, культури та культурні традиції.
2. Інформувати про державну політику України, надавати громадянам України та міжнародній громадськості достовірну інформацію про державну політику України, її офіційну позицію щодо суспільно

значущих подій національного та міжнародного життя, надавати громадянам доступ до відкритих державних інформаційних ресурсів.

3. Розвиток сучасних інформаційних технологій, вітчизняної інформаційної індустрії, включаючи інформатизацію, телекомунікації та галузі зв'язку, забезпечує попит внутрішнього ринку на свою продукцію та експорт цієї продукції на світовий ринок, а також: накопичення, зберігання та використання вітчизняних інформаційних ресурсів.
4. Захист інформаційних ресурсів від технічної розвідки та несанкціонованого доступу та забезпечення безпеки інформаційно-телекомунікаційних систем [7].

Крім того, в доктрині інформаційної безпеки України зазначено, що сучасна складність загроз національній безпеці в інформаційній сфері вимагає визнання інноваційних підходів до формування систем захисту та розвитку інформаційного простору в умовах глобалізації та свободи. Інформаційний потік. Це вимагає від національних спецслужб розробки нових методів науково-технічного забезпечення контррозвідувальної діяльності у світовому інформаційному просторі, зокрема розробки нових зразків спеціальної техніки, спеціальних методів і методів моніторингу вітчизняних та іноземних ЗМІ та мережі Інтернет. З метою оперативного виявлення, запобігання та усунення загроз національній безпеці України в інформаційній сфері [23].

Вирішальною складовою інформаційної безпеки є її правова складова, яка включає наявність системи правових норм та гарантії її ефективності при виконанні функцій держави у сфері інформаційної діяльності: нагляду та захисту. Як видно, суб'єкт закону про інформаційну безпеку складається із сукупності суспільних відносин, пов'язаних з інформацією, інформаційною діяльністю, інформаційною інфраструктурою та правовим статусом суб'єктів інформаційної сфери, які є об'єктами національного інтересу, і відображається формою інформаційної безпеки. Безпека цих об'єктів знаходиться під загрозою. Правові положення національної інформаційної безпеки є невід'ємною частиною

основного корпусу інформаційного права, особливо невід'ємною частиною адміністративного прав [21].

15 жовтня 2021 року Кабмін затвердив Стратегію інформаційної безпеки. Її метою є створення умов для забезпечення інформаційної безпеки в Україні, з метою захисту життєво важливих інтересів громадян, суспільства та країни від внутрішніх і зовнішніх загроз, забезпечення захисту національного суверенітету та територіальної цілісності України, підтримання соціальної та політичної стабільності, національної оборони, забезпечення захисту прав і свобод кожного громадянина. Реалізацію Стратегії планують до 2025 року. Бажаним результатом реалізації цієї Стратегії є забезпечення безпечного інформаційного простору в Україні. Проте, відповідний розділ стратегії містить лише загальне визначення бажаного стану під час реалізації Стратегії. Описуючи більш детально стан справ сфери інформаційної безпеки, окремі кількісні та якісні показники можуть краще пролити світло питання, як виміряти ефективність реалізації цієї Стратегії [45].

Цим задекларованим документом визначено сім важливих перспективних цілей інформаційної безпеки. Перша передбачає протидію дезінформації та інформаційним операціям, спрямованої проти України, насамперед державою-агресором. Друга – забезпечення всебічного розвитку української культури та утвердження українського громадянства. Третя – підвищення культури соціальних медіа та медіаграмотності суспільства. Четверта – забезпечення дотримання прав особи на збір, зберігання, використання і поширення інформації, права на свободу вираження своїх поглядів і переконань, права на захист приватного життя, права на отримання об'єктивної та достовірної інформації, а також забезпечення захисту прав журналістів. П'ята – інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на суміжних до них територіях України, інформаційного простору всієї України. Шоста – розвивається інформаційне суспільство та підвищується рівень культури діалогу. Сьома мета – створити ефективну систему стратегічних комунікацій. Тобто зазначені цілі становлять сфери, що потребують посиленого

державного контролю та є визначальними в контексті забезпечення інформаційної безпеки [52].

У Стратегії подолання глобальних викликів і загроз інформаційній безпеці вказано, що у всьому світі зросла кількість дезінформаційної активності, інформаційна політика Російської Федерації, соціальні мережі як головні суб'єкти впливу в інформаційному просторі та недостатній рівень грамотності соціальних медіа серед суспільства, що сприяють виникненню всіх проблем інформаційної безпеки. Серед загальнодержавних — інформаційний вплив Росії на українців як агресора, інформаційне домінування Російської Федерації на тимчасово окупованих територіях України, обмежені можливості реагування на дезінформаційну діяльність та недосконале регулювання відносин щодо захисту професійної діяльності журналістів, намагання маніпулювати обізнаністю громадян щодо європейської та євроатлантичної інтеграції України та низький рівень доступу до інформації через Інтернет на локальному рівні.

У Стратегії є деякі визначення, які відіграють ключову роль у забезпеченні інформаційної безпеки під час активної бойової фази:

1) Інформаційні заходи національної оборони – комплекс скоординованих заходів, які готуються та здійснюються суб'єктами національної безпеки і оборони України в мирний час, в особливий період, в умовах воєнного або надзвичайного стану щодо передбачення та виявлення інформаційних загроз.
2) Стратегічні наративи – це тексти, які спеціально використовуються для усної презентації в процесі стратегічної комунікації з метою інформаційного впливу на цільову аудиторію.
3) Урядова комунікація – низка заходів, що передбачають діалог між уповноваженими представниками Кабінету Міністрів України та цільовими аудиторіями для роз'яснення позиції та/або політики уряду з певних спірних питань [52].

Виходячи із умов стратегії, відчувається підготовка до ескалації конфлікту та відповідні плани діалогу з громадянами та світовими лідерами.

Якщо порівнювати Доктрину і Стратегію, то хоча зміст схожий, між ними є значні відмінності. Якщо Доктрина спрямована насамперед на відсіч агресії Російської Федерації, то Стратегія – це проєкт загальної перебудови українського інформаційного простору, стратегією розвитку всіх інформаційних відносин. Заходи стратегії протидії інформаційному впливу агресора є лише частиною запланованих операцій і особливо не висвітлюються. Крім того, на відміну від цієї доктрини, термін дії цієї стратегії не обмежується надзвичайними ситуаціями, пов'язаними з гібридною війною, і не передбачає припинення її реалізації після припинення агресії Російської Федерації. При цьому стратегія була представлена не як план Кабінету Міністрів чи документ Верховної Ради України, а як рішення РНБО [37].

Основним Закон України «Про національну безпеку України» визначено такі загрози національним інтересам України та національній безпеці України в інформаційній сфері: прояви обмеження свободи вираження поглядів і доступу громадян до інформації; пропаганда насильства, жорстокості, порнографічних матеріалів через засоби масової інформації; комп'ютерна злочинність і комп'ютерний тероризм; розголошення інформації, що є власністю держави або необхідної для забезпечення національних інтересів суспільства і країни; спроби маніпулювання суспільною свідомістю. До основних загроз інформаційній безпеці з боку державної політики України належать: монополія українського інформаційного ринку та окремих його секторів вітчизняними та іноземними інформаційними структурами; перешкоджання діяльності державних ЗМІ щодо інформування української та закордонної аудиторій; відсутність кваліфікованих кадрів, відсутність формування та впровадження системи державної інформаційної політики, неефективне інформаційне забезпечення української національної політики.

Прикладами загроз інформаційній безпеці України, є, зокрема, незаконна приватизація державних видавництв і друкарень, самовільний розподіл радіочастот тощо. Найбільше вражає те, що одна з основних загроз інформаційній безпеці лежить у сфері діяльності органів державної влади:

невиконання або неналежне виконання органами державної влади своїх повноважень в інформаційній сфері. Хоча, згідно з Конституцією України «забезпечення інформаційної безпеки є однією з найважливіших функцій держави і справою всього народу України» [44].

19 березня 2022 року Володимир Зеленський підписав три документи: «Рішення РНБО «Про реалізацію єдиної інформаційної політики…» та РНБО «Про усунення загроз національній інформаційній безпеці» Також РНБО ухвалив рішення "про призупинення діяльності окремих політичних партій", яке передбачало заборону 11 політичних партій, у тому числі "Опозиційної довічної платформи" та "Партії шаріату". Єдина інформаційна політика в умовах війни стосується об'єднання національних каналів (такими вважаються 29 інформаційних каналів з цифровим мовленням) та трансляції цілодобового марафону «Єдині новини #UAразом, який регулює Національна комісія з питань телебачення і радіомовлення За результатами підписання другого документу для забезпечення безперервності мовлення було націоналізовано телевізійну мережу ТОВ «Зеонбуд». Ці рішення дозволяють поширювати український наратив і впроваджувати політику єдиного голосу, а також полегшують комунікацію між операторами цифрового телебачення та державними органами. Підписання третього документу викликало спротив проросійських партій: «Опозиційна платформа – За життя» відреагувала на рішення РНБО, заявивши «всі звинувачення на адресу нашої партії сфабриковані владою, щоб виправдати свої неадекватні дії [2].

