Міністерство освіти і науки України
Національний університет «Острозька академія»
Навчально-науковий інститут міжнародних відносин та національної безпеки
Кафедра національної безпеки та політології

Кваліфікаційна робота на здобуття освітнього ступеня магістра на тему:

«Інформаційна безпека як складова національної безпеки»

Виконала студентка ІІ курсу, групи МНб-21
Спеціальності 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»
Чичеба Дарія Олегівна

Керівник – кандидат політичних наук, доцент
Жовтенко Тарас Григорович
Рецензент – кандидат політичних наук, доцент
кафедри політології та соціології Рівненського державного гуманітарного університету
Крет Роман Михайлович

Острог, 2022

ЗМІСТ

ВСТУП

Актуальність даної теми зумовлена тим, що сучасний етап суспільного розвитку характеризується підвищенням ролі інформаційної сфери, яка є сукупністю інформації, інформаційною інфраструктурою, суб'єктами, які збирають, формують, поширюють і використовують інформацію, а також формування системи регулювання суспільних відносин.

Інформаційна безпека є однією із проблем, з якою зіткнулося сучасне суспільство у процесі масового використання автоматизованих засобів її обробки. Проблема інформаційної безпеки обумовлена зростаючою роллю інформації у житті соціуму. Сучасне суспільство все більше набуває рис інформаційного суспільства.

У суспільстві зростає роль ЗМІ як інструменту пропаганди та агітації. Після закінчення холодної війни на тлі прискореного технологічного розвитку інформаційні конфлікти на короткий час затихли, а на початку XXI століття посилилися. Якщо у другій половині XX століття вона розвивалася за біполярною моделлю, то зараз боротьба ведеться за участю країн «третього світу».

В умовах збройних конфліктів, а також безпосередньо до та після їх активної фази роль ЗМІ як інструменту інформаційного протиборства багаторазово зростає. Інформаційна поразка може значно скоригувати і навіть звести нанівець результати перемоги збройних сил. Особливо актуальною дана тема є в сучасних реаліях, внаслідок російського вторгнення в Україну.

Проблему інформаційної безпеки розглядали у своїх працях багато вітчизняних та зарубіжних вчених, серед них Абрамов В. І., Ситник Г. П., Смолянюк В. Ф., Нижник Н.Р., Кравець Є. А. , Дмитренко М.А., Малик Я. Й., Гурковський В. І., Проноза І. І., Горбань Ю. О., Зінченко М. О., Плугова О. Б, Драглюк О. В., Попович К. В., Шумка А. В., Шпига П. С. та ін.

Тим не менш, розробка механізмів забезпечення інформаційної безпеки потребує подальшої розробки та наукового обґрунтування їх сучасних методів, що зумовлює вибір теми, цілей і завдань наукових досліджень.

Мета і завдання дослідження. Мета роботи полягає в дослідженні особливостей інформаційної безпеки як складової національної безпеки України. Виходячи з поставленої мети, завданнями роботи є:

1. Визначити сутність та особливості поняття та характеристики інформаційної безпеки.

2. Дослідити роль та місце інформаційної безпеки в системі національної безпеки.

3. Проаналізувати проблеми інформаційної безпеки в Україні у політичній сфері.

4. Вивчити сутність та особливості інформаційної війни.

5. Обґрунтувати особливості інформаційної війни як одного з елементів війни в Україні.

6. Дослідити висвітлення війни в Україні в російських інформаційних джерелах.

Об'єктом дослідження є відносини, пов'язані із особливостями інформаційної безпеки як складової національної безпеки України та проведення інформаційної війни як елемента війни на території нашої держави.

Предмет дослідження – інформаційна безпека як складова національної безпеки.

Теоретико-методологічні засади дослідження:

Дослідницьке питання: якими є актуальні проблеми інформаційної безпеки як складової національної безпеки України?

Методи дослідження. Для розв'язання поставлених завдань використані загальнонаукові та приватно-наукові методи, що застосовуються при вивченні суспільних відносин. При підготовці та написанні роботи, активно використовувалися діалектичний, логічний, історичний, системний методи, а також метод порівняння.

Структура магістерської роботи визначається поставленою метою, і складається зі вступу, основної частини, розділеної на два розділи, висновків, списку використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИЯК СКЛАДОВОЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1.1 Поняття та характеристика інформаційної безпеки

Інформаційна сфера стала системоутворюючим фактором суспільного життя та активно впливає на стан політичної, економічної, оборонної та інших складових безпеки України.

Законодавче визначення поняття «інформація» міститься у Законі України «Про інформацію», згідно зі ст. 1 якого: «Інформацією є будь-які відомості та/або дані, що можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [40].

З часів появи людини безпека була найважливішою потребою окремих людей і суспільства в цілому. З філософської точки зору вона служить проявом життєздатності і життєстійкості предметів матеріального світу. Однак просте, суто вербальне тлумачення цього поняття як відсутності небезпеки або «відсутності загрози для власних цінностей», або важливих умов діяльності для окремих людей, наших суспільств і держав, виглядає нерозумним, оскільки воно, здавалося б, означає усвідомлення можливості цієї ідеальної ситуації. Але в реальному житті завжди є різні небезпеки.

Тому категорія «безпека» є не абсолютною, а відносною, що має значення лише стосовно конкретного об’єкта чи сфери діяльності людини та навколишнього світу [51, с. 62].

У суспільній практиці все ширше вживається поняття «безпека життєдіяльності». Що стосується практичних потреб, то під «безпекою життєдіяльності» розуміється стан захищеності матеріального світу та людського суспільства від різноманітних негативних впливів різного характеру [3, с. 44].

З цього визначення видно, що об’єктами безпеки життєдіяльності є людина, природа і суспільство. Будь-яка класифікація повинна базуватися на певних основних характеристиках. Серед них насамперед слід виділити об’єкти безпеки, характер загроз та сфери життя. . Залежно від об'єкта, життєво важливі інтереси якого захищаються від внутрішніх та зовнішніх загроз, виділяються, наприклад, такі види безпеки, як безпека людини (особистості), суспільства, держави, етнічної групи (наприклад, російськомовного населення), державних службовців тощо [3, с.45].

Безпека — це рівень небезпеки, який можна допустити на сучасному етапі розвитку науки та економіки. Безпека є прийнятним ризиком. Насправді повна безпека не може бути досягнута, поки існує джерело небезпеки.

Безпека — це стан захищеності людей, суспільств і націй від внутрішніх і зовнішніх загроз. Залежно від об’єкта загрози можна виділити такі види безпеки, як особиста, публічна, національна, глобальна [2, с.2].

Особиста безпека стосується захисту людей, який визначається індивідуальними якостями людей і методами особистого захисту, які вони застосовують. Правове вираження особистої безпеки розуміється як правова можливість фізичних осіб як суб’єктів права підтримувати безпечні умови життя, виконувати та підтримувати яке зобов’язується держава [3, с. 57].

Особисту безпеку слід розглядати як комплексну законодавчу систему, яка включає не лише спеціалізовані нормативно-правові акти у сфері захисту особистої безпеки, а й галузеві акти. Громадська безпека залежить від рівня організованості державних установ і свідомості людей. Лише на основі єдності та міжнаціональної злагоди, з національною ідеєю, підтриманою всім народом, держава може стати найсильнішою та динамічнішою країною. Тому реалізація єдиної національної політики є запорукою громадської безпеки [3, с. 59].

Національна безпека включає оборону країни та всі види безпеки, передбачені Конституцією та її законодавством України, насамперед

національну, громадську, інформаційну, екологічну, економічну, транспортну, енергетичну та безпеку особистості.

Глобальна безпека — захист планети від внутрішніх (екологічних, природних, техногенних) і зовнішніх (космічних, позаземних) загроз, забезпечується шляхом міжнародного співробітництва та міждержавних угод. Нові виклики та загрози, серед яких зіткнення цивілізацій, міжнародний тероризм, глобальні фінансово-економічні кризи, енергетична та інформаційна безпека, природні, техногенні та соціальні катастрофи, кліматичні катастрофи, епідемії тощо. Вони проникливо ставлять питання про необхідність нової парадигми забезпечення якості глобальної безпеки. Водночас деякі експерти розглядають питання міжнародної безпеки (включаючи військово-політичну складову) як традиційні форми зовнішньополітичної діяльності [10, с. 99].

Основними принципами забезпечення безпеки є: дотримання і захист прав і свобод людини та громадянина; законність; системність і всебічність застосування органами державної влади політичних, організаційних, соціально-економічних, інформаційних, правових та інших заходів безпеки; пріоритет превентивних заходів, забезпечення порядку безпеки, взаємодія органів державної влади з громадськими об’єднаннями, міжнародними організаціями та громадянами з метою забезпечення безпеки [42].

Державні заходи з національної безпеки включають:

1) прогнозування, виявлення, аналіз та оцінка загроз безпеці;

2) визначає основні напрямки політики та стратегічного планування у сфері національної безпеки;

3) закони та нормативні акти у сфері безпеки;

4) розробку та застосування комплексу оперативних і довгострокових заходів щодо виявлення, запобігання та усунення загроз безпеці, локалізації та протидії наслідкам їх проявів;

5) вживати спеціальних економічних заходів для забезпечення безпеки;

6) розроблення, виробництво та використання сучасної зброї, військової та спеціальної техніки, техніки подвійного та цивільного призначення з метою забезпечення безпеки;

7) організація наукової діяльності у сфері безпеки;

8) координація діяльності органів та суб'єктів місцевого самоврядування у сфері безпеки;

9) фінансування витрат на охорону, контроль за цільовим витрачанням виділених коштів;

10) міжнародне співробітництво з метою забезпечення безпеки;

11) здійснення інших заходів у сфері безпеки відповідно до законодавства України [58, с. 33].

Литвиненко О. запропонував, що з точки зору захисту життєво важливих інтересів особи, суспільства та країни інформаційну безпеку слід розуміти як аспект розгляду інформаційних відносин у рамках інформаційного законодавства, зосередивши увагу на загрозах цим інтересам. Ці інтереси та механізми усунення або запобігання таким загрозам правовими засобами [29, с.47-49].

Л.Р. Наливайко вважає, що під інформаційною безпекою слід розуміти сукупність засобів забезпечення інформаційного суверенітету України та захисту інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Така безпека повинна включати ефективні заходи протидії комплексним інформаційним загрозам [32, с. 60].

За енциклопедичним визначенням під категорією «інформаційна безпека» можна розуміти: законодавче формування національної інформаційної політики, створення належних можливостей для прийняття рішень органами державної влади, громадянами та об'єднаннями громадян, іншими юридичними особами України відповідно до із законодавством України; гарантування свободи інформаційної діяльності та права доступу до інформації в інформаційному

просторі; всебічний розвиток інформаційних структур; підтримка розвитку національних інформаційних ресурсів України з урахуванням науково-технічних досягнень і особливостей духовного і культурного життя українського народу, створення та впровадження захищених інформаційних технологій, захисту прав власності всіх учасників інформаційної діяльності в національному просторі України; створити загальну систему захисту інформації, зокрема щодо захисту державної таємниці та іншої інформації з обмеженим доступом, захистити національний інформаційний простір України від поширення спотвореної або забороненої законодавством України інформаційної продукції, встановлення законодавством режиму доступу іноземних держав або їх представників до національних інформаційних ресурсів України та порядку використання цих ресурсів на підставі договорів з іноземними державами; законодавче визначення порядку розповсюдження на території України інформаційної продукції іноземного виробництва [26, с.744].

Учасниками системи захисту інформації є: власники об’єктів критичної інформаційної інфраструктури та організацій, що експлуатують такі об’єкти, засоби масової інформації та масових комунікацій, організації грошово-кредитної, валютної, банківської та інших сфер фінансового ринку, оператори зв'язку, оператори інформаційних систем, організації, які займаються створенням і експлуатацією інформаційних систем і мереж зв'язку, організації, що займаються розробкою, виробництвом і експлуатацією засобів забезпечення інформаційної безпеки, організації, що надають послуги у сфері забезпечення інформаційної безпеки, організації, які здійснюють освітню діяльність у цій сфері, громадські асоціації, інші організації та громадяни відповідно до законодавства беруть участь у вирішенні завдань із забезпечення інформаційної безпеки [24, с. 27-28].

Характер міжнародної ситуації дедалі більше визначається загостренням протистояння у глобальному кіберпросторі, оскільки держави прагнуть

використовувати інформаційні та комунікаційні технології для досягнення своїх геополітичних цілей, у тому числі шляхом маніпулювання суспільною свідомістю та фальсифікації історії. З'являються нові форми протиправної діяльності з використанням інформаційно-комунікаційних технологій. Основні загрози національній та громадській безпеці включають діяльність, пов'язану з використанням інформаційно-комунікаційних технологій для поширення та розповсюдження фашистських, екстремістських, терористичних та сепаратистських ідеологій, які ставлять під загрозу громадянське суспільство, соціально-політичну та соціальну стабільність [18, с. 239].

З метою захисту національної та громадської безпеки постійно вдосконалюється система виявлення, аналізу та протидії загрозам в інформаційній сфері. Вживаються заходи щодо посилення захисту громадян і суспільства від згубної інформації з боку екстремістських і терористичних організацій, іноземних спецслужб і пропагандистських структур.

Стратегічною метою забезпечення інформаційної безпеки у сфері оборони країни є захист життєво важливих інтересів особи, суспільства і держави від внутрішніх і зовнішніх загроз, пов'язаних із використанням інформаційних технологій у військово-політичних цілях з порушенням норм міжнародного права, в тому числі за здійснення діяльності, спрямованої на підрив суверенітету, порушення територіальної цілісності держави та воєнні дії та акти агресії, які загрожують міжнародному світу, безпеці та стратегічній стабільності [43].

Найважливішими цілями забезпечення інформаційної безпеки у сфері національної та громадської безпеки є захист суверенітету, підтримання політичної та соціальної стабільності, територіальної цілісності України, забезпечення основних прав і свобод людини і громадянина, захист критичної інформаційної інфраструктури; у стратегічній стабільності та рівноправному стратегічному партнерстві необхідно сформувати стійку систему неконфліктних міждержавних відносин в інформаційному просторі [43].

Наразі ефективне правове регулювання у цій сфері є ускладненим через відсутність системних законодавчих актів, які б закріплювали взаємовідносини у сфері забезпечення безпеки критичної інформаційної інфраструктури України. В економічній сфері метою забезпечення інформаційної безпеки є мінімізація впливу таких несприятливих факторів, як недостатній розвиток вітчизняних інформаційних технологій та електронної промисловості, розробка та виробництво конкурентоспроможних засобів. Забезпечити інформаційну безпеку та підвищити кількість і якість послуг у сфері інформаційної безпеки у сферах науки, техніки та освіти. Метою забезпечення інформаційної безпеки є підтримка інновацій та прискореного розвитку системи інформаційної безпеки, галузі інформаційних технологій та електронної промисловості [23, с. 83] .