Тож, інформаційна безпека є важливим елементом під час ведення військових дій. Інформаційна безпека спрямована на захист життєво важливих інтересів суспільства та держави.

Висновок до розділу 2

Отож, інформаційний простір характеризується набором деталей, які використовуються для поширення інформації та комунікації. Інформаційний простір України формується за допомогою засобів масової інформації, кабельного телебачення, відеомагнітофонів, друкованих видань, конференцій,

зустрічей тощо. Після 24 лютого завдяки телемарафону «Єдині новини» український інформаційний простір суттєво змінився, збільшилась кількість україномовного контенту, зменшилось використання російськомовного мовлення, а також ми спостерігаємо більше патріотичного контенту. Зростання залежності від Інтернету вимагає захисту інформаційного сектора. Саме тому в Україні активно розвиваються законодавчі інформаційного сектора. У 2016 році було прийнято «Указ про інформаційну безпеку України», а в 2021 році — «Стратегію інформаційної безпеки України», спрямовану на створення умов для забезпечення інформаційної безпеки України та захисту життєво важливих інтересів громадян.

РОЗДІЛ 3. ДІЯЛЬНІСТЬ УКРАЇНИ ЩОДО ПРОТИДІЇ ІНФОРМАЦІЙНИМ ВПЛИВАМ РФ

3.1. Інформаційний фронт в Україні: проблеми та перспективи

Як зазначалося раніше, паралельно з військовим фронтом Збройних Сил України у виконанні своїх конституційних обов'язків відкрився також інформаційний фронт, і його військо, оснащене багатим інструментарієм у медіа-сфері, розпочало масштабні крос-медійні зусилля для виробництва фільми на тему єдності змісту ідентичності, що об'єднує багатьох діячів культури, експертів креативної індустрії та аматорів України, які готові використати свою художню та журналістську силу, щоб протистояти війні.

Робота інформаційного фронту, у рамках якого народжувалась нова айдентика єдиного бренду України, була зумовлена низкою причин, які стали рушійною силою для його функціонування в нинішньому стані. Ще однією, чому інформаційний фронт розпочав свою потужну роботу, стала необхідність донести до міжнародної спільноти, організацій та політичних сил правду про події, які відбувалися на території України. Тобто, головним каталізатором на фронті стала трагічна подія в усій України та світі – збройне вторгнення Російської Федерації [28]. Неуспіх України в перші місяці гібридної війни стався передусім через інформаційні провали.

У сьогоднішній ситуації інформаційний фронт є одним із вирішальних факторів перемоги України. Можна сказати, що інформаційний фронт складається з серії інформаційно-технічних і психологічних впливів і протидії, спрямованих на зміну стану масової та індивідуальної свідомості, а саме:

- інформаційна робота для керівництва української держави, органів місцевого самоврядування, громадських і політичних діячів;
- інформаційно-дипломатичний фронт;
- інформаційно-психологічні спецоперації; інформаційно-просвітницькі кампанії;
- кампанії по боротьбі з дезінформацією та підробкою інформації;

- інтернет-ЗМІ, ютуб-канали, виступи експертів та їх висновки з коментарями.

Сергій Корсунський зазначив, що об'єктивні дані показали, що Україна виграла перший раунд інформаційного протистояння в 50-денній війні. Відкритість і високий професіоналізм в інформаційній діяльності Офісу Президента, Міністерства оборони, Міністерства закордонних справ та журналістських організацій України, готовність і вміння відстоювати свою позицію у світових ЗМІ, активна праця в соціальних мережах – усе це в українському «меню» виявилося значно «смачнішим», ніж нескінченна й відверта брехня кремлівської братії демагогів і пропагандистів [20].

Український медіа-простір є вразливим до російської інформаційної війни з таких причин:

1. В Україні поява нових електронних ресурсів є неконтрольованою. Тому чи не щодня з'являються нові інтернет-медіа, спрямованість яких часто характеризується антиукраїнською пропагандою.
2. Вільне і досить агресивне проникнення в супутникові медіа, соціальні мережі та рекламні матеріали електронною поштою.
3. Україна не повністю захищена від вірусів і шкідливих програм, що поширювали російські хакери.
4. На відміну від України, в Росії було багато різних розробок, спрямованих на пропаганду та маніпулювання свідомістю.
5. Недостатньою була підготовка фахівців до ведення інформаційної війни в ЗМІ. Українські вищі навчальні заклади не готували фахівців з кіберзахисту.
6. Була відсутня джерельна база, що надавала інформацію про стратегію і тактику інформаційної війни [57].

Варто зазначити, що багато проблем в інформації виникають через незнання користувачами основ кібербезпеки, недотримання встановлених норм поведінки в кіберпросторі та відсутність спеціально підготовленого персоналу на національному та місцевому рівнях, здатних ефективно вирішувати ці проблеми.

Значною мірою проблема підривного використання інтернет-ресурсів пов'язана із невизначеністю правового статусу інтернет-ЗМІ в Україні та обмеженими можливостями України впливати на ті інформаційні об'єкти, що діють на території інших країн [25].

Три ознаки нинішньої епохи в Україні – явне обмеження свободи слова, деукраїнізація масової інформації та поширення в ній порожнечі. Майже кожен українець відчув на собі руйнівні наслідки. Український інформаційний простір перебуває у духовній і змістовній кризі. Інформаційна сфера країни є другорядною. Вона перебуває в умовах комерційної, духовної та культурної залежності, передусім від інформаційної політики російського уряду та спільних постімперських та постколоніальних смаків українського та російського режимів. Несвобода, зовнішня залежність інформаційного простору, другосортність продукції та смислова порожнеча є головними загрозами суспільному розвитку та національній безпеці. Бази для розвитку якісного медійного середовища просто немає. Складна професійно-етична ситуація в журналістиці. Суспільство має добре усвідомлювати, що серед журналістів по всій Україні є ті, хто не вміє йти на внутрішні компроміси, доносити людям об'єктивну інформацію, захищати вільний простір. Однак це середовище не існує у вакуумі й уражене тими ж хронічними захворюваннями, що й політика, бізнес і суспільство в цілому [42].

Аналізуючи новинну динаміку українських медіа, можна виявити, що часто нейтральні чи навіть принципово позитивні новини набувають негативного відтінку через маніпулятивність назви матеріалу. Але, як відомо, багато людей взагалі не читають «текст» новин, а лише заголовки. Ці лінгвістичні спекуляції спотворюють український інформаційний простір і негативно впливають на психологічний стан суспільства в умовах воєнного стану.

Ми всі були свідками «ефекту Арестовича» на початку війни, коли суспільству було вкрай важливо почути позитивні новини, зрозуміти, що війна — це не кінець, її треба вести і вигравати, а через «два чи через три тижні» все б закінчилося. Тож місце Арестовича зайняло багато ворожок і екстрасенсів, які

розпускають в інформаційному просторі купу сміття. Унікальним для цих матеріалів є гучна назва, яка містить емоційно насичені слова, і часто обіцяють це або повна перемога, або повна зрада. Інколи замість того, щоб збалансувати чутливий вміст, ЗМІ навпаки розпалювали паніку в ситуаціях, яких можна було уникнути. Так, наприклад, була новина про те, що рашисти зібрали 100-тисячне військо в напрямку Куп'янська, і що окупанти зайняли Запорізьку АЕС тощо Усе це лякає суспільство [34].

На жаль, влада не любить детально розповідати про ті чи інші поразки (як буває на будь-якій війні), але через цю тишу глядачі все частіше звертаються до російських джерел. Звісно, глядачі їх слухали, коли про евакуацію з «Азовсталі» ледве заговорили, а росіяни при цьому активно коментували цю тему та погрожували нашим захисникам смертю – бо це було страшно, і люди вірили. Коли російські пропагандисти знову говорять про «окупацію Києва», мало хто сприймає це серйозно. Але коли вони говорять про окупацію Донбасу, а ми бачимо, що вони фактично захоплюють нові населені пункти, зростає песимізм і зростає рівень довіри до джерел пропаганди, як би сюрреалістично це не звучало. Все це відбувається через суперечливі повідомлення із Заходу, який не надав нам необхідної підтримки – або ми цього не знаємо. Журналісти люди і теж втомлюються. Іноді вони створюють кваліфіковану державну зраду там, де її ще немає – наприклад, заява Джозефа Байдена про те, що Сполучені Штати не будуть надавати Україні ракети великої дальності. Але мова не йшла про те, що нам не дадуть комплекси для цих ракет – а певно, ракети на 300 км нам зараз не дуже потрібні [40].

Особливе занепокоєння в інформаційній стратегії Києва викликає відсутність ефективної комунікації влади та суспільства. Українські аналітики часто наголошують на тому, що, окрім плачевних заяв провідних політиків, немає чіткої інформації про плани чи навіть умови прийняття конкретних рішень, особливо інформації, яка є надзвичайно важливою для різних соціальних груп. Ця комунікаційна прогалина заповнюється різними спекуляціями та вставками

інформації з російських чи проросійських ЗМІ. Інше питання – якість української журналістики.