До об'єктів критичної інформаційної інфраструктури віднесено інформаційні системи, інформаційно-телекомунікаційні мережі державних органів, а також інформаційні системи, інформаційно-телекомунікаційні мережі та автоматизовані системи управління технологічними процесами, що функціонують в оборонній промисловості, галузі охорони здоров'я, транспорту, зв'язку, кредитно-фінансовій сфері, промисловості, атомної промисловості, ракетно-космічної промисловості, гірничодобувної промисловості, металургійної промисловості та хімічної промисловості.

Пошкодження критичної інформаційної інфраструктури може бути катастрофічним, і враховуючи, що це ланка, що з’єднує інші сектори інфраструктури країни, це неминуче завдасть шкоди й цим секторам. Перехід інформаційно-комунікаційних технологій на цифрові системи сигналізації спрощує та частково автоматизує управління процесами, але водночас робить їх більш уразливими до комп’ютерних атак. Зловмисне програмне забезпечення, яке змінює бінарного коду програми (алгоритм програми, написаний у двійковій обчислювальній системі), здатне вивести з ладу будь-яке обладнання, яке використовує. Водночас не менш небезпечними є атаки окремих осіб, громад,

іноземних спецслужб і організацій у кримінальних, терористичних і розвідувальних цілях [23, с. 84].

Держава має вжити всіх можливих заходів для захисту своєї інформаційної сфери, необхідно створити «державний штаб», який займатиметься не лише захистом та експертизою інформаційного потенціалу, а й плануванням простору несанкціонованих інформаційних операцій.

До основних завдань, які потребують негайного вирішення, належить необхідність нормативно-правового регулювання протидії використанню потенціалу інформаційних технологій, що загрожують інтересам держави. Створення інформаційних військ супроводжувалося багатьма проблемами в різних сферах діяльності. В економічному плані – це не такий якісний, як у зарубіжних країнах, розвиток вітчизняної техніки, наприклад розвиток електронно-компонентної бази, програмного забезпечення, обчислювальної техніки, засобів зв'язку [30, с.14].

Таким чином, зберігається економічна залежність від інших країн. З точки зору науки стан інформаційної безпеки характеризується недостатньою кількістю наукових досліджень, спрямованих на створення перспективних інформаційних технологій. Проблемним є кадрове забезпечення у сфері інформаційної безпеки, оскільки ефективність діяльності в цій сфері залежить від рівня теоретичної та практичної підготовки працівників. Крім того, важливою проблемою є неефективне використання регіональних інформаційних ресурсів, недостатній рівень і можливість вільного доступу громадянам національних інформаційних ресурсів.

Ці проблеми характерні як для військ інформаційних операцій, а й у всій системи захисту інформаційного простору. Проблеми в науці та кадрах зумовлюють необхідність постійного вдосконалення норм та правового забезпечення інформаційної безпеки.

Вирішення зазначених проблем передбачає вдосконалення вітчизняних і розроблених інформаційних технологій, впровадження вітчизняних розробок, підвищення ефективності наукових досліджень, підвищення якості освіти в галузі інформаційних технологій, підвищення обізнаності громадян з питань інформаційної безпеки. Для удосконалення правового поля інформаційної безпеки є організація заходів, пов'язаних із популяризацією правозастосовної практики у даній сфері.

З цього можна стверджувати, що інформаційна безпека – це не тільки стан захищеності інформаційного середовища та ресурсів, а й задоволення інформаційних потреб громадян, суспільства і держави, захист прав суб'єктів інформаційні правовідносини. Негативні зовнішні та внутрішні фактори, що створюють загрозу конфіденційності, цілісності та доступності інформації, застосування яких сприятиме підвищенню рівня ефективності національної політики інформаційної безпеки.

1.2 Роль та місце інформаційної безпеки в системі національної безпеки

Сучасний етап суспільного розвитку характеризується зростанням ролі інформаційної сфери, яка є сукупністю інформації, інформаційною інфраструктурою, суб'єктами, що збирають, формують, поширюють і використовують інформацію, а також системи регулювання суспільних відносин. Інформаційна сфера, як системний фактор суспільного життя, активно впливає на стан політичної, економічної, оборонної та інших безпекових складових України.

Гурковський В.І. визначає національну інформаційну безпеку в Україні як суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства і держави від реальних і потенційних загроз в інформаційному просторі, що необхідно для захисту і примноження

духовних та матеріальних цінностей нації, прогресивного розвитку України, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів [15, с. 12].

У сучасних умовах політичного та соціально-економічного розвитку загострюється протиріччя між необхідністю розширення вільного обміну інформацією та необхідністю збереження певних обмежень на поширення інформації. Зростання соціальної відкритості, підвищення інтенсивності обміну інформацією, широке використання передових технологій збору та обробки інформації створюють передумови для можливих протиправних дій щодо інформації та її користувачів. Тому відкритість інформації має супроводжуватися дотриманням прав людини, соціальних і державних конституційних прав щодо захисту обмеженого доступу до інформації.

Захист інформації — це комплекс заходів, які здійснюються власниками інформації для захисту своїх прав на володіння і розпорядження інформацією, створення умов для обмеження її поширення, виключення доступу до конфіденційної інформації та її носіїв.

Тенденція збільшення ступеня відкритості держави перед суспільством вимагає мінімізації обсягу інформації, що віднесена до державної таємниці, відкритості загального переліку категорій інформації, механізмів засекречування та умов дешифрування, що, з одного боку, є потребою більшої відкрите та доступне сучасне суспільство, а з іншого боку, це необхідність захисту особистої, суспільства та держави.

Характер і особливості російсько-української війни свідчать про те, що її метою є зміна самоідентичності народу та перетворення східної частини нашої країни на «сіру зону», що дозволить мати Російській Федерації важелі свого впливу через постійну загрозу поширення нестабільності на всю Україну. Ця війна не за територію, а за світогляд, розум і душу людей. Оскільки контроль над інформаційною інфраструктурою є основою для формування громадської думки,

яка завжди проявляється спочатку в певних переконаннях, а потім у конкретних діях, то в умовах конкурентної боротьби контроль над інформаційною сферою стає основним ресурсом влади[20, с. 65].

У новій редакції Доктрини інформаційної безпеки України від 2017 року реальними загрозами національній безпеці України в інформаційній сфері визначено: проведення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інші військові формування, що провокують екстремістські прояви, розпалюють панічні настрої, загострення та дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних та міжконфесійних конфліктів в Україні; проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою формування негативного іміджу України у світі; інформаційна експансія держави-агресора та підконтрольних їй структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах; інформаційне домінування держави-агресора на тимчасово окупованих територіях; недостатній розвиток національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії; неефективність державної інформаційної політики, недосконаліть законодавства щодо регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіакультури суспільства; поширення закликів до радикальних дій, пропаганда федералізму та сепаратизму в Україні [19].

Специфіка забезпечення національної інформаційної безпеки відображена в Законах України «Про національну безпеку України» [41], «Про концепцію національної програми інформатизації» [40], «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [42], а також у затвердженій указом Президента Стратегії національної безпеки України [44], у

зв’язку з реалізацією Стратегії Національна рада безпеки і оборони України ухвалила рішення про створення спеціального нового органу як робочого органу – Національного координаційного центру кібербезпеки. Створення такого центру є обґрунтованим, оскільки повноваженнями щодо забезпечення інформаційної безпеки наділена значна кількість державних органів та установ (Національна рада України з питань телебачення і радіомовлення, Держкомтелерадіо України, Служба безпеки України, Служба зовнішньої розвідки України, Міністерство оборони України, МВС України, Міністерство закордонних справ України, Міністерство юстиції України та ін.).

Стратегія національної безпеки України актуальними загрозами національній безпеці України в інформаційній сфері визначає ведення інформаційної війни проти України та відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства [4, с. 12].

Не менш гостро в умовах гібридної війни постає питання кібербезпеки. У сучасному світі кібернетичний простір дедалі частіше слугує для проведення широкого спектра підривних операцій: від викрадення цінної інформації до актів кібертероризму [14, с. 18].

Зрозуміло, що сьогодні українське суспільство знаходиться під постійною загрозою отримання недостовірної, а часом і шкідливої інформації, несвоєчасного отримання інформації, шпигунства, комп’ютерних злочинів тощо. Ці фактори є елементами гібридної війни, які сприяють проникненню агресорів у національну свідомість громадян і підривають державну та інформаційну безпеку.

Основними складовими інформаційної безпеки є забезпечення громадян якісною інформацією та вільний доступ до різноманітних джерел інформації, а також захист від негативної інформації, що в цілому має сприяти цілісності суспільства. Першочерговим завданням суспільства та державних інституцій має стати розробка невідкладних ефективних заходів щодо нейтралізації

інформаційно-підривної діяльності Російської Федерації проти України та недопущення її подальшого розгортання.

Вирішення цього складного питання захист інтересів суспільства і держави, сприятиме реалізації права громадян на повну та якісну інформацію [28, с. 38].

В умовах гібридної війни країни, які стали об’єктами агресії, неминуче стикаються з широким спектром інформаційних загроз, які, з одного боку, потребують спеціальних правових та адміністративних заходів для їх усунення, а з іншого – можуть мати жорсткі обмеження. Знайти баланс між інтересами національної безпеки та концепцією верховенства права є стратегічно важливим завданням, яке стоїть перед країною.

Особливу роль в інформаційній війні відіграють соціальні медіа. Глибинні трансформації ментальної сфери відбуваються за допомогою когнітивної зброї, коли вигадують помилкові, неправильні, недостовірні концепти, розкручують їх у ЗМІ [36, с. 112].

Актуальною новинкою інформаційно-психологічної війни є подвійне поєднання онлайн-медіа. Ця «війна» триває і непомітно. Важко точно визначити його походження, оскільки це часто робиться з кількох джерел одночасно. Зрештою, ця тактика війни пронизує всі верстви суспільства за дуже низьку ціну. Навіть якщо аудиторія не обов'язково вірить в закладену інформацію, велика кількість непідтвердженої інформації сама по собі веде до постійної недовіри до громадської інформації та ЗМІ.

Можна виділити кілька видів військової діяльності, у яких використовуються соціальні мережі: збір розвідданих, таргетинг (розумна реклама), психологічна війна, наступальні та оборонні кібероперації, а також діяльність командування та управління.

Так, «Інтелектуальні агентства навчилися використовувати соціальні медіа в своїх інтересах. Використовуючи підроблені ідентифікатори, вони можуть

створити ілюзію підтримки ідей. Вони також можуть оскаржувати ідеї на платформах соціальних мереж, вставляючи зустрічні аргументи, які, як видається, виходять з низового рівня руху» [21, с. 6].

Зараз у міжнародних кризах майже будь-якого характеру можна спостерігати три додаткові явища в результаті впливу засобів масової інформації на висвітлення війни [58]: рішення приймаються швидше в рамках політичної системи; - завдяки одночасному висвітленню більшість подій у світі в різних регіонах, реалізація політичних цілей, яка виявляється неможливою або важкою; - наприклад, через емоційний вплив ЗМІ на громадську думку чи викриття таємних військових операцій, нарешті, визначення пріоритетів у рамках систем прийняття політичних рішень.

Ті, хто вивчає вплив ЗМІ, виявляють, що зміст новин відображається на політичному порядку денному. Хоча з цього короткого огляду стає очевидним, що було зроблено кілька цікавих спостережень щодо впливу ЗМІ на війну, дослідження та аналіз цього впливу на політику ЗМІ щодо ведення війни тільки починається [55, с. 207].

У зв’язку зі постійним зростанням значення самих соціальних медіа як інструменту, що використовується різними суб’єктами, висвітлення війни та вплив таких матеріалів привертають все більше уваги дослідників масової комунікації. Тому потрібен подальший аналіз ролі соціальних мереж у війні. Однак для кращого розуміння їхньої ролі в сучасній війні ще потрібно зробити багато роботи. Головною проблемою тут є відсутність загальної теоретичної «парасольки» в дослідницькій традиції, яка б дозволяла аналізувати поєднання різних методів і конкретних випадків, що використовуються в різних галузях дослідження соціальних наук.

Відповідно до демократичної точки зору, навіть під час війни соціальні медіа повинні дозволяти громадянам оцінювати війну, її легітимність чи законність, а також її наслідки з політичної точки зору, тобто брати війну під

демократичний контроль. Повна та неспотворена інформація, а також незалежне та нейтральне висвітлення подій засобами масової інформації є обов'язковою умовою демократичного устрою навіть під час війни. Лише надаючи всю доступну інформацію та ідеї, висвітлюючи та коментуючи проблеми та зосереджуючись на факторах, які можуть поставити під сумнів законність або виявити незаконність, суспільство може сформувати свої політичні уподобання, на основі яких демократ буде робити поінформовані, раціональні рішення надійнішими.

Окрім цих загальних професійних стандартів, важливі дві інші характеристики, які часто не помічаються. Через складність сучасної війни інформація, заснована на фактах, не дає достатнього розуміння проблем. Тому ЗМІ повинні прокоментувати інцидент і дати детальну оцінку.

Таким чином вони можуть зробити значущими і актуальними нові уривки інформації, що надаються журналістами в режимі реального часу, і допомогти людям орієнтуватися в ситуації. Ще одне досить просте завдання, яке є дуже важливим для залучення громадської думки до війни. Тиск на політиків, щоб діяти належним чином, лише посилюється, коли увага ЗМІ зосереджується на таких трагічних і важких подіях, як війна. Інакше ми навряд чи побачимо численні серйозні політичні ініціативи, адже багато воєн не досягають необхідного порогу для привернення уваги аудиторії ЗМІ.

Зайве говорити, що ЗМІ не можуть висвітлювати всі війни одночасно. Однак слід усвідомлювати велику відповідальність, пов'язану з вибірковістю, пов'язаною з цим станом. У багатьох випадках очікується, що засоби масової інформації сприятимуть встановленню миру — або майже автоматично через звичайне висвітлення подій, або свідомо використовуючи свій більший чи менший вплив і присвячуючи себе справі відновлення миру[1, с. 58].

Серед науковців немає консенсусу щодо того, чи просте відтворення реальних подій сприяє самому мирному процесу, чи, як це роблять деякі

прихильники миру, лише активні заклики до змін можна розглядати як внесок у справу миру. Тим більше важко відповісти на запитання, чи мають ЗМІ активно виступати за мир чи діяти лише як нейтральний літописець, бо дві універсальні цінності часто є взаємно несумісними [1, с. 59].