Одним із головних недоліків є все ще поширене незнання іноземних мов (що унеможливлює пряме використання іноземних джерел і спричиняє фундаментальні недоліки в інтерпретації європейських подій) та недотримання західних стандартів при підготовці матеріалів для преси (плагіат і порушення авторських прав), що впливає на якість повідомлення і, як наслідок, на довіру до окремих ЗМІ. Особливо це помітно, коли йдеться про висловлювання іноземних політиків про Україну чи Росію, які мають найбільший резонанс в українському суспільстві [79].

У ситуації, коли інформаційний фронт так само важливий, як і військовий, у липні 2023 року Національна спілка журналістів оприлюднила звернення до Президента, Уряду та керівництва «Укрпошти» щодо вирішення критичного стану розсилок української преси у воєнний час. Масові звільнення працівників пошти по всій країні призупинило доставку газет, залишивши українців без життєво важливої інформації. Газети, які мають як свою столітню історію, так і створені вже в часи Незалежної України, опинилися на межі банкрутства та закриття. У НСЖУ наголосили, що газети опинилися на межі банкрутства через скорочення листонош, закриття відділів передплати райбюро, поштових відділень та бюрократичні процедури. Витрати на доставку продовжують зростати і досягають 30% від усього редакційного бюджету. Водночас постійне скорочення штату «Укрпошти» вкрай негативно позначилося на своєчасній доставці газети до передплатників [17].

Експерти також відзначили основні моменти, на які варто звернути увагу, висвітлюючи події, які зараз відбуваються в нашій країні. Є дві головні помилки – світ звик дивитися на Україну і весь регіон через російську призму. Це триває багато років, ще з радянських часів. Світ бачить у цьому регіоні Росію — потужну константу — і щось у ній незрозуміле. Зараз усе змінюється, і ми голосно заявляємо про себе світові. Але іншу частину помилки можна назвати «хибною об’єктивністю». Доступ до інформації у цій війні дуже нерівний – з

українського боку журналісти мають досить широкий доступ, а з російського – лише державна пропаганда. І, оскільки світові ЗМІ звикли повідомляти про обидві сторони, вони часто розповідають про те, що бачили на власні очі в Україні, і нібито «для балансу» подають у матеріалі так звану другу сторону – тобто вони цитують російську пропаганду. Так виникає дуже небезпечне спотворення, коли доведений факт фактично дорівнює пропагандистській вигадці [35].

Андрій Кокотюха у своїй статті «Успіхи та помилки інформаційного фронту» гарно пояснює помилки та проблеми інформаційного простору в розпал війни. Наприклад, у перші дні війни у спільному телемарафоні виступали люди «які ще вчора» мали проросійську позицію. Народний депутат Максим Бужанський – одна з таких фігур. Ще за два тижні до того, як перші російські бомби впали на українські міста, він боровся за право проросійської пропаганди на існування. У перший день російського вторгнення телеграм-канал Максима Бужанського потрапив до списку розповсюджувачів російської дезінформації. Але тепер Максим Бужанський повернув свій проросійський корабель на сто вісімдесят градусів і засудив агресію Росії у прямому ефірі єдиного телемарафону [19].

Наступна помилка – безпідставна героїзація окремих росіян. Про відповідальність кожного росіянина за російську агресію писали не раз і будуть писати. У перші дні війни росіяни зробили багато звернень, як індивідуальних, так і колективних. По суті, це еквівалентно так званій «трубі Ахметова»: тобто в 2014 році олігархічні компанії засурмили в «протестний ріг» в окремо визначену дату та час на знак протесту. Ще один баг, який згадує Андрій, — це поява так званих VIP-жертв. Жителі Маріуполя, Чернігова, Ірпеня, Возеля та Бучі навряд чи зрозуміють, чому ЗМІ останнім часом висвітлюють окремих жертв. Мова йде про відомих українців, чиї будинки постраждали від російських обстрілів. Зокрема, яке відношення має вибух у Маріупольському пологовому будинку до пошкоджених будинків продюсерів Ігоря Кондратюка, Юрія Фаліози та багатьох

інших. Чому всі ці історії важливіші за десятки подібних трагедій? Війна для всіх однакова, біда для всіх однакова [19].

Як уже згадувалось, в арсеналі інформаційної війни українського президента є виступи, орієнтовані на вітчизняну аудиторію. Експерти зазначали, що київські чиновники використовують виступ глави держави як один із ефективних інструментів дипломатичного впливу на колективний Захід. При цьому спілкування керівників області і міста все ще залишається на рівні популістської риторики, такого собі робочого «візиту», метою якого є не інформаційний супровід роботи, не інформаційна контратака ворожій інформації, а рекламування своєї діяльності, перенасичення інформацією про особисті досягнення та нехтування основними складовими інформаційної гігієни. На жаль, популізм і недосвідченість – це сучасний тренд. Актуалізується також питання проведення ефективних комунікаційних кампаній та необхідність розробки відповідних інформаційних стратегій і тактик на національному рівні.

У цьому контексті ефективна стратегія боротьби української влади та суспільства з інформаційною агресією має містити такі основні напрями:

1) створити власний конструктивний міфологічний формат дизайну в Україні. На практиці це означає створення власних конструкцій, наративів, світоглядних і ціннісних установок, пов’язаних із західною цивілізацією та роллю України в європейській політиці та історичному дизайні, формування нової національної ідентичності у форміукраїнської історії, української музики, українського кіно тощо;
2) ігнорувати інформаційні теракти російських ЗМІ, а натомість здійснювати власні атаки на інформаційний простір противника та створювати з нього історичні конструкції, які призведуть до деміфологізації історичної спадщини агресора та не дозволять йому монополізувати інформаційний простір України;
3) російському пропагандистському наступу можна успішно протистояти, якщо створити реальну основу, що пояснює історичні та політичні події, експертні думки, лідерів думок, відомих представників сучасного

українського шоу-бізнесу. У результаті всі спроби російської монотонної пропаганди повинні бути зневажені;

4) розробити ефективні моделі культурної та інформаційної протидії, особливо у формі системних асиметричних атак з використанням методів і технік, а також ментальних і психологічних заходів протидії [29].

Основним політико-економічним аспектом створення єдиного інформаційного простору в Україні є знищення інформаційних монополій в управлінських і торговельних структур та прозорість інформаційних ресурсів. Загальновідомо, що інформаційні монополії є розсадником бюрократії, волюнтаризму та корупції. Лише відкритий для суспільства інформаційний фронт може бути ефективним і комплексно та системно досягати спільних інтересів громадян, суспільства та країни.

Ефективний інформаційний простір можна створити та почати розвивати відповідно до відповідної національної інформаційної політики, що забезпечить поступовий рух країни до побудови інформаційного суспільства. Цей рух має базуватися на новітніх інформаційних, комп'ютерних, телекомунікаційних технологіях. Їх розвиток відкриває інформаційні мережі, особливо інтернет, надаючи принципово нові можливості для міжнародного обміну інформацією. Майбутні інформаційні й телекомунікаційні технології посилюють вплив ЗМІ на суспільне, політичне та культурне життя людей.

Варто зазначити, що формування та розвиток українського інформаційного політичного простору відбувається у дуже складних умовах. Сьогодні Україна запустила процес прискорення євроінтеграції. Однак, Європейський інформаційний простір має багато характеристик, що висувають більш жорсткі вимоги до якості та безпеки інформаційних продуктів. Попутним питанням є можливість входження української інформаційної продукції в європейські інформаційні ресурси. Розглядаючи інформаційну безпеку як елемент європейського інформаційного простору, ця категорія охоплює два основних напрямки – кібербезпека та захист інтелектуальної власності.

У безпекових, економічних, соціальних та інформаційних цілях Україна потребує якнайшвидшої інтеграції в інформаційний простір ЄС, оскільки в умовах війни з Російською Федерацією та інформаційно-психологічних операцій проти українців існує велика потреба в достовірній та неспотвореній інформації, яка має бути інтегрована в спільний інфопростор, боротися з маніпуляціями та замовними оприлюдненнями інформації на національному та міжнародному рівнях, а також інформувати Європу та світ про проблеми та досягнення України [56].

Доцільно розглянути перспективи, що виступають рушійною силою ефективного розвитку інформаційного суспільства:

- швидкий розвиток інформаційно-комунікаційних технологій;
- надати великій кількості людей можливість підключатися до високошвидкісних мереж і користуватися додатковими сервісами;
- зниження цін на послуги, пов’язані з інформаційно-комунікаційними технологіями;
- посилення конкуренції на ринку інформаційно-комунікаційних послуг; удосконалення та приведення нормативно-правової бази до міжнародних стандартів багатьох країн [3].

Експерти вважають, що Україні варто контратакувати в інформаційному полі. По-перше, створити власний контент. По-друге, боротися з новою концепцією, яка починає опановувати західні уми про іншу Росію і добрих росіян, бо ця тема для нас «шкідлива».

3.2. Значення інформаційного фронту в протистоянні агресору

Звісно, ми багато зробили з того страшного дня 24 лютого 2022 року. По-перше, існує напруга між необхідністю дотримання принципу свободи слова та застарілою, але не менш гострою потребою деолігархізації ЗМІ, власники яких не завжди опиралися спокусі заробити через ЗМІ гроші та політичний капітал на поширенні антидержавних наративів. Незважаючи на деякі неприємні події, українські ЗМІ та журналісти показали себе в найкращому світлі під час тотальної війни. Працівники ЗМІ надихали і надихають суспільство у важкий

період вторгнення, заохочуючи громадян до більшої активності у підтримці передових і тилових, робили велику роботу для співвітчизників, які впали у відчай, і тих, хто навіть після початку навали продовжували коливатися у власному виборі сторони у цій війні. Після початку вторгнення він продовжував коливатися у своїй позиції щодо війни. Українські ЗМІ ще отримають заслужену оцінку за те, що українське суспільство зберегло єдність і згуртованість перед ворогами у найважчий для нашої країни період і зуміло мобілізувати якомога більше людей на захист України [55].

Українська інформаційна армія має три важливі фронти.

1. Західний або глобальний фронт (кожен українець намагається розповісти своїм друзям або родичам на Заході про ситуацію в Україні; необхідно донести до світу звістку про напад Росії на Україну, висловити потреби та прохання України про допомогу, закликати до посилення санкцій проти агресора та міжнародної ізоляції).
2. Український фронт (українська кіберармія має поширювати важливу та достовірну інформацію; допомагати владі, військовим і волонтерам працювати та координуватись; підвищувати бойовий дух і усувати паніку; просто розважати; яскравий приклад жінки, яка збила дрон банкою помідорів).
3. Російський фронт (основне завдання –зрив планів ворога; боротьба з кремлівською пропагандою) [46].

У 2022 році «Україна» була найпопулярнішим запитом у Google News. Занепокоєння щодо України виявляється на, здається, всіх можливих платформах. Лише в Раді Безпеки ООН питання нашої країни торкалися на щонайменше 22 різних засіданнях. Іноді країни об’єднуються саме заради України. Таким чином, наприклад, на однойменній американській базі в Німеччині був створений «формат Рамштайн». Мало що описує зміни за останній час так, як настрій виступів Володимира Зеленського у США 16 березня та 22 грудня. Від сказаного українською «Зараз вирішується доля нашої держави. Доля

нашого народу» до сказаного англійською «Всі ми, мільйони українців, прагнемо одного – перемоги».

Окрім дипломатичних заходів, вони із задоволенням зустрічають Президента України чи не на всіх культурних заходах світу. Від церемонії вручення премії «Греммі» та кінофестивалів у Каннах і Венеції до технічної події VivaTech у Парижі Володимир Зеленський постає як «голограма». Що вже й казати про традиційну журналістику. Перегляньте результати 2022 року в будь-якому поважному виданні, й ви обов'язково побачите Україну. Ось вона серед найпопулярніших текстів Politico або найпопулярніших фотографій Reuters. Також 2022 року в нас відкрилися представництва Washington Post та New York Times. І серед їхніх найпопулярніших матеріалів російсько-українська війна також входить до трійки лідерів [12].

Однією з особливостей комунікації української влади із зовнішнім світом є зосередженість на президенті України Зеленському. Люди можуть по-різному ставитися до такого підходу, але 2022 рік приніс Україні багато позитивних моментів. Унікальна харизма та акторський талант Володимира Зеленського, його вміння справляти враження на публіку та викликати бажані емоції були вдало реалізовані. За перші півроку Першої світової війни Україні вдалося посісти лідерство на інформаційному фронті, що є великим досягненням нинішнього глави держави.

Активна медійна діяльність Володимира Зеленського, його виступи в іноземних парламентах, зустрічі з провідними світовими політиками та відомими громадськими діячами принесли нашій державі багато користі в перші місяці після 24 лютого 2022 року. Доброю справою стало створення в травні 2022 року глобальної ініціативи United24 і однією з її складових є онлайн-платформа для збору коштів на підтримку України. Але інформаційний успіх – це не лише результат медійних чи дипломатичних кампаній. Вони безпосередньо пов'язані із зовнішнім середовищем [5].

Зараз ми стали свідомими щодо намірів Росії в Україні. Починаючи з 2022 року російська інформаційна війна в Україні фактично провалюється. Україна

показала світові свою надзвичайну стійкість, дивовижну креативність та автентичність спілкування. Це не порівняти з тим, як Володимир Путін говорить про війну в Україні: він виглядає втомленим, згорбившись над столом, краватка покручена, і він кричить на генералів. Оскільки соціальні мережі вчаться боротися з ботами та тролями, Росія стає менш досвідченою в поширенні дезінформації. Багато людей пророкували «втому від України», але це не так. І все це завдяки силі української історії та щирості спілкування, на відміну від брехні Кремля, яка просто не витримує критики в цій цифровій війн [54].

Також варто згадати про «інформаційний полк» WAW (War Against War), у якому українські креатори, журналісти, режисери, сценаристи та дизайнери співпрацюють з Міністерством культури та інформаційної політики України, щоб протистояти російській пропаганді та фейкам шляхом створення антидезінйормаційного контент. За перші сто днів війни було вироблено понад 500 хв контенту різними мовами, не лише європейськими, а й хінді, арабською, китайською, чеченською, що охоплюють велику географічну територію. Значна частина контенту виробляється російською мовою та поширюється на території противника через різні канали та різні платформи. Зараз росіянин, відвідавши «Російські пірати в прямому ефірі», спочатку подивиться одне з наших відео, а потім перегляне улюблений серіал. Зараз WAW не лише створює відеоконтент, але й розробляє комунікаційні стратегії для багатьох міністерств, та інформаційні кампанії проти ворогів [62].

Особливістю сьогоднішнього протистояння в Україні є відсутність інформаційного вакууму, який існував у 2014 році. В Україні є велика кількість медіаорганізацій та ЗМІ, які створюють контент і пояснюють різним аудиторіям, що насправді відбувається. Крім того, у нас є велика мережа організацій, які борються з дезінформацією, наприклад «Детектор медіа», StopFake, VoxCheck. Усі вони аналізують роботу противника в інформаційному полі та створюють текстовий, аудіо- та відеоконтент різними мовами.

У країні створено Центр протидії дезінформації при РНБО та Інформаційний центр стратегічних комунікацій та безпеки при Міністерстві

культури та інформаційної політики, який займається боротьбою в інформаційному полі. Більше того, Україна не приховує інформацію, а навпаки, максимально розкриває те, що сталося, наприклад те, що сталося в Бучі та Ірпені. Усі вони були виявлені за допомогою таких технологій, як OSINT, і задокументовані міжнародними ЗМІ та правоохоронними організаціями. Поки немає однозначної відповіді, чи зможе Україна перемогти в інформаційному протистоянні з Росією. У зв'язку з забороною російських ЗМІ та соцмереж проведено велику роботу по створенню великої кількості українського контенту для іноземної аудиторії, створенню умов для роботи іноземних журналістів, документуванню військових злочинів, посиленню рівень ЗМІ для підвищення рівня грамотності населення.

Наразі Україна виграє насамперед від свого успіху в привернені уваги Заходу та підтриманні цих симпатій. Але ніхто краще за українців не розуміє окупантів, оскільки Захід не відчуває присутності і думає, що хоче їх знищити. Ми це зробили, тому ми мотивовані розуміти ворога, поширювати цей досвід і домінувати в інформаційному просторі. Так робиться до тих пір, поки правдива історія не стане головним, про що знає весь світ [61].

Висвітлення російського військового вторгнення у світових ЗМІ не залишає сумнівів у тому, наскільки кривавою та незаконною є війна Росії проти України. Західні ЗМІ визнають, що російські ЗМІ є частиною кремлівської машини, але бачать необхідність перевіряти інформацію, яку поширюють росіяни. У міжнародному інформаційному просторі все активніше поширюється інформація про негативні наслідки війни Росії в Україні для економіки, енергетичного та фінансового секторів, продовольчого забезпечення різних регіонів світу. Наприклад, Нігерійська асоціація виробників заявила, що продовження війни матиме негативний вплив на всі сектори економіки країни, якщо її не зупинити. Або інший приклад: з посиланням на оцінки ООН ЗМІ Ірану пишуть, що українська війна спричиняє продовольчу та енергетичну кризу на Близькому Сході та в Африці. Іноземні ЗМІ все частіше повідомляють про реальні проблеми Російської Федерації та її керівництва. Зокрема, протягом

досліджуваного періоду хорватські ЗМІ оприлюднили матеріал про те, що психічне здоров'я Володимира Путіна погане й через це існує цілком реальна загроза використання ядерної зброї. Не залишилася без уваги в закордонних ЗМІ кібератака проти російських медіа, коли хакери «увірвалися» в анонс понеділкової телепрограми провідних російських телеканалів і виклали на табло інформацію про те, що «на руках у влади кров тисяч українців та їхніх дітей» [4].