Що стосується миротворчого потенціалу ЗМІ, навіть дотримання професійних стандартів у висвітленні подій можна розглядати як значний внесок у рамках, визначених роллю незалежних ЗМІ як агентства, що повідомляє про загрози.

Серед таких стандартів центральне місце посідає заповідь плюралізму. Саме облік найрізноманітніших думок та точок зору закладає основу для встановлення та підтримки миру. У Декларації ЮНЕСКО 1978 р. про роль засобів масової інформації йдеться: «Справа зміцнення миру та міжнародного взаєморозуміння, розвитку прав людини і боротьби проти расизму, апартеїду та підбурювання до війни потребує вільного, ширшого і більш збалансованого поширення інформації [1, с. 59].

У цьому найважливіший внесок мають зробити засоби масової інформації. Цей внесок буде ефективнішим, якщо інформація відображатиме різні аспекти теми. Щоб зробити такий внесок, основним завданням ЗМІ під час війни має бути представлення всіх точок зору. Ця проста вимога сама по собі є дуже складним завданням у воєнний час.

У разі підривного інформаційного впливу на цільові аудиторії в Україні та інших країнах світу з боку держави-агресора Російської Федерації вживаються такі основні заходи щодо захисту національного інформаційного простору та забезпечення національної інформаційної безпеки України: по-перше, удосконалити регулювання у сфері інформаційної державної політики та нормативно-правову базу, яка визначатиме взаємодію владних структур України з органами місцевого самоврядування, державними органами та громадськими інституціями; по-друге, встановлення єдиної міжвідомчої координації орган для

керівництва, координації та контролю за заходами інформаційної безпеки (його, наприклад, можна створити у вигляді міжвідомчої комісії при РНБО); по-третє, створити комплексну систему моніторингу популярних аудіовізуальних друкованих ЗМІ та популярних Інтернет-ресурсів; по-четверте, заохочувати більш складні наукові дослідження в сфера інформаційної безпеки.

Слід зазначити, що фактично від надійності та безпеки функціонування інформаційно-телекомунікаційних мереж та інформаційних систем безпосередньо залежить сталий розвиток України та її національна безпека. У поєднанні з аналізом правозастосовної практики необхідно продовжити вдосконалення нагляду за безпекою та правового нагляду.

Як видно, роль інформаційної безпеки та її статус у системі національної безпеки також визначаються тісною взаємодією національної інформаційної політики та національної політики забезпечення національної безпеки через систему інформаційної безпеки. Важлива ланка, яка об’єднує всі основні компоненти національної політики в єдине ціле.

1.3 Проблеми інформаційної безпеки в Україні у політичній сфері

Розглядаючи питання інформаційної безпеки, важливо визначити загрози інформаційній безпеці та проаналізувати шляхи захисту від них. Загрози інформаційній безпеці — це явища з негативними характеристиками, поведінкою факторів або процесів, що призводять до: часткової або повної втрати соціальних об'єктів, на які поширюється інформаційна безпека, можливостей забезпечення інтересів осіб в інформаційній сфері; порушення нормальної життєдіяльності, знищення або обмеження розвитку технологій та інформаційних об'єктів у сфері безпеки.

Загалом виділяють такі типи інформаційних загроз: політичні, економічні, цивільні, військові та науково-технічні [47, с. 106].

У політичній сфері це: державні адміністративні системи, системи

підготовки прийняття політичних рішень, виборчі системи, приватні телекомунікаційні системи. Економіка: системи прийняття рішень, банківська інфраструктура, управління економічною ситуацією в надзвичайних ситуаціях, системи управління державними відносинами економічного характеру, корпоративні війни та промислове шпигунство [47, с.107].

Серед громадськості: загрози системі формування громадської думки, системі ЗМК, структурам політичних партій, громадських рухів, релігійних організацій, структурам забезпечення основних прав і свобод людини. У війську: військові інформаційні ресурси, системи військового управління, системи постійного контролю та спостереження, доступ до інформації стратегічного, оперативного та розвідувального характеру. Науково-технологічні аспекти: системи накопичення знань, об'єкти інтелектуальної власності, структури фундаментальних і прикладних досліджень, структури аналізу тенденцій і прогнозування в галузях науки і техніки, бази даних і конфіденційні бази даних.

Закон України «Про національну безпеку України» визначає такі загрози національним інтересам і національній безпеці України в інформаційній сфері: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність і комп'ютерний тероризм; розголошення відомостей, що становлять державну та іншу передбачену законом таємницю, а також конфіденційної інформації, яка є власністю держави або спрямована на забезпечення потреб і національних інтересів суспільства і держави; спроби маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної чи упередженої інформації [41].

Вітчизняні дослідники Бондаренко В.О. та Литвиненко О.В. у загальній системі захисту інформації виділяють такі напрями: законодавче та нормативне забезпечення, що передбачає розробку відповідних законодавчих

актів, нагляд за виконанням законодавства правоохоронними органами, судовий захист; організаційно-технічне забезпечення, яке розкриває систему заходів, спрямованих на запобігання реалізації загроз безпеці інформаційного ресурсу; страхування інформаційних ризиків, що прийнято лише для недержавних установ [6, с. 131].

Реальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є [19]:

- проведення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності країни, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування проявів екстремізму, нагнітання паніки, загострення та дезорганізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжнаціональної суперечки та міжконфесійний конфлікт в Україні;

- держава-агресор проводить спеціальні інформаційні операції в інших країнах з метою створення негативного іміджу України у світі;

- інформаційна експансія держави-агресора та її керуючих структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та інших держав;

- інформаційна перевага держави-агресора в тимчасово окупованій зоні, недостатній розвиток національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та агресивно діяти в інформаційному полі для реалізації національних інтересів України;

- неефективність державної інформаційної політики, недосконаліть законодавства щодо регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;

- поширення закликів до радикальних дій, пропаганда ізоляціоністських

та автономістських концепцій співіснування регіонів в Україні [19].

Організаційні удосконалення, спрямовані на уникнення та усунення форм і методів загроз інформаційній безпеці, передбачають: розробку нормативно-правових засад важливих напрямків діяльності системи інформаційної безпеки, розмежування повноважень органів державної влади, які мають забезпечити безпеку інформаційній сфері; розвиток системи моніторингу для аналізу стану інформаційної безпеки; розробка ідей щодо створення позитивних факторів для подолання критичного стану промисловості України у сфері інформатизації та захисту інформації; аналіз техніко-економічних показників українського та зарубіжного програмно-технічного забезпечення інформаційного забезпечення безпеки та вибір ефективних напрямів розвитку української технічного забезпечення; розробка систем даних економіко-статистичного характеру для розуміння ефективності систем у таких сферах, як забезпечення інформаційної безпеки; дослідження стандартів і методів оцінки ефективності інформаційної безпеки тощо.

Сучасна стратегія національної безпеки України серед основних загроз національній безпеці, безпосередньо пов’язаних з інформаційною сферою, визначає російські акти агресії, які спрямовані на виснаження української економіки та дестабілізацію суспільства і політики з метою знищення української держави та захоплення її території, зокрема інформаційно-психологічна війна, приниження української мови та культури, фальсифікація української історії, формування російськими засобами масової комунікації альтернативної реальності спотвореної інформаційної картини світу та інформаційна війна проти України, відсутність цілісної комунікаційної політики держави, культура недостатній рівень медіа-культури суспільства, вразливість об’єктів критичної інфраструктури, національних інформаційних ресурсів до кібератак, фізична та моральна застарілі системи захисту держави, доступ до секретної та інших видів інформації [42].

Слід зазначити, що Стратегія розмежовує прояви інформаційно-психологічної війни (п. 3.1), загрози кібербезпеці та безпеці інформаційних ресурсів (п. 3.7) від суто загроз інформаційній безпеці (п. 3.6), що є недоцільним. Доктрини інформаційної безпеки держави, а також Стратегія кібербезпеки України визначають цілий комплекс загроз для національних інтересів та національної безпеки України в інформаційній сфері [42].

При розробці стратегії забезпечення національної безпеки також необхідно враховувати, наскільки сучасні інформаційні маніпуляції впливають на суспільну свідомість. Розвідувальні та контррозвідувальні органи різних країн використовують в інформаційній боротьбі неправдиву інформацію та методи пропаганди, намагаючись отримати секретну інформацію та ввести в оману противника неправдивою інформацією. Сучасна інформаційна війна спрямована проти двох типів «мішеней»: технологічних засобів противника (комп'ютерні мережі та обладнання) та людських ресурсів. Якщо метою атаки на інформаційну систему противника є порушення критичних секторів життєзабезпечення нації – енергетики, оборони, управління тощо, то другий вид атаки спрямований на психологічну «обробку» населення [13 с. 9-10].

Таким чином, національна політика у сфері формування інформаційних ресурсів та інформатизації, безумовно, повинна бути спрямована на створення умов для ефективного та якісного інформаційного забезпечення вирішення завдань економічного та соціального розвитку країни.

Основними напрямками державної політики у сфері інформатизації є: забезпечення умов для розвитку та захисту різних форм власності на інформаційні ресурси; формування та захист державних інформаційних ресурсів; створення та розвиток державної і регіональної інформаційних систем і мереж, забезпечення, щоб вони знаходяться в єдиному інформаційному просторі; сумісність і взаємодія національних інформаційних ресурсів; створення умов для якісного та ефективного інформаційного

забезпечення громадян, органів державної влади, організацій та громадських об’єднань на основі державних інформаційних ресурсів; забезпечення національної безпеки у сфері інформатизації, а також забезпечення реалізації прав громадян і організацій в умовах інформатизації; сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем, технологій, засобів їх підтримки; формування та реалізація єдиної науково-технічної та промислової політики у сфері інформатизації з урахуванням сучасного світового рівня розвитку інформаційних технологій; підтримка проектів і програм інформатизації; створення та вдосконалення системи залучення інвестицій та механізму стимулювання розробки та реалізації проектів інформатизації; розвиток законодавства у сфері інформаційних процесів, інформатизації та захисту інформації [6, с. 17].

Протидія загрозам інформаційній безпеці нашої держави відбувається з тенденцією до переформатування сфер впливу на світовий простір під час глобалізаційних процесів, яким зазнають політичні, соціально-економічні та культурні відносини.

Виявлення та аналіз загроз може бути ускладнене низкою факторів: певна частина суспільства вважає, що в країні немає зовнішніх загроз; невпевненість щодо явної потенційної зовнішньої загрози для країни в рамках військової доктрини та доктрини інформаційної безпеки, що призводить до відсутність чіткої класифікації та ранжування загроз за важливістю та їх порівняльної динаміки зростання; відсутність усвідомлення того, чому та за яких умов виникають такі небезпеки тощо.

Механізм протидії інформаційним загрозам – це комплекс різноманітних форм роботи та взаємодії органів державного та військового управління, громадських організацій, політичних інституцій тощо, здатних оперативно впливати на загрози інформаційній безпеці або управляти ризиками, які вони викликають та їх нейтралізації [6, с. 19].

Конкретні механізми боротьби з інформаційними загрозами характеризуються формуванням реальних і потенційних загроз для системи та ймовірністю їх виникнення з урахуванням циклу розвитку системи (процесу народження, становлення, зрілості, трансформації), і її конкретний стан (криза, депресія, підйомний процес) з урахуванням наявних фінансових, матеріальних і людських можливостей країни, балансу інтересів суспільства, держави, груп, індивідів. Механізми оцінюються на основі: політики статусу інформації та її впливу на характеристики безпеки; виявлення відхилень у характеристиках стабільної роботи системи захисту інформації; визначення зовнішніх умов, які призводять до таких відхилень, наприклад: підвищення небезпеки (у несприятливе зовнішнє економічне середовище) або зменшення (за сприятливого зовнішнього середовища).

Отже, механізм реагування на загрози інформаційного характеру, заснований переважно на принципах управління ризиками, може блокувати деструктивні елементи, атрибути, процеси, що завдають шкоди системам інформаційної безпеки та національній безпеці в цілому, а також стимулювати конструктивні елементи, атрибути, процеси для покращення їх функцій і можливість розвитку.

Враховуючи, що одним із головних пріоритетів політики національної безпеки України на найближчі роки є захист інформаційної сфери, слід зазначити, що поряд із раніше відомими загрозами інформаційній безпеці (фейки, маніпуляції, спрямовані на суспільної свідомості за допомогою засобів масової інформації та соціальних мереж, залучення хакерів до вирішення політичних проблем, проведення кібератак на критичну інфраструктуру тощо), іноземні спецслужби намагаються «озброїтися» сучасними IT-рішеннями для отримання переваги в рамках міждержавного протистояння, дослідження методів цілеспрямованого інформаційного впливу на користувачів мобільних

послуг та використання їх персональних даних та технологія обробки BigData на основі штучного інтелекту.

У свою чергу, для вирішення вищезазначених проблем України в інформаційній сфері необхідно передусім реалізувати послідовну державну інформаційну політику, залучити значні кошти та зрештою змінити суспільну свідомість.

Тому Україна як держава має звернути увагу на забезпечення ефективної політики у сфері інформаційної безпеки, недопущення інформаційної залежності та блокування України, інформаційної експансії інших країн та міжнародних структур, а також інтеграції України у світовий інформаційний простір.

Безумовно, Україна має необхідні основи для створення методологічної бази інформаційної безпеки, а також науковий потенціал для успішного вирішення цієї проблеми. Однак зараз як ніколи необхідно досліджувати та вивчати не лише інформаційну політику України, а й покращувати її інформаційну безпеку. Разом нам потрібно змінити обличчя України, зробити конкретні кроки для відновлення та розвитку інформаційного середовища, привести законодавство у відповідність зі світовими стандартами, створити стабільну державу, якою б пишалися українці та яка була б надійним партнером у відносинах з іншими державами.

Висновок до Розділу 1

Отже, можна стверджувати, що інформаційна безпека є не тільки станом захищеності інформаційного середовища та ресурсів, задоволення інформаційних потреб громадян, суспільства та держави, але й захищеністю прав суб'єктів інформаційних правових відносин від негативних зовнішніх та внутрішніх факторів, що становлять загрозу конфіденційності, цілісності та доступності інформації, застосування якого сприятиме підвищенню рівня обґрунтованості державної політики інформаційної безпеки.

Найважливішими цілями забезпечення інформаційної безпеки в галузі державної та громадської безпеки є захист суверенітету, підтримання політичної та соціальної стабільності, територіальної цілісності України, забезпечення основних прав та свобод людини та громадянина, а також захист критичної інформаційної інфраструктури; у сфері стратегічної стабільності та рівноправного стратегічного партнерства необхідно сформувати стійку систему неконфліктних міждержавних відносин в інформаційному просторі.