Однак у перші кілька місяців тотальної війни навіть головні західні ЗМІ спочатку називали війну в Україні «українською кризою» або «українським конфліктом». Умовно висвітлення війни можна поділити на наступні етапи: перший – перший – усі збентежені, шоковані та ще не підозрюють, що ця війна триватиме довго, та й саме слово війна використовувалося максимум відсотках у 30; отім «українська криза», «український конфлікт», просто війна – якась абстракція, а потім «російське вторгнення» і «російська війна проти України». Потім війна в Україні почала потроху розгортатися, переходячи на інші теми. У Великій Британії на перші шпальти вийшов скандал з Борисом Джонсоном. Потрібно розуміти, що через наші війни ми змагаємося з усіма проблемами світу за увагу західної аудиторії. Не зникає, але не завжди веде. Проте війна повернулася на передову, коли українські війська звільнили значну частину Харківської, а згодом і Херсонської областей. Цікаво, що на початку переважала звітність, що, звісно, природно, але потім стало з'являтися все більше аналізу, причому дуже-дуже якісного [22].

Україна стала темою номер один у більшості західних ЗМІ. Велика кількість журналістів прибула в Україну, незважаючи на ризики. 10 березня 2022 року головний радник Офісу президента України Михайло Подоляк заявив: «Щодня на найгарячіших теренах цієї війни перебувають майже 2 тисячі іноземних журналістів». Основними темами публікацій у західних та вітчизняних ЗМІ у період з 24 лютого 2022 року до 6 квітня 2022 року були: повідомлення про початок широкомасштабної війни, блискавичні відомості про об'єкти атаки та міста, кількість жертв нападників, втрати бойової техніки противника, зах. реакція країн на санкції РФ, аналіз і прогнози подальших дій

агресорів, про гуманітарну катастрофу в мирних містах України, про організацію коридорів для евакуації мирних громадян, репортажі та статті про героїчний опір Українські захисники, про організацію волонтерської роботи, новини та аналітичні матеріали про надзвичайні засідання ООН, заходи, події та зустрічі, зустрічі представників НАТО, України та Росії в Білорусі та Туреччині, президента США Джозефа Байдена, генерального секретаря НАТО Єнса Столтенберга Виступи , промови Президента України перед парламентами майже всіх демократичних сил про звірства російських карателів над мирним населенням у Бучі та багатьох інших місцях. Президент України Володимир Зеленський забезпечує належний рівень комунікації з громадянами України через медійну діяльність. Щодня один-два виступи Президента містять важливу інформацію про хід оборони України, пояснюють позицію нашої країни, підтримують моральний дух військових та інформують про взаємодію із західними союзниками [10].

Якщо говорити про країни, найбільш сприйнятливі до пропаганди з боку Російської Федерації, то до списку входять 5 європейських країн. Перша країна – Угорщина, де російський уряд прямо чи опосередковано контролює більшість ЗМІ в Угорщині. Тому місцеві ЗМІ активно пропагують, що країна ні в якому разі не повинна допомагати Україні у війні та відмовляється від тісної співпраці з РФ задля підтримки українців. Характерно й те, що Угорщина часто висловлює антизахідну риторику і критикує європейські санкції проти Росії, красномовно вказуючи на неефективність і беззмістовність цієї риторики. Значна частина цих наративів поширюється провладними громадськими ЗМІ, які складають більшість ЗМІ країни. Тому незалежні ЗМІ, які висловлюють протилежні погляди, просто не можуть збалансувати загальну картину інформаційного простору.

На другому місці – Франція, яка займає нейтральну позицію, а ЗМІ намагаються «стримувати і балансувати», час від часу публікуючи висновки та зауваження російських політиків і псевдоекспертів-пропагандистів. Пояснення

такої позиції полягає в тому, що уникнути російської пропаганди неможливо через її розгалужену мережу дезінформації, поширену по всьому світу.

Третє місце посідає Німеччина. Значну частину інформації про події в Україні повідомили німецькі журналісти, які особисто побували в зоні бойових дій і контактували з українськими експертами, військовослужбовцями, речниками та представниками ЗМІ. Тому військова та гуманітарна підтримка України викликає велике занепокоєння. Проте російський наратив з'явився в німецьких ЗМІ. Зокрема, цей вплив здійснювався через заклики проросійських інтелектуалів, які наполягали на необхідності досягнення миру в Україні «будь-якими засобами».

На четвертому місці Італія. Згідно з висновками дослідників, Італія орієнтована на вирішення внутрішніх проблем країни. Тому новини про Україну зосереджуються лише на найважливіших подіях чи питаннях, які безпосередньо стосуються місцевих інтересів. Також варто зазначити, що італійські бізнесмени, які втратили частину доходів через санкції проти РФ, активно поширюють риторику «мир за всяку ціну». Тому заклик Росії до «примирення братніх народів» отримав резонанс у ЗМІ.

Остання – Латвія. Громадяни та представники Латвії дуже підтримували Україну з початку повномасштабного вторгнення. Однак головною перешкодою є те, що 40% населення країни розмовляє російською. Тому спілкування з українськими представниками ведеться російською мовою. Крім того, російські наративи часто потрапляють в латвійський інформаційний простір саме через мовні бар'єри та те, що ЗМІ використовують російськомовні джерела [63].

Варто зазначити, що навіть через рік після повномасштабного вторгнення новини про війну не зникли, як очікував ворог. Крім того, спостерігаються певні позитивні тенденції у висвітленні війни в Україні західними ЗМІ. По-перше, зараз більше аналітичних новин, «чому Україна виграла» і «як Росія все програла». Останнім часом з'явилося багато матеріалів про контратаки та їх важливість. По-друге, все частіше в зарубіжних ЗМІ з'являються пояснення глобальних економічних процесів, наприклад російської агресії, яка призвела до

інфляції в ЄС. Тобто західні читачі правильно сформували причинно-наслідковий зв'язок, у якому Росія відповідальна за економічні проблеми. По-третє, іноземні ЗМІ неодноразово закликали до нових обмежувальних заходів і санкцій проти Російської Федерації [9].

Справді, для боротьби з ворогами в інформаційній сфері проведено велику роботу. Зрештою, українці вже добре знають про наміри російської пропаганди. Нас уже не так легко ввести в оману, як це було на початку.

Висновок до розділу 3

У сучасній боротьбі з ворогом важливу роль відіграє інформаційний фронт. Інформаційний фронт складається з комплексу прийомів інформаційно-психологічного впливу, які використовуються для трансформації масової свідомості. Загалом, оскільки поняття інформаційного фронту та його природа є для українців досить новими, проблем з управлінням ним чимало. Наприклад, необізнаність користувачів щодо безпеки мережі, так звана «інформаційна гігієна», нерозуміння правильності подання інформації тощо. Але навіть якщо порівняти перші дні війни з сьогоденням, то інформаційний фронт України виріс, тому в цьому можна побачити багато перспектив. Судячи з того, як війна подається в зарубіжних ЗМІ та які зміни відбулися і будуть, можна з упевненістю сказати, що український інформаційний фронт тримається.

ВИСНОВКИ

Дослідивши питання інформаційного простору України в умовах російсько-української війни можна зробити такі висновки.

Розвиток інформаційної ери означає, що ми повинні переглянути наші теорії за допомогою нової концепції: інформаційної війни. Загальноприйнятого визначення інформаційної війни не існує. Основою більшості визначень є те, що інформаційна війна — це конфлікт, у якому інформація одночасно є і ресурсом, і мішенню, і зброєю Інформація має багато характеристик, які відрізняють її від інших видів ресурсів. Головне, що інформація існує візуально, а не фізично. Його не торкнешся, як кулі чи бомби. Це необмежений ресурс: він може існувати в багатьох місцях одночасно, і ту саму інформацію можуть використовувати обидві сторони конфлікту. Інформація також є нелінійною: хоча великі обсяги даних можуть не мати впливу, невелика кількість даних може змінити хід історії, а значну тактичну чи стратегічну перевагу, на розвиток якої були потрібні роки, можна миттєво втратити. Інформаційна війна стосується всіх аспектів конкуренції, від економічного чи політичного конфлікту до повної війни. Хочемо ми цього чи ні, але наші вороги використовуватимуть проти нас невійськову інформаційну війну. В інформаційній війні існує багато різних видів діяльності. Дані спочатку потрібно зібрати, а потім обробити в певну придатну для використання форму інформації. Цю інформацію необхідно передати відповідним організаціям. Інформаційна війна може набувати багатьох форм: блокування телевізійних, інтернет- та радіопередач для порушення комунікацій; логістичні мережі можуть бути відключені; організоване використання соціальних медіа та інших онлайн-платформ для створення контенту, який можна використовувати для впливу на сприйняття громадськості; ворожі комунікації Мережа може бути відключеним або зміненим тощо.

Боротьба з тотальним вторгненням ведеться на всіх фронтах. Водночас надзвичайно важливу роль відіграє інформаційний фронт, який протидіє масовій пропаганді расистських ідеологій, захищає інформаційні платформи України,

об’єднує українців для пошуку ефективних шляхів припинення війни та подолання її наслідків.