Сталий розвиток України та її національна безпека, по суті, поставлені у пряму залежність від надійності та безпеки функціонування інформаційно-телекомунікаційних мереж та інформаційних систем. Необхідно продовжити роботу щодо вдосконалення нормативно-правового регулювання забезпечення безпеки з урахуванням аналізу правозастосовної практики.

Роль інформаційної безпеки та її місце у системі національної безпеки країни визначаються також тим, що державна інформаційна політика тісно взаємодіє з державною політикою забезпечення національної безпеки країни через систему інформаційної безпеки, де остання виступає важливою сполучною ланкою всіх основних компонентів державної політики в єдине ціле.

Україна, як держава, повинна дбати про забезпечення ефективної політики у сфері інформаційної безпеки; недопущення інформаційної залежності та

блокади України, інформаційної експансії з боку інших держав та міжнародних структур, а також інтеграцію України в світовий інформаційний простір.

Безумовно, що необхідну базу для створення методологічних основ інформаційної безпеки Україна має, є у неї і науковий потенціал для успішного вирішення цієї проблеми. Проте, нині, як ніколи, потрібно не тільки досліджувати й вивчати інформаційну політику України, а й вдосконалювати її інформаційну безпеку.

РОЗДІЛ 2. ІНФОРМАЦІЙНА ВІЙНА ТА РОЛЬ СОЦІАЛЬНИХ МЕДІА В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

2.1 Сутність та особливості інформаційної війни

На тлі стрімкого розвитку військової техніки (поява високоточної зброї, безпілотних літальних апаратів), зміни методів ведення сучасних війн (появи концепцій інформаційних війн, кібервійни та ін.), зниження ймовірності великомасштабних бойових дій — дослідники стали відзначати, що в сучасних конфліктах немає фронту і тилу в їх класичному розумінні, що внутрішні конфлікти легко перетікають в міжнародні, а також, вони вказують на хиткість межі між бойовими, миротворчими, гуманітарними, контр-терористичними операції.

Річард Шафранський вважає, що мету війни (підпорядкування противника своїй волі) в сучасних реаліях можна досягти без застосування насильства, за допомогою «знищення достатньої кількості мізків, в внаслідок чого воля помре разом з організмом» [59, с. 42].

Іншими словами Р. Шафранський вважає, що мета війни - це не знищення, а управління, а управляти можна і без насильства і кровопролиття.

У науковому середовищі на сьогоднішній день не сформовано єдиної думки щодо самого науково-теоретичного концепту інформаційних воєн, а також основних методик, форм та методів їх проведення. Порівняно недовге існування у науковому середовищі та практиці застосування інформаційних технологій як методу впливу на свідомість, поведінку та громадську думку не дозволяє вважати дослідження даного феномену вичерпаним.

Важливу роль грає також те що, що у з розвитком інформаційних технологій, як і із загальним процесом науково-технічного прогресу, ми можемо спостерігати еволюцію і запровадження принципово нових інноваційних прийомів, які у сучасних інформаційних протистояннях у сфері. Процес застосування інформаційно-комунікативних форм впливу є динамічним.

Фактично з кожним відносно невеликим відрізком часу відбувається теоретико-методологічна та структурна видозміна вже наявного інструментарію концепту інформаційних воєн.

Вперше термін «інформаційна війна» був ужитий у звіті Томаса Рона «Системи зброї та інформаційна війна», підготовленому в 1976 для компанії «Боїнг». Тоді він викликав підвищений інтерес з боку деяких експертів спецслужб США і з 1980 року почав з'являтися в документах міністерства оборони та інших аналогічних інституцій. Слід зазначити, що інформаційна війна — це поняття неоднозначне [38, с. 77].

Інформаційні війни (information warfare) — в широкому сенсі це протиборство в інформаційному середовищі та засобах масової інформації для досягнення різних політичних цілей; у вузькому сенсі це військове протиборство в інформаційній сфері з метою досягнення односторонніх переваг при зборі, обробці та використанні інформації на полі бою [46, с. 41].

Або ж у широкому значенні під інформаційною війною можна розуміти будь-який негативний інформаційний вплив на супротивника. Цим супротивником може бути держава. Таке протистояння може бути між будь-якими суб'єктами — як приватними, і публічними. Тому сторони у такій війні — фізичні особи або групи осіб, що діють в індивідуальному порядку чи організовано, спонтанно чи за згодою, юридичні особи, держави. Раніше така дія мала назву пропаганди або ідеологічної війни, але з появою Інтернету та широкого застосування електронних засобів комунікації коло учасників такого впливу, а також різноманітність його видів і форм різко збільшилися.

Такий вплив може бути спрямований і проти системи обороноздатності, закритої інформації, банківсько-фінансової системи, систем навігації — тобто проти об'єктів, що становлять національну безпеку держави. Безперечно, обмеження такого впливу та запровадження відповідальності за нього є об'єктом правового регулювання, у тому числі міжнародно-правового, однак у цій роботі

більшою мірою розглядається проблематика регулювання інформаційних воєн у вузькому значенні. У вузькому сенсі — це новий, що не укладається у міжнародно-правову кваліфікацію, вид або спосіб ведення збройних конфліктів.

З одного боку, тим самим «змащується» саме поняття «озброєний конфлікт», проте реальні наслідки інформаційної війни можуть бути істотні, призвести до значних жертв і руйнувань [46, с. 42].

Такого роду конфлікти призведуть «до проблеми визначення статусу цивільних осіб, озброєних процесором і клавіатурою і що знаходяться на іншому континенті, і контролю за їхніми діями». Цей спосіб ведення збройного конфлікту породжує самі проблеми, як і класичний конфлікт: розмежування по об'єктах і особам; кого вважати учасниками такої війни і якими ознаками повинен мати комбатант; чи є такі комбатанти об'єктом нападу традиційними видами зброї; чи отримують вони статус військовополонених і тому подібне збройного конфлікту.

Поняття «інформаційна війна» аналізується військовими, юристами, фахівцями у сфері інформаційних технологій, про неї йдеться у військових доктринах держав. Найбільш широке розуміння інформаційної війни пов'язані з її трактуванням як явного чи прихованого цілеспрямованого інформаційного впливу систем друг на друга з метою отримання певного виграшу у політичній, економічній, ідеологічній сфері [53, с. 62].

У рамках такого трактування інформаційної війни зазвичай виділяють два різні підходи. Відповідно до першого, взаємодія систем має на меті дезорганізацію системи управління, вплив на системи озброєння, включаючи інформаційні технології та інформаційні ресурси ворожих держав, та захист відповідних елементів власної інформаційної інфраструктури від аналогічних впливів.

Другий підхід є більш універсальним і передбачає вплив через різні інформаційні технології (інформаційної зброї) не тільки на військову

інфраструктуру і кадри, але і на все населення ворогуючої держави. Інформаційна зброя є нічим іншим, як алгоритмом або методикою впливу (навчання) на інформаційну систему, що самонавчається, тобто систему, що знаходиться під впливом ззовні [53, с. 63].

У разі збройного конфлікту (і його початком) може вестися інформаційна війна. За рівнями вона може включати впливу: на населення; на системи управління та озброєння; комплексний вплив. Саме третій рівень впливу у поєднанні з високою інтенсивністю дозволяє говорити про особливий вид збройного конфлікту — інформаційну війну.

Можна виділити два види інформаційних воєн: поза збройними конфліктами, назвемо їх «холодні інформаційні війни»; в умовах збройних конфліктів, або що передують збройному конфлікту (наступні за його закінченням). Безсумнівно, у крайніх формах ці види переходять один до одного, і тут напрошується аналогія зі ступенем насильства, що характеризує послідовно злочинність, стан внутрішньої напруженості, масові заворушення, збройний конфлікт. За ступенем інтенсивності інформаційна війна може містити: ідеологічний вплив; вплив на системи управління та озброєння; комплексний вплив [52, с. 327].

Китайська військова доктрина, визнаючи існування інформаційних війн, розглядає їх у широкому та вузькому значенні. У вузькому значенні – це польова інформаційна війна, тобто. — бойові дії у сфері управління військами. У широкому розумінні інформаційна війна — це бойові великомасштабні дії з переважанням інформаційної складової, що характеризуються застосуванням спеціально призначених для її ведення військових формувань та високоточної зброї.

Отже, інформаційна війна сприймається як із способів ведення бойових дій. Китайська доктрина є специфічною, але не унікальною. Багато країн світу сьогодні усвідомлюють важливість та суттєвість інформаційної складової війни,

а також нового виду зброї – інформаційної. США ще на початку 1980-х років. почали формувати стратегію ведення інформаційної війни [22, с. 39].

Франція, Німеччина, Великобританія та деякі інші держави нині активно розвивають у собі інформаційні стратегії нападу та оборони. Можна сказати, що існування інформаційної війни як виду або частини збройного конфлікту у цих країнах не викликає сумніву.

Цікавим є французький підхід до цієї проблеми. Французькі експерти дотримуються концепції інформаційної війни, що складається з двох основних елементів: військового та економічного (цивільного). Військовий елемент розглядається у контексті збройних конфліктів та миротворчих операцій, а економічний включає ширший діапазон потенційного застосування інформаційних операцій [22, с. 40].

У разі ведення «гарячих» інформаційних воєн, воєн із високим ступенем на інформаційні системи противника, виникає питання застосування міжнародного гуманітарного права. Інші позиції не настільки категоричні у запереченні інформаційної війни як виду війни та збройного конфлікту. На мою думку, незалежно від розуміння, інформаційна війна завжди повинна залишатися в рамках міжнародного гуманітарного права, а це означає, що і право Женеви, і право Гааги має застосовуватися під час інформаційної війни.

Порівняно із застосуванням інших видів зброї, організація нападу на інформаційні мережі не потребує значних матеріальних ресурсів. Хімічну або біологічну зброю називають зброєю масового ураження не через обсяг руйнівної енергії, що виділяється при їх застосуванні, а через кількість втрат і невибірливості дії, що викликаються ними. Широкомасштабне застосування звичайних озброєнь також викликає серйозні збитки. Незважаючи на природу інформаційної атаки, що не вимагає застосування значних сил, руйнування систем цифрового контролю атомної електростанції може мати настільки ж масштабні наслідки.

Важливість запобігання інформаційним атакам такого роду відчутна і безперечна. На жаль, Міжнародний Комітет Червоного Хреста поки що не виробив єдиної доктрини, яка однозначно відповідала б на всі питання, пов'язані з міжнародно-правовим регулюванням інформаційних воєн [11, с. 138].

На превеликий жаль, серйозні зміни у міжнародному гуманітарному праві наступають лише після великих жертв і тому сприйняття нового виду воєн і застосування міжнародного гуманітарного права до них можливо матиме місце тільки після широкомасштабних інформаційних воєн. Проте вже зараз необхідно зосередити увагу на використанні інформаційної зброї в конфліктах, які мають і більш традиційні форми активності сторін. Такі конфлікти, як згадувалося вище, багатьма вченими також називаються інформаційними, але вони вже припускають застосування різних видів зброї та різних стратегій.

Насамперед слід усвідомити, що застосування таких конфліктів міжнародного гуманітарного права обов'язково. Питання можуть виникнути під час застосування власне інформаційної зброї. При цьому застосовність міжнародного гуманітарного права матиме особливо важливе значення у разі застосування інформаційної зброї до об'єктів, що містять небезпечні сили природи та забезпечують життєдіяльність регіонів (атомні електростанції, греблі, системи водопостачання), до медичних об'єктів (лікарні, шпиталі, епідеміологічні центри) тощо [11, с. 139].

Норми міжнародного гуманітарного права містять пряму заборону напад на такі об'єкти, незалежно від характеру використовуваних засобів нападу — у них вказується на наслідки нападу — вивільнення небезпечних сил природи. Така заборона міститься як у Додаткових протоколах до Женевських конвенцій, так і в Гаазьких конвенціях.

Впродовж усієї війни важливе значення надається інформаційній боротьбі, де основними дієвими суб’єктами є ЗМІ та Інтернет; інформаційна боротьба, яка здійснюється протягом усієї війни, спрямована на руйнування духовного світу

націй і народів, проти яких вона ведеться; до елементів інформаційної війни належать: добування розвідувальної інформації, дезінформування, психологічні операції, напади на інформаційну структуру, зараження комп'ютерними вірусами обчислювальних мереж супротивника, а також відповідні заходи протидії для захисту власних інформаційних ресурсів [35, с. 77].

Метою інформаційної війни є «управління процесом зміни свідомості людей, їх світогляду, ставлення до суспільства і держави» [51, с.70].

Її вважають навіть не складовою війни, а окремою війною — інформаційною. Називають «війною сенсів», що вирізняється застосуванням «передових методів агітації та пропаганди» [27, с. 121].

Найбільш повно розглянув гібридну-інформаційну війну Г. Почепцов у праці «Від покемонів до гібридних війн: нові комунікативні технології XXI століття» [36, с. 83].

Слід виокремити такі визначальні риси інформаційної війни. Інформаційні операції спрямовані на:

а) масову свідомість у тактичному аспекті, коли вирішуються завдання близького плану;

б) масову свідомість у стратегічному аспекті, коли вирішується проблема досягнення цілей далекого плану;

в) структури управління, алгоритми прийняття рішень, що має за мету зміну цінності популяції.

Згідно з офіційним сайтом Сухопутних військ Сполученого Королівства основними завданнями Бригади є моніторинг та аналіз інформаційного середовища, проведення інформаційних дій, збір, створення і поширення інформаційного контенту, ведення пропагандистської діяльності.

Таким чином, незважаючи на те що документи військового планування Великобританії не розкривають зміст терміну «гібридна війна», можна зробити висновок про те, що під ним розуміється в першу чергу інформаційна війна.

У цьому контексті не можна не згадати той факт, що на тлі конфлікту в Україні та наступного протистояння між Росією та Заходом спочатку військовий теоретичний зонтичний термін інформаційна війна став активно вживатися в ЗМІ і, отже, в повсякденному житті жителів всієї земної кулі.

Інформаційна війна спрямована на дестабілізацію країни, що атакується, для чого починає підтримувати наявні контртренди у вигляді людей, ідей і ЗМІ, які можуть допомогти в справі делегітимізації влади і держави. Гібридна війна здійснює військові кроки, проте пропагандистська війна спрямована на те, щоб доводити протилежне, що ніякої війни немає [45].

Екс-заступник міністра оборони України І. Кабаненко заявив, що гібридна війна, яку веде щодо України Російська Федерація, вимагає переходу від реактивних стратегій до проактивних. Тобто, «гібридна війна побудована на промацуванні слабких місць, послідовному просуванні або одночасному за кількома напрямами, такими «хвилями», які йдуть на спад, а потім піднімаються. Розуміючи цю природу, і як це працює, можна достатньо ефективно працювати на випередження» [12].