Основними засобами інформаційної війни в Російській Федерації є соціальна дезінформація та кібератаки. 15 лютого 2022 року українські сайти, а також сайти та сервіси багатьох українських банків зазнали кількох хвиль атак. За даними Ради національної безпеки США, ці напади безперечно пов'язані зі спецслужбами РФ. У перші кілька днів метою було зірвати та залякати українські сили та змусити їх припинити захист України. 24 лютого українці опинилися у так званому інформаційному вакуумі — відсутність певної інформації, нерозуміння того, що відбувається, відсутність офіційних пояснень. В інформаційному вакуумі люди схильні вірити першій і найкращій інформації, яка дасть відповіді на актуальні теми або забезпечить певний ступінь новизни.

Для створення інформаційного хаосу окупанти не лише використовують поточний інформаційний привід для створення нових фейків, а й поширюють нісенітницю кількарічної давності. Чутки є одним із найдешевших і найефективніших способів поширення неправдивої або спотвореної інформації. Ці звіти надходять з одного або кількох джерел і стосуються непідтверджених інцидентів. Пояснення неперевіреної інформації сумнівного походження, яка не піддається перевірці, але поширюється швидко і масово. Якщо раніше чутки поширювалися виключно з вуст в уста, то тепер вони, швидше за все, поширюватимуться у форматі текстових повідомлень через месенджери та соціальні мережі. «Неофіційно», «Секретно», «Терміново», «Повідомити рідним».

Наразі мета російської інформаційно-психологічної війни – створити найкращі умови для контролю російськими військами української території, тобто зробити все можливе, щоб українці припинили опір російським окупантам. Зазвичай це неформальне спілкування, радіопередачі, інформаційні бюлетені, листівки, взагалі все, що допомагає охопити якомога більше людей. У рамках інформаційних атак окупанти поширюють неправдиві документи під виглядом указів, постанов чи законів офіційної української влади. Поширювати

пропаганду, спрямовану на поширення паніки, альтернативних версій та створення інформаційної плутанини, дискредитацію українських Збройних сил, влади, волонтерів та ЗМІ, розпалювання ворожнечі та руйнування суспільної моралі.

Основними негативними тенденціями та проблемами розвитку інформаційного простору є: відсутність виваженої інформаційної політики та слабкі позиції держави як основного суб'єкта інформаційного ринку, недостатній розвиток інформаційної інфраструктури та низький рівень сучасної інформаційні технології часткова участь України в процесах глобалізації та дефіцит інформації у світі Низький рівень присутності інформаційна експансія інших країн на територію України та її неконкурентоспроможність у сфері інформаційних технологій на світовому ринку .

Проте розвиток інформаційного простору має як проблеми, так і перспективи, особливо початок переходу до контрнаступу на інформаційному фронті та інтеграція в інформаційний простір ЄС з позитивною метою.

Про подальше вдосконалення та перспективи інформаційного простору України варто додати:

1. Поступово відходити від постійного трансляції повідомлення «все добре». Завищені очікування, створені в суспільстві споживанням таких інформаційних продуктів, можуть (і призводять) до ще більшого розчарування. Треба також бути готовим до тривалої боротьби на передовій та в інформаційному просторі. І говорити про це відкрито.
2. Перехід від реальності «інформаційного захисту» чи «інформаційного опору» до інформаційного злочину. Не просто задовольнятися тим, що Україна рухається до кордонів 1991 року; Це буде кінець війни, але змоделювати післявоєнну систему, обговорити складні гарантії безпеки, нарешті представити варіанти, які мають сформуватися в нинішній позиції Російської Федерації, щоб вона відмовилася від планів агресії проти України та інші сусідні країни.

3. Не мовчати про побутові проблеми. Звичайно, жорстока, а тим більше безпідставна критика керівництва країни, яке протистоїть агресору, зіграє на руку ворогу. Але вказати на деякі затримки в спроможності України виконати вимоги, необхідні для європейської та євроатлантичної інтеграції, викрити корупційні плани, які часто, особливо на місцях, не дають жодного прогресу, запропонувати більш ефективні механізми розвитку економіки, соціальна мобілізація та підвищення рівня самоідентифікації українців – що можуть і повинні робити ЗМІ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ:

1. Антонова С. Є., Мартинюк Г. Ф. Інформаційна безпека. Державне управління: удосконалення та розвиток, 2019. 7 с. URL:http://www.dy.nayka.com.ua/pdf/11_2019/38.pdf (дата звернення: 01.09.2023)

2. Бовкун С. Ю. Методи протидії російській дезінформації в Україні (24 лютого – 31 травня 2022 року). Київ, 2022. 97 с. URL:https://ekmair.ukma.edu.ua/server/api/core/bitstreams/b3e4defc-8c0b-4aaf-b94f-fca5e6159700/content (дата звернення: 15.07.2023)

3. Боднар І. Р. Проблеми та перспективи інтеграції України до глобального інформаційного простору. Львів, 2021. 6 с. URL:http://journals-lute.lviv.ua/index.php/visnyk-econom/article/view/960/912 (дата звернення: 01.08.2023)

4. Війна в Україні у фокусі закордонних мас-медіа. Арміяinform, 2022. URL:https://armyinform.com.ua/2022/05/11/vijna-v-ukrayini-u-fokusi-zakordonnyh-mas-media/ (дата звернення: 14.07.2023)

5. Герасименко П. Як Україні не допустити провалу на інформаційному фронті. Zn, ua, 2023. URL:https://zn.ua/ukr/POLITICS/jak-ukrajini-ne-dopustiti-provalu-na-informatsijnomu-fronti.html (дата звернення: 06.08.2023)

6. Дмитренко М. А. Проблемні питання інформаційної безпеки України.

7. Довгань О. Д., Ткачук Т. Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. Інформація і право №2 (25), 2018. URL:http://ippi.org.ua/sites/default/files/9_8.pdf (дата звернення: 09.08.2023)

8. Доктрина информационной безопасности Российской Федерации, 2016. URL:https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html

9. Железняк Я. Не кількістю, а якістю. Як змінилися згадки про війну в Україні в західних медіа. LB.ua, 2022.

URL:https://lb.ua/blog/yaroslav_zhelezniak/528915_kilkistyu_yakistyu_yak_zminilisya.html (дата звернення: 26.06.2023)

10. Жугай В. Й. Висвітлення російсько-української війни 2022 року у ЗМІ. Одеса, 2022. URL:http://dspace.onua.edu.ua/bitstream/handle/11300/20038/%D0%96%D1%83%D0%B3%D0%B0%D0%B9%20%D0%92%D1%96%D1%82%D0%B0%D0%BB%D1%96%D0%B9%20%D0%99%D0%BE%D1%81%D0%B8%D0%BF%D0%BE%D0%B2%D0%B8%D1%87.pdf?sequence=1&isAllowed=y (дата звернення: 17.09.2023)

11. Закон України про інформацію від 1992 року. Верховна Рада України, Законодавство України. URL:https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 27.07.2023)

12. Зубченко Я. Рік України. Як ми вигравали велику медійну війну 2022 року. Детектор медіа, 2023. URL:https://detector.media/infospace/article/206599/2023-01-02-rik-ukrainy-yak-my-vygravaly-velyku-mediynu-viynu-2022-roku/(дата звернення: 16.06.2023)

13. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Політичні науки, 2016. 6 с. URL:https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf (дата звернення: 03.09.2023)

14. Ілюк К. Інформаційна війна – це не тільки фейки. Чому не вірити російським фейкам замало для перемоги в інформаційній війні. Media sapiens, 2022. URL:https://ms.detector.media/propaganda-ta-vplivi/post/29264/2022-03-31-informatsiyna-viyna-tse-ne-tilky-feyky/ (дата звернення: 05.08.2023)

15. Інтеграція України у світовий інформаційний простір. ManagerHelp. URL:http://www.managerhelp.org/hoks-576-1.html(дата звернення: 07.07.2023)

16. Інформаційний простір: український та світовий. Реферат. Освіта.ua. URL:https://osvita.ua/vnz/reports/journalism/25501/(дата звернення: 21.07.2023)

17. Інформаційний фронт не менш важливий, ніж військовий. Косів, 2023. URL:https://kosivart.if.ua/2023/07/20/12405/ (дата звернення: 22.08.2023)

18. Карпук І. О. Значення мовної політики в інформаційному просторі України. Луцьк, 2016. URL:https://www.academia.edu/ (дата звернення: 15.09.2023)

19. Кокотюха А. Успіхи та помилки українського інформаційного фронту у гарячій фазі війни. Детектор медіа, 2022. URL:https://detector.media/infospace/article/197660/2022-03-19-uspikhy-ta-pomylky-ukrainskogo-informatsiynogo-frontu-u-garyachiy-fazi-viyny/ (дата звернення: 28.06.2023)

20. Корсунський С. Інформаційна складова війни: як Росія намагається послабити підтримку Заходу. Радіо Свобода, 2022. URL:https://www.radiosvoboda.org/a/informatsiyna-viyna-rosiyskyy-vplyv/31811302.html (дата звернення: 21.08.2023)

21. Кунєв Ю. Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження. Київ, 2021. URL:https://dspace.nau.edu.ua/bitstream/NAU/53719/1/%D0%AE.%20%D0%94.%20%D0%9A%D1%83%D0%BD%D1%94%D0%B2.pdf (дата звернення: 17.07.2023)

22. Кур'ята Н. Як іноземні ЗМІ висвітлюють війну Росії в Україні та що ми маємо їм донести. Thepage, 2022. URL:https://thepage.ua/ua/experts/yak-zahidni-zmi-visvitlyuyut-vijnu-v-ukrayini(дата звернення: 23.08.2023)

23. Маркєєва О., Розвадовський Б. Сучасний фронт української контррозвідки: планка вимог підвищується. Національний інститут стратегічних досліджень, 2020. URL:https://niss.gov.ua/news/statti/suchasniy-front-ukrainskoi-kontrrozvidki-planka-vimog-pidvischuetsya (дата звернення: 16.08.2023)

24. Матвієнків С. М., Шмаленко Ю. І., Кольцов В. М. Національний інформаційний простір України: проблеми та перспективи розвитку. Актуальні проблеми філософії та соціології, 2022. 5 с. URL:http://dspace.onua.edu.ua/bitstream/handle/11300/22884/%d0%a8%d0%bc%d0%b0%d0%bb%d0%b5%d0%bd%d0%ba%d0%be-

%d0%90%d0%9f%d0%a4%d0%a1-2022.pdf?sequence=1&isAllowed=y (дата звернення: 15.09.2023)

25. Матвієнків С. М., Шмаленко Ю. І., Кольцов В. М. Національний інформаційний простів України: проблеми та перспективи розвитку. Актуальні проблеми філософії та соціології, 2022. 5 с.

26. Медіаспоживання українців: другий рік повномасштабної війни. Опитування ОПОРИ, 2023. URL:https://www.oporaua.org/polit_ad/mediaspozhivannia-ukrayintsiv-drugii-rik-povnomasshtabnoyi-viini-24796 (дата звернення: 19.07.2023)

27. Москвич О. Світлина як інструмент боротьби на інформаційному фронті: соціокультурний аспект. Збірник тез І Міжнародної благодійної науково-практичної конференції. Луцьк, 2023. С. 155-158. URL:https://vnu.edu.ua/sites/default/files/2023-01/Zbirnyk_tez_3.pdf#page=155 (дата звернення: 25.08.2023)

28. Нетреба М. М., Рижова Д. О. Digital креативи як інструмент інформаційного супротиву в умовах війни. Вчені записки таврійського національного університету імені В. І. Вернадського, 2022. С. 373-381. URL:http://www.philol.vernadskyjournals.in.ua/journals/2022/3_2022/3_2022.pdf#page=385 (дата звернення: 17.07.2023)

29. Ніколаєнко Н. Інформаційний фронт російсько-української гібридної війни. Суспільні комунікації та мовні універсалії, 2022. URL:https://www.relint.vnu.edu.ua/index.php/relint/article/view/248/223 (дата звернення: 21.07.2023)

30. Новомова: як російська пропаганда намагається конструювати реальність росіян і деморалізувати українців за допомогою слів. Реанімаційний пакет реформ, 2023. URL:https://rpr.org.ua/news/novomova-iak-rosiyska-propahanda-namahaietsia-konstruiuvaty-realnist-rosiian-i-demoralizuvaty-ukraintsiv-za-dopomohoiu-sliv/ (дата звернення: 23.08.2023)

31. Орел В. Наслідки інформаційної війни, як загроза територіальній цілісності держави. Київ, 2022. 43 с.

URL:https://er.nau.edu.ua/bitstream/NAU/55628/1/%d0%b4%d0%b8%d0%bf%d0%bb%d0%be%d0%bc%20%d0%bf%d1%80%d0%b0%d0%b2%d0%ba%d0%b8%20%28%d0%b2%d0%be%d1%81%d1%81%d1%82%d0%b0%d0%bd%d0%be%d0%b2%d0%bb%d0%b5%d0%bd%29.pdf (дата звернення: 18.07.2023)

32. Осмоловська А. О. Інформаційний простір України: національний та зовнішньополітичні виміри. 3 с.

33. Під час війни ключовим мінусом є контрольований інформаційний простів, який іде через єдиний суспільний марафон, - нардепка Савчук. Еспресо, 2022. URL:https://espreso.tv/pid-chas-viyni-klyuchovim-minusom-e-kontrolovaniy-informatsiyniy-prostir-yakiy-yde-cherez-ediniy-suspilniy-marafon-nardepka-savchuk(дата звернення: 14.08.2023)

34. Правила поганого тону: заголовки новин подеколи суттєво викривляють український інформаційний простір. Інститут демократії ім. Пилипа Орлика, 2023. URL:https://idpo.org.ua/articles/5460-pravila-durnogo-tonu-zagolovki-novin-podekoli-suttyevo-vikrivlyayut-ukra%D1%97nskij-informacijnij-prostir.html(дата звернення: 03.09.2023)

35. Руденко О. Після початку повномасштабного вторгнення світ чітко зрозумів, що таке Україна. The Aspen Institute, 2023. URL:https://aspeninstitutekyiv.org/pislia-pochatku-povnomasshtabnoho-vtorhnennia-svit-chitko-zrozumiv-shcho-take-ukraina-holovna-redaktorka-kyiv-independent-olha-rudenko/(дата звернення: 16.08.2023)

36. Сабрі К.Н. Інформаційно-іміджевий аспект гібридної війни. «Молодий вчений» №5. Київ, 2018 р. С. 206-209. URL:https://molodyivchenyi.ua/index.php/journal/article/view/4495/4419 (дата звернення: 16.07.2023)

37. Сафаров А. Аналіз Стратегії інформаційної безпеки в порівнянні з чинною Доктриною інформаційної безпеки. Інститут масової інформації, 2021. URL:https://imi.org.ua/monitorings/analiz-strategiyi-informatsijnoyi-bezpeky-v-porivnyanni-z-chynnoyu-doktrynoyu-informatsijnoyi-i38852 (дата звернення: 05.09.2023)

38. Сивак Р. І. Меми як засіб інформаційного опору в часи російсько-української війни (на прикладі мему «Могилізація»). Донецький національний університет імені Василя Стуса. Вінниця, 2022. URL:http://r.donnu.edu.ua/bitstream/123456789/2621/1/%d0%a0%d0%9e%d0%94%d0%98%d0%93%d0%86%d0%9d%20%d0%9a%2c.pdf (дата звернення: 21.08.2023)

39. Сідченко С. О., Залкін С. В., Хударковський К. І. Основні етапи інформаційної кампанії Російської Федерації в ході збройної агресії проти України станом на вересень 2022 року. Харківський університет Повітряних Сил ім. І Кожедуба. Харків, 2022. 14 с.

40. Скібіцька Ю. Війна на інформаційному фронті. Чого ми досягли, а в чому наробили помилок. Суспільне культура, 2022. URL:https://suspilne.media/245559-vijna-na-informacijnomu-fronti-cogo-mi-dosagli-a-v-comu-narobili-pomilok-poasnue-uliana-skibicka/ (дата звернення: 16.07.2023)

41. Сливка М. М., Лук'янова Г. Ю. Правове забезпечення інформаційної безпеки: досвід країн Європейського Союзу. Юридичний науковий електронний журнал №11, 2021. URL:http://www.lsej.org.ua/11_2021/134.pdf(дата звернення: 23.07.2023)

42. Соколенко Н. Що МИ здатні зробити для створення НАШОГО інформаційного простору. Українська правда, 2023. URL:https://blogs.pravda.com.ua/authors/sokolenko/5165492a7ca1b/ (дата звернення: 12.07.2023)

43. Становлення і розвиток інформаційного суспільства. Букліб. URL:https://buklib.net/books/27579/ (дата звернення: 13.08.2023)

44. Степко О. М. Аналіз головних складових інформаційної безпеки держави. 10 с.

45. Стратегія інформаційної безпеки – 2025: що зміниться у сфері цифрових прав. GigitalSecurityLab, 2021.

URL:https://dslua.org/publications/stratehiia-informatsiynoi-bezpeky-2025-shcho-zminytsia-u-sferi-tsyfrovykh-prav/(дата звернення: 11.07.2023)

46. Стрикун Г. Як стати солдатом інформаційного війська. Національна платформа малого та середнього бізнесу, 2022. URL:https://platforma-msb.org/yak-staty-soldatom-informatsijnogo-vijska/ (дата звернення: 07.08.2023)

47. Субота І. Інформаційна світова війна: як РФ втручається в інформаційний простір і підриває кібербезпеку. LB.ua, 2023. URL:https://lb.ua/news/2023/03/16/549053_informatsiyna_svitova_viyna_yak_rf.html(дата звернення: 05.07.2023)

48. Султан С. Л. Використання методів «Інформаційної війни» під час збройного конфлікту на сході України (2014-2020 рр.) Україна у світовому історичному просторі. Маріуполь, 2020. С. 140-142. URL:https://mdu.in.ua/Nauch/Konf/2020/ukrajina_v_svitovomu_istorichnomu_prostori_2020.pdf#page=140 (дата звернення: 16.07.2023)

49. Сьогодні інформаційна війна – це стрижнева конструкція будь-якої війни. Арміяinform, 2023. URL:https://armyinform.com.ua/2023/02/27/sogodni-informaczijna-vijna-cze-stryzhneva-konstrukcziya-bud-yakoyi-vijny-ganna-malyar-2/ (дата звернення:18.07.2023)

50. Ткаченко О. «Інформаційний Рамштайн» - початок єдиного інформаційного фронту країн-союзників. Українська правда, 2022. URL:https://www.pravda.com.ua/columns/2022/09/30/7369845/(дата звернення: 15.08.2023)

51. Указ президента України №43/2021. Про рішення Ради національної безпеки і оборони України від 2 лютого 2021 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». URL:https://www.president.gov.ua/documents/432021-36441 (дата звернення: 27.10.2023)

52. Указ Президента України про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". Законодавство України, 2021.