Разом з тим, директор Українського інституту національної пам'яті Володимир В'ятрович заявив, що Кремль веде в Україні не гібридну, а «більшовицьку» війну. Події, що відбувалися на Сході України до 24 лютого 2022 року, дуже схожі на те, що відбувалося у 1918-1920 рр. «Такі події як утвердження радянської влади насправді у 1918, 1919, 1920 роках і те, що відбувається зараз – в цьому можна провести багато паралелей. Світ говорить про якийсь новий тип війни, який застосовується проти України, так звану гібридну війну, але мені здається, насправді, цей тип не новий — це типовий більшовицький тип ведення війни, який вівся проти України ще в 1918 році», — зазначив В. В'ятрович [9].

За його словами, суть цього методу полягала в тому, що «на певній території твориться якась паралельна, альтернативна влада, в Харкові на

противагу УНР твориться Раднарком Радянської України, який підтримується з Москви, створюються збройні формування, саме ці збройні формування визнаються Москвою, ведеться активна інформаційна, пропагандистська промивка місцевого населення для того, щоб його підтримувати, а потім розгортається вже безпосередня агресія — вторгнення на територію України» [9].

Деякі дослідники висловлюють думку про те, що наполягання на визначенні подій в Україні як «гібридної війни» фактично означає підтримку концепції Російської Федерації, яку вона нав'язує Україні. Гасло, що його застосовує політичне керівництво Росії, — це «допомога місцевому населенню, громадянам України в боротьбі за своє виживання» [12].

На думку доктора К. Вуйціцького з Центру студій Східної Європи Варшавського університету, те, що відбувається в Україні, можна назвати «гібридною війною». Вона полягає в тому, що сильна держава не може напасти на слабшу, тому намагається розділити її. Москва робить це, висилаючи диверсантів, мобілізуючи злочинців і проводячи інформаційну війну проти України [46].

Тому Кремль і наполягав та і зараз продовжує наполягати на тому, що він нібито не є стороною конфлікту на Сході, хоча ввів на нашу територію свою армію. Таким чином, власну агресію Росія намагається представити як миротворчу місію, в рамках якої вона рятує життя мирного населення іншої держави, що, мовляв, зазнає геноциду як від української влади, так і від частини найбільш радикально налаштованого суспільства нашої країни.

Сьогодні економісти, політики, історики досі не дійшли спільної думки відносно реальних причин розв'язування РФ агресії щодо країн-сусідів, зокрема України.

Основні версії, які розглядаються, включають такі причини:

- геополітичні амбіції Москви на лідерство в сучасному світі;

- наміри щодо захоплення нових територій, зокрема й за межами колишнього Радянського Союзу напередодні його розпаду;
- створення «осі безпеки» з огляду на розширення НАТО та розміщення елементів ПРО в Європі;
- зміщення акцентів населення Росії з внутрішніх проблем держави на зовнішні за рахунок формування образу «ворога», згуртування нації навколо міфічної ідеї «руського міра»;
- наміри щодо зменшення (погіршення) економічного потенціалу інших країн, які внаслідок потенційної зовнішньої воєнної загрози змушені значну частину свого економічного, наукового потенціалів, матеріальних і грошових ресурсів спрямовувати на зміцнення військового потенціалу;
- тиск, який змушує інші країни бути максимально лояльними до агресора, передусім у політичній та економічній сферах [46].

Не можна однозначно визначити лише одну причину. Проте все частіше експерти говорять про низку, сукупність причин, що сприяли розв'язанню РФ такого типу протистояння.

Проте очевидною є думка, що будь-яка з наведених вище причин має під собою суто економічне підґрунтя. Поточний стан світової і, зокрема, російської економіки однозначно слід вважати важким, і вийти з нього за нинішнього розкладу сил Росія не в змозі.

Тому Москві так необхідні дієві й однозначні важелі впливу на світову спільноту. Будучи протягом декількох століть сировинним придатком розвиненого світу, Російська Федерація на початку нового тисячоліття має критично неефективну економіку внаслідок низки причин, серед яких непрофесійне керівництво, технічна й технологічна відсталість, кричущий рівень внутрішньої корупції тощо.

Крім того, світ стає все менше залежним від традиційних джерел енергії, експорт яких був і залишається для РФ по суті єдиним джерелом отримання прибутків. Ті сфери, які нещодавно дозволяли Росії мати відносно диференційований «портфель» отримання доходів (металургійна, космічно-будівна сфери, торгівля зброєю), на сьогоднішній день приносять доходів все менше й менше [45].

Все це змушує керівництво країни до дій, що могли би терміново виправити ситуацію. Проте, не бажаючи розвиватися в тому напрямку, в якому рухається весь цивілізований світ, Росія, по суті, замість того щоб «тягнутися» до рівня цивілізованої світової спільноти, намагається опустити її на той рівень, на якому перебуває сама.

Отже, з розвитком технологій змінюються й умови ведення війни; звичні бойові дії заміняють інформаційні технології, і їхня складова стає все вагомішою.

Таким чином, інформаційну війну можна розглядати, по-перше, як військове протиборство або дії, що вживаються для заподіяння шкоди інформаційним системам, ресурсам тощо з метою отримання інформаційної переваги. По-друге, як інформаційно-психологічну війну, що передбачає вплив на суспільну свідомість таким чином, щоб змусити людей діяти проти своїх інтересів.

2.2 Особливості інформаційної війни як одного з елементів війни в Україні

Однією з основних функцій засобів масової інформації є пропаганда політики держав на міжнародному рівні. Військова пропаганда існує давно, але останнім часом засоби масової інформації на війні стали використовуватися більш активно та витончено. Створюються спеціальні підрозділи, що аналізують проблеми, пов'язані з передачею інформації до і після бойових операцій та подальшої перемоги. Це вважається тим більше необхідним, тому що наші

демократичні суспільства оголосили тотальну цензуру неприйнятним явищем, що швидше приносить політичні втрати, ніж військові переваги.

Військові дії на сході України є формою гібридного протистояння, тобто військовою стратегією, яка поєднує традиційну війну та кібервійну. Невід'ємною складовою такої гібридної війни є інтерпретація реальності шляхом масованого та тенденційного інформаційно-психологічного впливу, який, як правило, здійснюється своєрідною тріадою органів державної влади, аналітико-експертних структур, а також соціальних медіа [22, с. 39].

Інформаційний масив центральних органів державної влади відіграє важливу роль у формуванні громадської думки щодо сучасної ситуації на Донбасі. Можна стверджувати, що як у Росії, так і в Україні дуже часто влада вдається до використання низки інформаційно-маніпуляційних методів з метою формування консолідованої громадської думки та єдиної картинки бачення процесів, що відбуваються на Сході України з 2014 року, а також і зараз, згодом російського збройного вторгнення до нашої країни, задля подолання антагоністичних настроїв.

Основні бойові дії ведуться у соціо-культурній сфері, включаючи економіку, освіту, ЗМІ, науку, охорону природи, силові відомства, органи управління державою. Для закріплення контролю застосовуються різні методи:

1. Диверсифікація — намагання змінити громадську думку, спроби вплинути на настрої суспільства і викорінити усталені уявлення про державність та патріотизм.

Її формами є: дестабілізація обстановки в державі чи її окремих регіонах; активізація кампанії проти політичного курсу правлячої еліти держави та окремих її лідерів різними міжнародними установами; ініціювання антидемпінгових кампаній та іншого роду скандальних судових процесів, застосування міжнародних санкцій з інших причин [7, с. 39].

2. Приховування суттєвої інформації. Цей метод полягає у замовчуванні інформації, що суттєво впливає на прийняття рішення або просто цікава суспільству. Монополія цього методу належить, звісно ж, державі. У телеефірі цей метод застосовується при рекламі чудодійних ліків, про побічні ефекти рекламодавці повідомити забувають.

3. Інформаційне сміття. Цей спосіб у тому, що, якщо сховати дуже необхідну інформацію не можна, її занурюють у великий потік порожній інформації. Якщо ви не хочете, щоб людина мала доступ до якісної інформації, а приховати її не можете, засмітіть її інформаційні канали . Звідси фактичне заохочення сміття у поштових скриньках, спаму, телефонного дзвінка з рекламними пропозиціями. Сюди ж примикає велика кількість безглуздих репортажів та шоу на телебаченні [7, с. 40].

4. Зміщення понять. Цей метод у тому, що визнаний термін використовується за призначенням, та її сенс у суспільній свідомості зміщується.

5. Відволікання уваги. Цей метод полягає в тому, що увага людини, яка вибирає інформацію, привертається до незначних подій, відволікаючи її від істотних подій.

6. Пропаганда — дії, спрямовані на зміну світогляду аудиторії на користь свої держави. Одним з перших питання розвитку інформаційно-комунікаційних технологій та інформаційної війни в XX ст. почав системно досліджувати Г. Д. Лассуел (1902-1978). Він активно залучав методи соціальної психології, психоаналізу, психіатрії для дослідження політичної поведінки та пропаганди, виокремлюючи роль масових комунікацій в процесі ведення інформаційних протистоянь між провідними країнами світу. Саме Лассуел першим провів аналіз здійснення пропаганди під час Першої світової війни. Свої розробки він узагальнив у роботі «Техніка пропаганди у світовій війні» (1927 р.), де вперше було виділено інформаційно-психологічну сферу війни, а пропаганду подано як особливий вид зброї, що впливає на моральний стан ворога [25, с. 35]. Серед

основних цілей пропаганди автор визначає: збудження ненависті до ворога; підтримка дружніх відносин із союзниками; збереження добрих відносин із нейтральними країнами і, якщо можливо, намагання співпрацювати з ними; деморалізація супротивника [25, с. 38].

7. Негативна інформація отримує пріоритет над позитивною.

8. Поширення чуток.

Особливою технологією інформаційної війни. Г. Почепцов відзначає, що відсутність інформації моментально компенсується чутками. Він навіть вказує на вірогідність існування певного закону про можливості вакууму інформації: коли її не дають офіційні джерела, вона тут же з'являється в неофіційних каналах [36, с. 83].

9. Інформаційні табу. Цей метод у тому, що з деяких питань вважається забороненою за визначенням. Він відрізняється від замовчування тим, що про наявність такої інформації всім відомо, але вона приховується.

10. Провокація — яка дозволяє спонукати противника здійснити невигідні для нього дії. Провокації мають колосальний вплив вже не на інформаційне, а на збройне протистояння в Україні, вони провокують загострення, порушення тиші, руйнацію української державності. Саме тому, поняття «інформаційної війни» у контексті соціальних комунікацій потребує пильної уваги з боку науковців. Адже в епоху інформаційного суспільства кожна людина має надлегкий доступ до будь-якої інформації. Це, з одного боку, позитивне явище, оскільки провокує подальший суспільний розвиток людства, з іншого боку, несе в собі небезпеку, адже, якщо подача інформації має пропагандистську мету, то це завжди призводить до конфлікту із застосуванням зброї — саме так, як це зараз в нашій країні [34].

За поглядами фахівців НАТО ідеальної стратегією такої війни є виведення з психічної рівноваги великих мас населення противника і напрямки їх енергії проти своїх властей. Дезінформація, брехня, дезорієнтація, залякування,

підбурювання спрямовуються на те, щоб змінити соціальні установки людей, створити сильне емоційне напруження, трансформувати його в нетерпимість, непокору, саботаж, бунт, терористичні акти, спрямовані проти основ власної держави.

До таких основ відносяться влада, законність, безпеку, віра, які персоніфікуються в «носіях державності».

Порушення психічної рівноваги людей здійснюється за допомогою дискредитації носіїв державності. Останнім часом з цією метою все більш активно використовуються віртуальні соціальні мережі (групи діалогів) месенджерів (WhatsApp, Viber, Telegram, Skype, Facebook Messenger, та інші). В цьому відношенні месенджери мають ряд очевидних переваг перед іншими засобами комунікації [17, с. 26].

До числа таких переваг належать:

1. Широка можливість інформаційно-психологічного впливу (ІПВ) на населення через месенджери. Безкоштовна можливість необмежений час обмінюватися письмовою, усною, фото і відеопродукцією, синхронізація з ПК і телефонної адресному книгою робить месенджери все більш популярними засобами комунікації.

2. Потужний інформаційно-психологічний потенціал месенджерів пов'язаний, по-перше, з можливістю миттєво розсилати повідомлення великим аудиторіям, по-друге, інтеграцією можливостей всіх відомих засобів інформаційно-психологічного впливу (листівок, радіо і телемовлення, інтернету, тет-а-тет- контактів), по-третє, використання переваг текстових, фото- і відеоматеріалів.

3. Примусовий характер повідомлень, що пересилаються по віртуальним соціальних мереж месенджерів (будь-який суб'єкт, що має контакти конкретного абонента, може послати йому повідомлення).

4. Анонімність справжніх суб'єктів інформаційно-психологічного впливу.

5. Можливість реалізації схеми краудсорсингу (англ. Crowdsourcing, crowd - натовп і sourcing - використання ресурсів) в ІПВ, тобто делегування суб'єктами ІПВ своїх функції якомога більшій кількості учасників інформаційного процесу [17, с. 36].

Під час подій в Україні наприкінці 2013 — на початку 2014 р. західні ЗМІ неодноразово називали Віктора Януковича диктатором, який винищує свій народ. Наприклад, французька «Ла Монд» (Le Monde) писала у лютому 2014 р., що саме на ньому «лежить вся відповідальність за кровопролиття та втрачені людські життя» [35].

Важливим принципом ЗМІ є доступність інформації для розуміння максимально великою аудиторією. Розвиток на сайтах ЗМІ інфографіки, яку називають одним із трендів сучасної журналістики, цьому дуже сприяє. Вона лаконічна, оскільки може замінити цілу статтю; вона акцентує увагу на важливій інформації, що економить час, тому що не треба багато читати, слухати чи дивитися; вона візуально приваблива; вона наочна, оскільки, на думку психологів, інформація легко сприймається у графічному вигляді. Сьогодні, що важливо, інфографікою легко поділитися у соціальних мережах, де є обмеження щодо обсягу тексту.

У 2014–2015 рр., готуючи матеріали на теми, пов'язані із ситуацією в Україні, зарубіжні журналісти активно використовували інфографіку. Як відомо, різні кольори викликають певні асоціації, а колір відіграє в інфографіці важливу роль. Розглянемо такий приклад. У березні 2014 р. на сайті британської «Гардіан» (Guardian) було опубліковано наступну інфографіку «Росія та Україна: графік військового дисбалансу» (Russia and Ukraine: the military imbalance — graphic). Перше, що впадає у вічі (ще до того, як починаєш читати текст) — це червоно-чорний колір агресора [31, с. 92], який схематично показує зосередження різних пологів (танкові, ВПС) військ РФ біля українського кордону. Відразу йде асоціація із руйнівністю, насильством. Водночас

зосередження українських військ показано у жовто-блакитних тонах, що асоціюються зі справедливістю, спокоєм.

Відтоді, як 24 лютого Росія почала збройне вторгнення до нашої країни, світ згуртовується переважною кількістю на підтримку України. Переважна більшість міжнародного співтовариства також засудила російську агресію. Це призвело до безпрецедентних міжнародних санкцій і переконало багато найбільших компаній світу розірвати всі зв'язки з країною. Навіть колишні надійні партнери, такі як Китай, все більше не бажають публічно виступати з Кремлем [62].

Тим часом, фальшивим російським наративам більше не надається рівний безперешкодний простір у міжнародних ЗМІ. Спроби Путіна виправдати своє вторгнення не набули значної популярності. Натомість його слова про українських «неонацистів» та «наркоманів» були широко висміяні або просто відкинуті.

Однією з ключових відмінностей нинішньої війни від російського вторгнення 2014 року є наявність великої кількості міжнародних кореспондентів в Україні.Безпрецедентна присутність міжнародних ЗМІ в Україні дозволила сотням журналістів на власні очі познайомитися з реальністю країни.

Завдяки цьому надзвичайно вільному та надійному інформаційному середовищу міжнародні журналісти в Україні змогли взаємодіяти з широким колом місцевих колег, щоб скласти повну картину справжньої ситуації в країні. Ця взаємодія також допомогла підкреслити спільну професійну етику та спільні цінності, які поєднують українців та західних колег.

Оскільки в перші тижні події йшли не так, як планувалося, Росія швидко вжила заходів. Кремль обмежив діяльність іноземних ЗМІ, закрив три останні незалежні ЗМІ Росії, заборонив основні платформи соціальних мереж, створив нові закони проти журналістів, які кидають виклик його пропаганді, і наполягав на тому, щоб назвати війну «особливою військовою операцією» [62].

Результатом цього стала російська громадськість, яка майже не має доступу до будь-якої альтернативи власному антиукраїнському, антизахідному наративу Путіна.

Великий успіх нашої держави в інформаційній війні, безсумнівно, полягав у тому, щоб показати світові конфлікт, як конфлікт Росії проти не лише України, а й Заходу. Це допомогло завоювати низку шанувальників у Європі та Північній Америці, як серед політиків, так і серед звичайних виборців. Але саме той успіх, причина того, що на Заході вважають, що Україна виграє в інформаційній війні, також є причиною, чому це не так.

Кампанії з дезінформації набагато ефективніші, якщо в їх основі є потужна правда і вона використовує цю правду для ведення дискусії. Пряма реальність полягає в тому, що в багатьох частинах світу антипатія до Заходу глибока, а симпатія до Росії реальна.

Захід проголосив перемогу України в інформаційній війні. Новини на кшталт Привиду Києва та солдатів Зміїного острова, палкі промови президента України Володимира Зеленського, жахливі зображення знищення, спричиненого Росією, фотографії мільйонів українців, які тікають із своїх домівок, полонили Захід. Без сумніву, цей наратив частково несе відповідальність за поширення західних боєприпасів і військову допомогу Україні, санкції проти Росії та допомогу переміщеним українцям. Метою інформаційної війни України було завоювати симпатії та допомогу з боку Заходу, і Україна, безперечно, досягла успіху [60].

Проте інформаційна війна має не тільки західний фронт. У той час як Захід відкидає російські наративи, деякі впливові країни слухають і приймають їх.

Південь неохоче засуджує Росію за війну та протидіє її дезінформації. Сорок країн не підтримали надзвичайну резолюцію Генеральної Асамблеї ООН, яка засуджує вторгнення Росії в Україну. Білорусь, Еритрея, Північна Корея та Сирія вирішили підтримати Росію. Серед 35 тих, хто утримався, не дивно, були

Китай та Іран, а також Індія, Іран, Ірак, Пакистан, Південна Африка, Південний Судан і В'єтнам. Світ був стривожених відмовою багатьох африканських держав засудити конфлікт, що спричинило напруження у міждержавних відносинах. Загалом 17 африканських держав утрималися під час голосування на Генеральній Асамблеї ООН, а вісім були відсутні. З 28 африканських держав, які підтримали резолюцію, жодна не пояснила свою позицію, за винятком пристрасної антиколоніалістичної промови кенійського посла [60].

Президент Південної Африки Сіріал Рамафоса продовжує повторювати офіційну позицію Росії про те, що вона сприймає «національну екзистенційну загрозу» з боку НАТО, і критикував чутки про розширення НАТО в Україні. Відповідно, аналіз соціальних мереж, проведений у середині березня фірмою CASM Technology, показав, що проросійські наративи є тенденційними в мовних групах, які зустрічаються в більшій частині Південної Азії, Південної Африки, Нігерії, Пакистану та Ірану. Здається, Путін націлений на ці країни своїм посланням, щоб отримати там вплив. Виходячи з позицій їхніх лідерів, схоже, що це працює [62].

Китай, який більш жорстко контролює свій Інтернет, ніж будь-яка інша країна світу, невпинно пропагує наратив Москви. Хоча Китай офіційно може неоднозначно ставитися до своєї підтримки війни Путіна, його контрольовані державою ЗМІ оголюють свою позицію. У 2015 році Китай і Росія вирішили посилити співпрацю у сфері ЗМІ, і війна показала успіх цієї ініціативи. Через кілька годин після вторгнення Росії в Україну видання Global Times Комуністичної партії Китаю опублікувало відео, в якому йдеться про те, що велика кількість українських військових здалася, посилаючись на російську державну медіа-мережу. Після цього Державна Центральна телевізійна станція Китаю миттєво повідомила та поширила в соцмережах, що Зеленський втік з Києва.

Китайські ЗМІ повторюють позицію Росії про те, що війна протистоїть Заходу, розширенню НАТО, нацизму та фашизму, і тому є виправданою. Тим часом повідомлялося, що Україна використовує мирних жителів як живий щит і катує полонених солдатів.

Окрім цього, китайські урядовці поширили заяви Росії про те, що Пентагон фінансує біологічну зброю в Україні. Китайські урядовці повторювали теорію змови на прес-конференціях, у пресі та в офіційних акаунтах у соціальних мережах [60].

Через свої інформаційні кампанії Україна досягла важливих стратегічних і військових цілей і справедливо переконала більшість світу в своїй правді. Однак ми програли деякі важливі інформаційні баталії. Росія виграла важливі інформаційні битви в Китаї, Індії та більшій частині Африки. А оскільки інформаційна війна триватиме ще довго після припинення обстрілів, це матиме наслідки для подальших міжнародних відносин. Держави, які продовжують піддаватися російському наративу, можуть продовжувати мати напружені відносини зі США та Заходом. Оскільки США та їхні союзники по НАТО прагнуть розвивати міцніші відносини з багатими на ресурси африканськими державами — не меншою мірою, щоб зменшити залежність від Росії та Китаю, вони можуть виявити, що їм не довіряють як політичним та діловим партнерам. Російський наратив також може зашкодити довготривалим прагненням розширити міжнародну співпрацю у сфері безпеки.

Президент Володимир Зеленський щодня публікує повідомлення у соц-мережах про свої бесіди зі світовими лідерами, зазначаючи, чи погоджуються вони надіслати зброю чи надати гуманітарну допомогу, чи просто висловила солідарність. Український президент також щоденно транслює звернення до свого народу у промовах та брифінгах, покликаних підняти моральний дух та підтвердити єдність перед обличчям російського військового нападу.

Його звернення до світових лідерів на пропозицію евакуації з Києва була такою: «Мені потрібні протитанкові боєприпаси, а не втеча» та зухвала відповідь українського прикордонника, який стояв на Зміїному острові, у Чорному морі, у перший день війни, після того, як йому та його товаришам по охороні було наказано здатися: «Російський військовий корабель, іди ....», мабуть, увійдуть в історію як одні з найбільш пам'ятних фраз з війни Росії з Україною 2022 року [60].

Замість того, щоб публікувати сухі дипломатичні послання, офіційний акаунт Ukraine Twitter публікує вірусний, іноді гумористичний контент та меми з фотографіями, пояснювальними відео та підписами, оптимізованими для максимального залучення світової спільноти. Українські посли, державні службовці, журналісти, активісти та багато інших офіційних діячів розміщують у соцмережах власний контент, зокрема зображення покинутих або знищених російських танків та іншої техніки; розповіді про російські напади та очевидні військові злочини, такі як вбивство мирних жителів, зґвалтування та пограбування; страшні історії втечі від українців, які були переміщені чи стали біженцями, а також жарти, що піднімає настрій українцям.

Цифрова діяльність Києва, яку очолює 31-річний віце-прем'єр-міністр країни та міністр цифрової трансформації Михайло Федоров, також з помітним успіхом зосередився на тому, щоб спонукати компанії та глобальні корпорації призупинити чи обмежити діяльність у Росії або повністю припинити діяльність на знак протесту проти війни. Близько 500 компаній вже зробили це, включаючи технологічних гігантів, таких як Google, Facebook, Twitter та Apple.

Доктор Я. Лев'ятан, експерт з інформаційної війни з Хайфського університету, сказав The Times of Israel, що Україна фактично «здобула перевагу в інформаційній війні» [60].

Зеленський став величезною зіркою завдяки своїм чітким повідомленням, його лідерству та здатності підтримувати моральний дух і переконувати світ, що ця війна – це також їхня війна.

Як зазначила І. Менор, найуспішнішою частиною інформаційної війни України було примушування технологічних гігантів обирати та приєднуватися до однієї сторони у війні. Залишатися безстороннім неможливо [60].

Українська влада оприлюднює контент, спеціально націлений на росіян, щоб підірвати моральний дух, запускаючи групи в Telegram з інформацією про полонених або загиблих російських солдатів і гарячу лінію для стурбованих російських батьків, поширюючи історії про дезертирство військових і залишення техніки, і прямий заклик до російських матерів не допустити своїх синів до участі у війні.

Коли почали з'являтися повідомлення про те, що російські солдати були введені в оману та заздалегідь не знали про вторгнення, Україна почала зосереджуватися на кількості російських генералів, які загинули в бою, і публікувати оцінки щодо загиблих.

На кібер-фронті українських хакерів звинуватили у зломі російського веб-сайту, щоб опублікувати статтю з посиланням на російське міністерство оборони про те, що є приблизна оцінка кількості загиблих російських солдатів.

За оцінками НАТО, за перші чотири тижні війни в Україні було вбито від 7 000 до 15 000 російських солдатів, і до 40 000, як вважають, були вбиті або поранені [56].

Зеленський також прямо звернувся до російських солдатів з проханням здатися, сказавши їм в одному зі своїх звернень, що він знає, що вони «хочуть вижити», і пообіцяв, що з ними будуть добре поводитися.

У соцмережах українці зосередилися на розповідях про «героїзм і опір», наприклад, коли українку зняли на відео, яка пропонувала російським солдатам покласти в кармани насіння соняшнику, «щоб принаймні соняшники виросли, коли ви всі тут ляжете». Інша історія, — жінка збила зі свого балкона російський дрон банкою маринованих огірків.

Протягом перших тижнів вторгнення рясніли статті та дописи про те, що мирні жителі збираються разом, щоб готувати бомби — також відомі як «коктейлі Молотова» — і беруться за зброю в організаціях цивільного захисту.

Повідомлення України були зосереджені на активізації зовнішньої та внутрішньої підтримки, закликаючи людей «використовувати все, що вони можуть, щоб зупинити російські сили.

Популярними стали також відео, на яких українські аграрії буксирують російські вантажівки та танки тягачами, а також жартівливе оголошення про те, що українцям не потрібно декларувати вилучені російські танки чи БТР.

30 квітня 2022 року Голлівудська актриса Анджеліна Джолі відвідала українське місто Львів, вирушивши на вокзал, щоб зустрітися з переселенцями внаслідок війни з Росією. Джолі є спеціальним представником Агентства ООН у справах біженців, яке повідомляє, що понад 12,7 мільйона людей залишили свої домівки за два місяці війни, що становить близько 30% довоєнного населення України. Її приїзд в Україну є важливим у боротьбі за перемогу у війні з Росією, адже це привертає все більше уваги світу [54].

Підсумовуючи, варто зазначити, що оскільки збройна агресія затягується, Україна ризикує втратити перевагу в інформаційній війні через явну втому. Найбільшою загрозою для нашої країни є втрата інтересу, а це вже починає відбуватися у той час, коли відбуваються інші події у світі. Поки ця війна триває, Україна має бути в циклі новин. Саме тому, ми повинні продовжувати говорити правду — достатньо голосно, щоб світ почув.

2.3 Висвітлення війни в Україні в російських інформаційних джерелах

Відомий письменник та блогер Дмитро Бєляєв у книзі «Розруха в головах. Інформаційна війна проти Росії» звертає увагу на те, що і інформаційна війна набуває особливого значення в XXI ст. - столітті нових технологій [5, с. 113].

Основним рупором Росії є міжнародна багатомовна інформаційна телевізійна компанія RT (раніше - Russia Today), крім телеканалу існує також МІА Росія Сьогодні - інформаційне агентство, основним напрямком діяльності якого є освітлення за кордоном державної політики Російської Федерації і суспільного життя в Російської Федерації.

Sputnik - це підрозділ МІА Росія Сьогодні, яке здійснює мовлення на закордонну аудиторію.

Не можна не згадати той факт, що на тлі конфлікту в Україні та наступного протистояння між Росією та Заходом почав активно вживатися термін гібридна війна в ЗМІ і, отже, в повсякденному житті жителів всієї земної кулі.

Ось як описав російську воєнну тактику Начальник Генерального штабу Збройних сил Росії, перший заступник міністра оборони РФ генерал армії В. Герасимов на конференції в Академії військових наук у січні 2013 р.: «*Акцент сместился на использование политических, экономических, информационных, гуманитарных и других невоенных мер, наряду с применением протестного потенциала местного населения». Все это должно сопровождаться скрытыми военными операциями – например с применением методов информационной войны, задействованием сил спецназа. Открытое использование силы, часто под прикрытием миротворческой деятельности и посредничества в разрешении кризиса, может быть задействовано на финальной стадии, как правило, с целью добиться полной победы в войне*» [35, с. 77].

Як бачимо, РФ певною мірою зробила висновки із власних ганебних поразок фактично в усіх воєнних конфліктах другої половини XX ст., «відкатала» тактику у власному «бліцкригу» на території Грузії і спробувала вже на більш масштабному рівні застосувати механіку «гібридної війни» на території України. Колишній радник з безпеки при ООН і НАТО, генерал-майор у відставці Франк ван Каппен в ефірі радіо «Свобода» підтвердив, що «Путін веде в Україні гібридну війну» [45].