URL:https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення:12.08. 2023)

53. Українська аудиторія після початку великої війни: зміни у медіаспоживанні, сприйняття інформаційного простору, чутливість до спотвореного контенту. Реанімаційний пакет реформ, 2022. URL:https://rpr.org.ua/news/ukrainska-audytoriia-pislia-pochatku-velykoi-viyny-zminy-u-mediaspozhyvanni-sprryniattia-informatsiynoho-prostoru-chutlyvist-do-spotvorenoho-kontentu/(дата звернення:10.09.2023)

54. Ульяновська М. Російська інформаційна війна в Україні провалюється – Ніна Янковіч. Інтерв'ю. Голос Америки, 2023. URL:https://www.holosameryky.com/a/jankowicz-russian-disinformation-failing/6961072.html(дата звернення:13.06.2023)

55. Філіонов М. Трансформація українських медіа під час війни: здобутки, виклики і перспективи. Interfax Ukraine, 2023. URL:https://interfax.com.ua/news/blog/914975.html(дата звернення: 29.08.2023)

56. Фролова О., Чекмарьова В. Інтеграція України до Європейського інформаційного простору. Київський національний університет імені Тараса Шевченка. Київ, 2022. 12 с. URL:http://relint.vnu.edu.ua/index.php/relint/article/view/244/238(дата звернення: 27.07.2023)

57. Хорошко В., Хохлачова Ю., Прокофьєв М. Концепція застосування інформаційних впливів та протидія інформаційній зброї. Правове забезпечення захисту інформації. Проблеми розвитку нормативної та методичної без систем захисту інформації, 2016. 15 с. URL:https://ela.kpi.ua/bitstream/123456789/25490/1/31_p9.pdf (дата звернення: 15.06.2023)

58. Шабанова Я. Як змінився український медіаландшафт після 24 лютого. Speka media, 2022. URL:https://speka.media/yak-zminivsya-ukrayinskii-medialandsaft-pislya-24-go-lyutogo-2022-vzxd4p(дата звернення:01.08.2023)

59. Шаталова І. Рік повномасштабної брехні: що передрікає російська дезінформація. Zmina, 2023. URL:https://zmina.info/articles/rik-povnomasshtabnoyi-brehni-shho-peredrikaye-rosijska-dezinformacziya/(дата звернення: 30.07.2023)

60. Шуляк А., Панас В. Забезпечення інформаційної безпеки. Україна та Польща: минуле, сьогодення, перспективи, 2019. URL:https://ukrpolnauka.wordpress.com/2019/11/21/ (дата звернення: 30.10.2023)

61. Шутяк Л. Битва за громадську думку: як Україна воює з Росією на інформаційному фронті. Explainer, 2022. URL:https://explainer.ua/bitva-za-gromadsku-dumku-yak-ukrayina-voyuye-z-rosiyeyu-na-informatsijnomu-fronti/(дата звернення: 22.07.2023)

62. Що треба знати про «інформаційний полк». War Against War Vogue, 2022. URL:https://vogue.ua/article/culture/lifestyle/shcho-potribno-znati-pro-informaciyniy-polk-war-against-war-48771.html(дата звернення: 19.08.2023)

63. Як висвітлюють Україну у різних медіа Європи? Visit Ukraine, 2023. URL:https://visitukraine.today/uk/blog/1889/yak-visvitlyuyut-ukrainu-u-riznix-media-jevropi(дата звернення: 13.07.2023)

64. Bertolin Giorgio, “Conceptualizing Russian Information Operations: Info-War and Infiltration in the Context of Hybrid Warfare,” IO Sphere, Summer 2015, p. 10.

65. Cunningham Conor. A Russian Federation Warfare Primer. The Henry M. Jackson School of International Studies, University of Washington, 2020. URL:https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/(дата звернення: 21.09.2023)

66. Cybersecurity in Ukraine: National Strategy and international cooperation. GFCE, 2017. URL:https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/ (дата звернення: 15.08.2023)

67. Dahm Mike. The Reality of War Should Define Information Warfare. U.S. Naval Institute, 2021.

URL:https://www.usni.org/magazines/proceedings/2021/march/reality-war-should-define-information-warfare (дата звернення: 06.08.2023)

68. De Schutter Patric. Information Warfare: How Does It Work And How To Protect Yourself. Mailfence Blog, 2022. URL:https://blog.mailfence.com/information-warfare/ (дата звернення: 04.09.2023)

69. Disinformation and Russia's war of aggression against Ukraine. OECD Policy Responses in the Impacts of the War in Ukraine, 2022. URL:https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/ (дата звернення: 12.07.2023)

70. Facts vs Fiction: Russian Disinformation on Ukraine. U.S. Department of State, 2022. URL:https://www.state.gov/fact-vs-fiction-russian-disinformation-on-ukraine/ (дата звернення: 10.09.2023)

71. Five Things to Know About the Information War. Peraton. URL:https://www.peraton.com/news/five-things-to-know-about-the-information-war/

72. How Does Cyber Warfare Work? Forbes. URL:https://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work/?sh=5036bc8644ce (дата звернення: 04.09.2023)

73. Information Security: The Ultimate Guide. Imperva. URL:https://www.imperva.com/learn/data-security/information-security-infosec/ (дата звернення: 05.08.2023)

74. Information Space. Infovis. URL:https://infovis-wiki.net/wiki/Information_Space (дата звернення: 23.08.2023)

75. Information Warfare. European Center for Populism Studies. URL:https://www.populismstudies.org/Vocabulary/information-warfare/ (дата звернення: 19.07.2023)

76. Joyal Paul M. Cyber Threats and Russian Information Warfare. Jewish Policy Center, 2016. URL:https://www.jewishpolicycenter.org/2015/12/31/russia-information-warfare/ (дата звернення: 11.08.2023)

77. Klepper David. Russian disinformation spreading in new ways despite bans. APnews, 2022. URL:https://apnews.com/article/russia-ukraine-misinformation-

european-union-government-and-politics-e5a1330e834fde428aab599b5c423530(дата звернення: 18.07.2023)

78. Koridze Nata. Report| Atlantic Council: Russia's Information Warfare Against Ukraine Spans Many Fronts, 2023. URL:https://civil.ge/archives/526619 (дата звернення: 08.07.2023)

79. Lelonek. A. Rosyjska wojna informacyjna – front ukraiński. Fundacja im. Kazimerza Pułaskiego. URL:https://pulaski.pl/rosyjska-wojna-informacyjna-front-ukrainski/(дата звернення: 17.09.2023)

80. Panhalkar Tushar. Top categories which includes in Information Warfare. Infosavvy Security and IT Management Training. URL:https://info-savvy.com/information-warfare/(дата звернення:27.07.2023)

81. Paul Christopher, Matthews Miriam. The Russian "Firehouse of Falsehood" Propaganda Model, 2016. URL:https://www.rand.org/pubs/perspectives/PE198.html(дата звернення: 16.07.2023)

82. Perez Christian, Nair Anjana. Information Warfare in Russia's War in Ukraine. Foreign Policy, 2022. URL:https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/(дата звернення:19.08.2023)

83. Sarkar Mithun. Information Warfare: Manipulation of Information in a War. Unrevealed Files, 2022. URL:https://www.unrevealedfiles.com/information-warfare-manipulation-of-information-in-a-war/ (дата звернення: 05.09.2023)

84. Schulze Matthias, Kerttunen Mika. Cyber Operations in Russia's War against Ukraine. Stiftung Wissenschaft und Politik, 2023. URL:https://www.swp-berlin.org/10.18449/2023C23/ (дата звернення:09.09.2023)

85. Snegovaya Maria. Putin's Information Warfare in Ukraine, 2015. URL:https://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf (дата звернення: 17.08.2023)

86. What is information warfare and how pervasive is it& World Economic Forum, 2022. URL:https://www.weforum.org/agenda/2022/04/what-is-information-warfare-and-how-pervasive-is-it/ (дата звернення: 26.08.2023)

87. Wilde Gavin, Sherma Justinn. No Water's Edge: Russia's Information War and Regime Security. Carnegie endowment for international peace, 2023. URL:https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644 (дата звернення: 05.07.2023)

88. Yasar Kinza, Information security (infosec). TechTarget. URL:https://www.techtarget.com/searchsecurity/definition/information-security-infosec (дата звернення: 16.09.2023)