В подібні способи офіційна Москва намагається переконати весь світ у тому, що в Україні відбувається саме громадянська війна. Росія називала війну на Сході громадянською, а сьогоднішню війну – військовою спецопераціею, оскільки такий підхід розв'язує їй руки як агресорові.

Тим самим відбувається підміна понять, спотворення дійсності, щоб перенести відповідальність за події в Україні (передусім за воєнні дії на нашій території) на саму Україну, її керівництво. В цей час РФ, як «вовк в овечій шкірі»,

виступає нібито як миротворець, що захищає українське населення, українських громадян від «геноциду», який розв'язало керівництво України проти своїх громадян на окупованих територіях Донбасу та всій Україні.

Керівництво РФ зазначає, що вони передусім «защищают» російськомовних громадян, яких РФ вважає «соотечественниками» і яких покликана захищати, оскільки взяла на себе таку відповідальність ще з 1995 р., що закріплено в державному документі «Стратегічний курс Російської Федерації щодо країн держав-членів СНД», затвердженому колишнім президентом Б. Єльциним [12].

Безумовно, на сьогодні очевидним є факт, що гібридну війну проти України Росія розпочала не в квітні 2014 р., як нерідко прийнято вважати, а вже з 14 серпня 2013 р. [35, с. 78].

Саме того дня Росія в явочному порядку й масово стала дискримінувати український експорт на свою територію, завдаючи Україні, таким чином, значного економічного збитку, якщо враховувати, наскільки тісно обидві держави були традиційно взаємопов'язані.

Майже не викликає сумнівів, що до таких кроків керівництво Росії підштовхнула загроза можливого підписання Україною угоди про асоціацію з ЄС – замість приєднання до Митного союзу, ідеї якого активно пропагуються керівництвом РФ.

За словами доктора К. Вуйчицького з Центру східноєвропейських досліджень Варшавського університету, те, що відбувається в Україні, можна назвати «гібридною війною». Це те, що сильна держава не може напасти на слабшу, тому вона намагається її розділити. Москва робить це, посилаючи диверсантів, мобілізуючи злочинців і веде інформаційну війну проти України [35, с. 78].

Тому Москві так потрібні дієві й однозначні важелі впливу на світове співтовариство. Як сировинний придаток розвиненого світу протягом кількох століть, Російська Федерація має критично неефективну економіку на початку нового тисячоліття через низку причин, серед яких непрофесійне керівництво,

техніко-технологічна відсталість, високий рівень внутрішньої корупції та більше.

Крім того, світ стає все менш залежним від традиційних джерел енергії, експорт яких був і залишається для Росії по суті єдиним джерелом доходу. Ті сфери, які нещодавно дозволили Росії мати відносно диференційований «портфель» доходів (металургія, космос, торгівля зброєю), тепер приносять все менше і менше доходів.

Все це змушує керівництво країни вживати заходів, які могли б терміново виправити ситуацію. Однак, не бажаючи розвиватися в тому напрямку, в якому рухається весь цивілізований світ, Росія, по суті, замість того, щоб «дійти» до рівня цивілізованого світового співтовариства, намагається опустити його до того рівня, на якому вона є.

Зіткнувшись із реальністю катастрофічної поразки на інформаційному фронті, Путін відступив і тепер починає відчайдушну боротьбу, щоб захистити свою владу від внутрішньої російської аудиторії. Протягом перших десяти днів війни Москва заборонила Facebook і Twitter, закрила більшість незалежних ЗМІ, що залишилися в країні, і ввела нові закони, які обіцяють тривалі ув’язнення всім, хто наважиться поставити під сумнів партійну лінію Кремля щодо війни в Україні [62].

Результатом цього стала російська громадськість, яка майже не має доступу до будь-якої альтернативи власному антиукраїнському, антизахідному наративу Путіна.

Риторика пропагандистських шоу досить маніпулятивна, провідні агресивні, войовничі та безкомпромісні. У студії збирають експертів, що нібито має на увазі дискусію, але насправді кожен черговий спікер лише «підсилює» думку попереднього.

Якщо коротко спробувати пояснити логіку початку війни в Україні, то за версією пропагандистів вона виглядає так: вісім років тому в Україні стався державний переворот. Влада захопили нацисти, які лише пригнічували російськомовне населення. Наразі Росія прийшла звільнити Україну від цієї

хвороби — денацифікувати людей від бандерівців та галичан, дати можливість жити «нормально», не боятися висловлювати свою думку. Війну у Росії називають «спецопераційою» [37].

Телеведуча, російська пропагандистка Скабеєва в ефірі рейтингової програми «60 хвилин» на телеканалі «Росія-1» голосно кричить: *«Решение о спецоперации было трудным для Путина. Но ведь выбора не было. Потому что люди на Донбассе — не бродячие собаки и наблюдать за тем, как их уничтожают украинские нацисты, Россия больше не могла. Путин отмечал, что Россия пыталась разрешить конфликт мирно. Надо было позволить людям разговаривать на своем языке по-своему, а власти националистов устроили блокаду»* [37].

Також одним із найвпливовіших діячів кремлівської пропаганди є журналіст Володимир Соловйов. Він веде популярну політичну передачу «Вечір із Володимиром Соловйовим», щоденне політичне радіо-шоу та робить огляд робочого тижня президента. Стверджується, що Соловйов входить у близьке оточення Путіна і є одним із небагатьох, кому президент Росії дав кілька довгих інтерв'ю. Медіа-експерт Рауль Ребане назвав передачі Соловйова про Путіна «гімном культу особистості».

На своєму телеграм-каналі «Соловьев», який на сьогодні налічує більше міліонну підписників, журналіст постійно називає українську армію «неонацистами» та виправдовує дії російський солдатів, називаючи їх «освободителями». Коли російські війська стали відходити від Києва, журналіст написав «я действительно не понимаю, почему это происходит. Надеюсь, что нам это объяснят» [49].

Головним своїм ворогом пропагандисти вважають президента України Володимира Зеленського, який, за їхніми словами, сидить у бункері у Польщі. У різних програмах вони його порівнюють із Гітлером. Вони вважають, що треба говорити саме з місцевою владою. Адже росіяни нібито «не планируют оккупировать Украину, они хотят искоренить из нее национализм и фашизм». А ще — залишити на захоплених територіях свої війська, щоб люди, які стільки

років боялися висловлювати свою думку через страх бути знищеними бандерівцями, нарешті відчули себе вільними [37].

Невдовзі після початку війни, Росія або пов'язані з Росією організації, схоже, використали перший у війні діпфейк, опублікувавши кліп з «Зеленським», який говорить своїм військам складати зброю і здатися. Відео швидко розвінчали та видалили.

Росія також поширює теорії змови, які насторожують західні уряди, посилюючи теорії про те, що Росія готова застосувати хімічну зброю в Україні.

В березні у Раді Безпеки ООН Сполучені Штати звинуватили Росію у «брехні та поширенні дезінформації» в рамках потенційної операції Росії під фальшивим прапором щодо використання хімічних або біологічних агентів в Україні [61].

На зустрічі посол Росії в ООН повідомив, що у Міноборони є документи, які стверджують, що в Україні є щонайменше 30 біологічних лабораторій, які проводять «дуже небезпечні біологічні експерименти» за участю патогенів, і їхня робота «виконується, фінансується та контролюється Агентством зі зменшення загрози оборони Сполучених Штатів».

Західні країни, у свою чергу, звинуватили Росію в поширенні теорій змови та повній нісенітниці.

Як заявляє Міністр закордонних справ РФ Лавров: «*Сейчас на Западе пытаются уже не просто приравнять победителей нацизма к преступникам, а сделать из нас главных виновников той войны, и всячески обелять нацизм, поощрять нацизм уже в Европе*» [48].

За словами дослідників, інформаційні операції Росії в основному спрямовані на Індію, Китай, Африку та країни Південної Азії. На жаль, за межами Заходу російські повідомлення досі мають вплив [48].

Отже, проаналізувавши російські соціальні медіа, можна прослідкувати наявність жорсткої пропаганди, яка відбувалася протягом більше 8 років, що пояснює нам таку кількість налаштованих «за війну» громадян Росії.

Висновок до Розділу 2

Отже, на сьогодні, у зв’язку зі збройним конфліктом в нашій країні та введенням воєнного стану внаслідок російського вторгнення, питання щодо ведення інформаційної війни є особливо важливим.

У науковому середовищі на сьогоднішній день не сформовано єдиної думки щодо самого науково-теоретичного концепту інформаційних воєн, а також основних методик, форм та методів їх проведення.

Інформаційні війни (information warfare) — в широкому сенсі це протиборство в інформаційному середовищі та засобах масової інформації для досягнення різних політичних цілей; у вузькому сенсі це військове протиборство в інформаційній сфері з метою досягнення односторонніх переваг при зборі, обробці та використанні інформації на полі бою.

Крім того, інформаційну війну спочатку можна розглядати як різновид військового протистояння або дії, спрямовані на завдання шкоди інформаційним системам, ресурсам тощо з метою досягнення інформаційної переваги. По-друге, як інформаційно-психологічна війна, що передбачає вплив на громадську свідомість і примушення людей діяти всупереч власним інтересам.

Через свої інформаційні кампанії Україна досягла важливих стратегічних і військових цілей і справедливо переконала більшість світу в своїй правді.

Отже, проаналізувавши російські соціальні медіа, можна прослідкувати наявність жорсткої пропаганди, яка відбувалася протягом більше 8 років, що пояснює нам таку кількість налаштованих «за війну» громадян Росії.

Варто зазначити, що оскільки збройна агресія затягується, Україна ризикує втратити перевагу в інформаційній війні через явну втому. Найбільшою загрозою для нашої країни є втрата інтересу, а це вже починає відбуватися у той час, коли відбуваються інші події у світі.

Поки ця війна триває, Україна має бути в циклі новин. Саме тому, ми повинні продовжувати говорити правду — достатньо голосно, щоб світ її почув.

ВИСНОВКИ

Таким чином, під час написання роботи були сформульовані наступні висновки:

1. Існують різні позиції щодо трактування поняття «інформаційна безпека». Можна стверджувати, що інформаційна безпека є не тільки станом захищеності інформаційного середовища та ресурсів, задоволення інформаційних потреб громадян, суспільства та держави, але й захищеністю прав суб'єктів інформаційних правових відносин від негативних зовнішніх та внутрішніх факторів, що становлять загрозу конфіденційності, цілісності та доступності інформації, застосування якого сприятиме підвищенню рівня обґрунтованості державної політики інформаційної безпеки.

2. Роль інформаційної безпеки та її місце у системі національної безпеки країни визначаються також тим, що державна інформаційна політика тісно взаємодіє з державною політикою забезпечення національної безпеки країни через систему інформаційної безпеки, де остання виступає важливою сполучною ланкою всіх основних компонентів державної політики в єдине ціле.

Сталий розвиток України та її національна безпека, по суті, поставлені у пряму залежність від надійності та безпеки функціонування інформаційно-телекомунікаційних мереж та інформаційних систем. Необхідно продовжити роботу щодо вдосконалення нормативно-правового регулювання забезпечення безпеки з урахуванням аналізу правозастосовної практики.

3. Сучасними загрозами національним інтересам та національній безпеці України в інформаційній сфері є:

- проведення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності країни, деморалізацію особового складу Збройних Сил України та інших військових організацій, провокування проявів екстремізму, нагнітання паніки, загострення та дезорганізації суспільно-політичної та соціально-економічної ситуації, розпалювання міжнаціональної

суперечки. та міжрелігійний конфлікт;

- держава-агресор проводить спеціальні інформаційні операції в інших країнах з метою створення негативного іміджу України у світі;

- інформаційна експансія держави-агресора та її керуючих структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та інших держав;

- інформаційна перевага держави-агресора в тимчасово окупованій зоні, недостатній розвиток національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та агресивно діяти в інформаційному полі для реалізації національних інтересів України;

- національна інформаційна політика є неефективною, законодавство про нагляд за зв'язками з громадськістю в інформаційній сфері недосконале, стратегічний наратив невизначений, а культурний рівень соціальних медіа недостатній;

- широкі заклики до радикальних дій, пропагуючи концепцію ізоляціонізму та автономізму, що співіснують у різних регіонах України.

З огляду на те, що один з головних пріоритетів політики української національної безпеки найближчих років – це захист інформаційної сфери, слід зауважити, що разом із тенденцією до втілення відомих раніше загроз інформаційній безпеці (фейки, спрямоване на суспільну свідомість , маніпулювання за допомогою ЗМІ та соціальних медіа, залучання хакерів до вирішення політичних завдань, здійснення кібератак на критичну інфраструктуру та інше), спецслужби іноземних країн намагаються «озброїтися» сучасними ІТ-рішеннями, щоб отримати переваги в межах міждержавного протистояння, вивчаючи методи, покликані здійснювати цілеспрямований інформаційний вплив на користувачів мобільних послуг, використовуючи їхні персональні дані та технології обробки BigData на базі

штучного інтелекту.

У свою чергу для вирішення названих проблем України у інформаційній сфері необхідно, перш за все, впровадження послідовної державної інформаційної політики, залучення значних коштів, і зрештою певні зміни у суспільній свідомості.

Україна, як держава, повинна дбати про забезпечення ефективної політики у сфері інформаційної безпеки; недопущення інформаційної залежності та блокади України, інформаційної експансії з боку інших держав та міжнародних структур, а також інтеграцію України в світовий інформаційний простір.

Безумовно, що необхідну базу для створення методологічних основ інформаційної безпеки Україна має, є у неї і науковий потенціал для успішного вирішення цієї проблеми. Проте, нині, як ніколи, потрібно не тільки досліджувати й вивчати інформаційну політику України, а й вдосконалювати її інформаційну безпеку.

Нашому народу потрібно змінювати обличчя України, вживати конкретних заходів щодо відновлення та розбудови інформаційного середовища та приведення національного законодавства у відповідність зі світовими нормами, будувати стабільну державу, якою б пишалися українці і яка була б надійним і прогнозованим партнером у відносинах з іншими державами.

4. У науковому середовищі на сьогоднішній день не сформовано єдиної думки щодо самого науково-теоретичного концепту інформаційних воєн, а також основних методик, форм та методів їх проведення.

Інформаційні війни (information warfare) — в широкому сенсі це протиборство в інформаційному середовищі та засобах масової інформації для досягнення різних політичних цілей; у вузькому сенсі це військове протиборство в інформаційній сфері з метою досягнення односторонніх переваг при зборі, обробці та використанні інформації на полі бою.

Окрім цього, інформаційну війну можна розглядати, по-перше, як військове протиборство або дії, що вживаються для заподіяння шкоди інформаційним системам, ресурсам тощо з метою отримання інформаційної переваги. По-друге, як інформаційно-психологічну війну, що передбачає вплив на суспільну свідомість таким чином, щоб змусити людей діяти проти своїх інтересів.

5. На сьогодні, у зв'язку зі збройним конфліктом в нашій країні та введенням воєнного стану внаслідок російського вторгнення, питання щодо ведення інформаційної війни є особливо важливим.

Через свої інформаційні кампанії Україна досягла важливих стратегічних і військових цілей і справедливо переконала більшість світу в своїй правді.

Українські посли, державні службовці, журналісти, активісти та багато інших офіційних діячів розміщують у соцмережах власний контент, зокрема зображення покинутих або знищених російських танків та іншої техніки; розповіді про російські напади та очевидні військові злочини, такі як вбивство мирних жителів, зґвалтування та пограбування; страшні історії втечі від українців, які були переміщені чи стали біженцями, а також жарти, що піднімає настрій українцям.

Цифрова діяльність Києва, яку очолює 31-річний віце-прем'єр-міністр країни та міністр цифрової трансформації Михайло Федоров, також з помітним успіхом зосередився на тому, щоб спонукати компанії та глобальні корпорації призупинити чи обмежити діяльність у Росії або повністю припинити діяльність на знак протесту проти війни. Близько 500 компаній вже зробили це, включаючи технологічних гігантів, таких як Google, Facebook, Twitter та Apple.

Найуспішнішою частиною інформаційної війни України було примушування технологічних гігантів обирати та приєднуватися до однієї сторони у війні. Залишатися безстороннім неможливо.

6. Проаналізувавши російські соціальні медіа, можна прослідкувати наявність жорсткої пропаганди, яка відбувалася протягом більше 8 років, що пояснює нам таку кількість налаштованих «за війну» громадян Росії.

Варто зазначити, що оскільки війна затягується, Україна ризикує втратити перевагу в інформаційній війні через явну втому. Найбільшою загрозою для нашої країни є втрата інтересу, а це вже починає відбуватися у той час, коли відбуваються інші події. Поки ця війна триває, Україна має бути в циклі новин соціальних медіа світу. Саме тому, ми повинні продовжувати говорити правду — достатньо голосно, щоб світ почув.

Підсумовуючи, варто зазначити, що питання забезпечення інформаційної безпеки є вкрай важливими для української держави на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір України.

Зважаючи на те, що стратегічно визнаним пріоритетом зовнішньої політики України є європейська інтеграція, то завданням для української влади повинно стати розвиток ефективного діалогу з ЄС у питаннях забезпечення інформаційної безпеки.

Окрім того, потрібно детально вивчати практичний досвід зарубіжних країн, які вже мають організаційно-правову основу щодо забезпечення інформаційної безпеки та максимально використати їхній досвід у національній законотворчості та здійсненні дієвих заходів у зазначеній сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Айлдерс К. Средства массовой информации под обстрелом. Факты и вымысел в условиях войны URL: https://international-review.icrc.org/sites/default/files/reviews-pdf/2020-11/497_0.pdf (дата звернення 20.10.2022)

2. Арламов О. Ю. Безпека життєдіяльності та цивільний захист. Конспект лекцій. Київ, 2018. 93 с. URL: http://opcb.kpi.ua/wp-content/uploads/2014/09/BZDCZkonspekt.pdf (дата звернення 20.10.2022)

3. Безпека життєдіяльності та цивільний захист: підручник для студ. спеціальностей з природничих, соціально-гуманітарних наук та інженерно-комунікаційних технологій О. Г. Левченко, О. В. Землянська, Н. А. Праховнік, В. В. Зацарний; КПІ ім. Ігоря Сікорського. . Київ: КПІ ім. Ігоря Сікорського, 2019. 267 с.

4. Бєлай С.В., Корнієнко Д.М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою держави. Київ : Національна академія Служби безпеки України, 2018. 408 с.

5. Беляев Д. П. Разруха в головах. Информационная война против России. СПб. : Питер, 2014. 460 с.

6. Бондаренко В.О., Литвиненко О.В. Інформаційна безпека сучасної держави: концептуальні роздуми. Стратегічна панорама. 1999. № 1-2. С. 127-133

7. Вишняков О. Інформаційна війна з Росією: уроки виживання URL: fakty.ictv.ua/index/readblog/id/1713. (дата звернення 20.10.2022)

8. Войціховський А.В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. Журнал східноєвропейського права. 2018. № 53. С. 26–37.

9. В'ятрович В. Кремль веде в Україні не гібридну, а «більшовицьку» війну. Еспресо. URL:

http://espreso.tv/news/2014/11/29/vyatrovych_kreml_vede_v_ukrayini_ne_hibrydnu__a_quotbilshovyckuquot_viynu (дата звернення 20.10.2022)

10. Глобальна та національна безпека: підручник авт. кол. :В..І. Абрамов, Г.П. Ситник, В.Ф. Смолянюк та ін. за заг. ред. Г.П.Ситника. Київ: НАДУ, 2016. 784 с.

11. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. *Вісник НАДУ*. 2015. Вип. № 1. С. 136–141

12. Горбулін В. Гібридна війна: все тільки починається. Дзеркало тижня. 2016. URL: http://gazeta.dt.ua/internal/gibridna-viyna-vse-tilki-pochinayetsya.html. (дата звернення 20.10.2022)

13. Григор'єв В. І. Технології сучасної інформаційно-психологічної війни. Інформаційна безпека людини, суспільства, держави. 2015. № 3 (19). С. 48-52.

14. Гуржій Т. Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право. 2018. № 4. С. 16–26.

15. Гурковський В. І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки : автореф. дис. ... канд. наук з держ. управ. : спец. 25.00.02; Нац. акад. держ. управ. при Президентові України. Київ, 2004. 23 с.

16. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 2 (18). С. 16-22.

17. Дзьобань О. П. Інформаційна війна в Україні: «гра» навиживання. Безпека Сходу України в умовах гібридної війни: виклики 2019 року: матеріали Харківського безпекового форуму (м. Харків, 7-8 грудня 2018 р.). Харків: Право, 2019. С. 25-27

18. Дмитренко М.А. Проблемні питання інформаційної безпеки України. Міжнародні відносини. Серія Політичні науки. 2017. № 17. С. 236–243.

19. Доктрина інформаційної безпеки України : затверджено Указом Президента України від 25 лютого 2017 р. № 47/2017. URL:

http://zakon.rada.gov.ua/laws/show/47/2017. (дата звернення 20.10.2022)

20. Задірака В.К. Сучасні методи розв'язання задач інформаційної безпеки. Вісник НАН України. 2014. № 5. С. 65–69.

21. Захаров А.В. Массовое общество и культура: социально-типологический анализ. Вопросы философии. 2003. №9. 12 с.

22. Зінченко М.О., Плугова О.Б, Драглюк О.В. Інформаційна війна, засоби реалізації та протидії. Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. Київ : НУОУ, 2017. С. 38–40.

23. Інформаційна безпека держави: навч. посіб. для студ. спец. «Управління інформаційною безпекою», «Кібербезпека» В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея». 2018. 166 с.

24. Інформаційна безпека: питання правового регулювання: монографія А.Ю. Нашинець-Наумова. Київ: Видавничий дім «Гельветика», 2017. 168 с.

25. Інформаційна війна коштує Росії 4$ мільярди URL: www.ukrinform.ua/ukr.news/2030605 (дата звернення 20.10.2022)

26. Кравець Є. А. Інформаційна безпека держави. Юридична енциклопедія: в 6 т. К.:Укр. енцикл., 1992. 744 с.

27. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі: навч. посіб. Київ: *ВІКНУ*, 2016. 286 с.

28. Левченко Ю.О. Проблеми протидії інформаційній окупації в умовах гібридної війни. Інформаційна безпека в умовах гібридної війни: Міжнародна науково-практична конференція (м. Хмельницький, 16–17 листопада 2017 р.). Хмельницький : МВС УКРАЇНИ, 2017. 50 с.

29. Литвиненко О. Інформація і безпека. Нова політика. 1998. №1. С. 47-49.

30. Малик Я. Й. Інформаційна безпека України: стан та перспективи розвитку. Ефективність державного управління. 2015. Вип. 44(1). С. 13-20.

31. Маруненко О. Зовнішні і внутрішні інформаційні війни у медійному просторі України. Освіта регіону. Політологія, психологія, комунікації. Український науковий журнал. 2011. № 4. С. 92.

32. Наливайко Л.Р. Інформаційна безпека та інформаційна політика в Україні: конституційно-правовий аспект. Вісник Запорізького державного університету. 2003. № 1. С. 60-65.

33. Нижник Н.Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): Навч. посіб. Н.Р. Нижник, Г.П. Ситник, В.Т., В.Т. Білоус; за заг. ред. П.В. Мельника, Н.Р. Нижника. Ірпінь, 2000. 304с.

34. Парубій А. Війна Росії проти України і світу. Українська правда. URL: www.pravda.com.ua/articles/2014/08/6/7034046/ (дата звернення 20.10.2022)

35. Попович К.В. Гібридна війна як сучасний спосіб ведення війни. *Науковий вісник Ужгородського університету*, серія «Історія», вип. 2 (35), 2016. С. 75-79.

36. Почепцов Г. Від покемонів до гібридних війн: нові комунікативні технології XXI століття. Київ: ВД «Києво-Могилянська академія», 2017. 260 с.

37. «Пришли освобождать от нациков». Что на российском телевидении говорят о войне с Украиной URL: https://hromadske.ua/ru/posts/prishli-osvobozhdat-ot-nacikov-chto-na-rossijskom-televidenii-govoryat-o-vojne-s-ukrainoj (дата звернення 20.10.2022)

38. Проноза І. І. Інформаційна війна: сутність та особливості прояву URL: http://app.nuoua.od.ua/archive/61_2018/9.pdf (дата звернення 20.10.2022)

39. Про інформацію: Закон України від 02.10.1992 року. Відомості Верховної Ради України, 1992, № 48, ст.650 URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 20.10.2022)

40. Про Концепцію Національної програми інформатизації : Закон України від 04 лютого 1998 р. № 75/98-ВР. URL: http://zakon.rada. gov.ua/laws/show/75/98-%D0%B2%D1%80. (дата звернення 20.10.2022)

41. Про національну безпеку України: Закон України від 21.06. 2018. Відомості Верховної Ради, 2018, № 31, ст.241 URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення 20.10.2022)

42. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр. : Закон України від 09 січня 2007 р. № 537-V. URL: http://zakon.rada.gov.ua/laws/show/537-16?find=1&text=%E1%E5%E7%E. (дата звернення 20.10.2022)

43. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України №685/2021 URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення 20.10.2022)

44. Про Стратегію державної політики сприяння розвитку громадянського суспільства в Україні та першочергові заходи щодо її реалізації : указ Президента України від 26 травня 2015 р. № 287/2015. URL: http://zakon.rada.gov.ua/laws/show/287/2015#n14. (дата звернення 20.10.2022)

45. Путін веде в Україні гібридну війну. Радіо Свобода. 2016. URL: http://www.radiosvoboda.org/a/25363591.html (дата звернення 20.10.2022)

46. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012. *Вісник Книжкової палати*. 2013. № 1. С. 40-43

47. Соснін О.В. Інформаційна політика України: проблеми розбудови URL: http://www.niisp.gov.ua/vvdanna/panorama (дата звернення 20.10.2022)

48. Телеграм –канал «Сигнал» URL: https://t.me/ssigny (дата звернення 20.10.2022)

49. Телеграм –канал «Соловьев» URL: https://t.me/SolovievLive (дата звернення 20.10.2022)

50. Теорія управління безпекою соціальних систем : навчальний посібник. І. П. Отенко, Н. О. Москаленко, Г. Ф. Азаренков. Х. : ХНЕУ ім. С. Кузнеця, 2014. 220 с.

51. Феськов І. В. Основні методи ведення гібридної війни в сучасному інформаційному суспільстві. *Актуальні проблеми політики.* 2016. Вип. 58. С. 66-76

52. Шпига П. С. Основні технології та закономірності інформаційної війни. Проблеми міжнародних відносин. 2014. Вип. 8. С. 326-339.

53. Шумка А. В. Досвід локальних війн і збройних конфліктів другої половини XX століття у формуванні концепцій інформаційної війни. Львів: ЛВІ, 2006. 180 с.

54. Angelina Jolie visits residents at boarding school and medical institution in Ukraine URL: https://edition.cnn.com/2022/04/30/world/angelina-jolie-ukraine-lviv/index.html (дата звернення 20.10.2022)

55. Christiane Eilders/Lutz M. Hagen, «Kriegsberichterstattung als Thema kommunikationswis) senschaftlicher Forschung. Ein Uberblick zum Forschungsstand und zu den Beitragen in diesem Themenheft ,» Themenheft Medien & Kommunikationswissenschaft , 2005/2)3, pp. 205–221.

56. NATO: 7,000 to 15,000 Russian troops dead in Ukraine URL: https://apnews.com/article/russia-ukraine-zelenskyy-kyiv-europe-nato-e35e54b40359e52f3ffd4911577b669a (дата звернення 20.10.2022)

57. Oliker, Olga, Lynn E. Davis, Keith Crane, Andrew Radin, Celeste Gventer, Susanne Sondergaard, James T. Quinlivan, Stephan B. Seabrook, Jacopo Bellasio, Bryan Frederick, Andriy Bega, and Jakub P. Hlavka. Security Sector Reform in Ukraine. Santa Monica, CA: RAND Corporation, 2016. 136 p.

58. Steven Livingston, «Clarifying the CNN effect: An examination of media effects according to type of military intervention,» The Joan Shorenstein Center, Research Paper R)18, 1997

59. Szafranski R. Neocortical Warfare? The Acme of Skill. *Military review*. 1994. №11. 41-55 p.

60. Ukraine has upper hand in information war, but Russia eyes a long game URL: https://www.timesofisrael.com/ukraine-has-upper-hand-in-infowar-battle-but-russia-eyes-a-long-game/ (дата звернення 20.10.2022)

61. UN rejects Russia's allegations of US-Ukrainian biological weapons program URL: https://www.tellerreport.com/news/2022-03-11-un-rejects-russia-s-allegations-of-us-ukrainian-biological-weapons-program.HJZcWjrF-q.html (дата звернення 20.10.2022)

62. Why Vladimir Putin is losing the information war to Ukraine URL: https://www.atlanticcouncil.org/blogs/ukrainealert/why-vladimir-putin-is-losing-the-information-war-to-ukraine/ (дата звернення 20.10.2022)