Особливості забезпечення інформаційної безпеки в умовах російсько-української війни

Леонтій Чистоклетов[1], Святослав Обрембальський[2]

Опубліковано	Секція	УДК
29.05.2024	Право	32.019.51

DOI: https://doi.org/10.5281/zenodo.11381101

Анотація. У цій статті здійснено правовий аналіз забезпечення інформаційної безпеки в період російсько-української війни, її правову регламентацію, законодавче закріплення та міжнародний вплив на загальне формування в цілому.

Проаналізовано сучасні виклики для інформаційної безпеки після розв'язання країною-агресором повномасштабної війни, участь суб'єктів владних повноважень у формуванні інформаційної політики та створення більш сприятливих умов для захисту інформаційного простору у наш час.

З метою дотримання чіткого курсу на підтримку політичного розвитку у сфері інформаційних прав людини та громадянина визначено ряд нормативно-правових актів, що встановлюють основні принципи реалізації державної інформаційної політики, а також ключові напрямки, які повинна враховувати державна політика з питань захисту інформації.

Доведено, що головні інтереси повинні забезпечувати виконання політичних прав та свобод громадян для задоволення інтересів конкретної особи та суспільства загалом, зміцнення демократії, встановлення та підтримання політичної стабільності, включаючи стабільність державної влади та її інститутів. Інформаційна безпека в умовах повномасштабної російської агресії слугує міцним фундаментом для формування в Україні чітких та послідовних стратегічних завдань щодо зміцнення стійкості політичної та військової системи, забезпечення стабільності соціально-політичного розвитку в умовах російсько-українській війні.

Ключові слова: інформаційна безпека, російсько-українська війна, інформація, інформаційні технології, російська агресія.

Features of ensuring information security in the conditions of the Russian-Ukrainian war

Abstract. This article explores the importance and role of information law during the Russian-Ukrainian war, its legal regulation, legislative framework, and international influence on its formation as a whole. Modern challenges for information security are analyzed after the resolution of the full-scale war by the aggressor country, the involvement of entities with

[1] професор кафедри адміністративного та інформаційного права Навчально-наукового Інституту права, психології та інноваційної освіти Національного університету "Львівська політехніка" д.ю.н., професор
[2] студент 4-го курсу Навчально-наукового Інституту права, психології та інноваційної освіти Національного університету "Львівська політехніка"

governing powers in shaping information policy, and creating more favorable conditions for ensuring information rights in the present time.

The main points regarding a clear course towards supporting political development in the field of human and citizen information rights are identified. The primary interests should ensure the exercise of political rights and freedoms of citizens to satisfy the interests of individuals and society as a whole, strengthen democracy, and establish and maintain political stability, including the stability of state power and its institutions. Information security serves as a robust foundation for establishing clear and consistent strategic objectives in Ukraine.

Keywords: information security, russian-ukrainian war, information, information technologies, russian aggression.

Вступ

Постановка проблеми. Ретельне управління інформаційною діяльністю та ефективне застосування основних міжнародно-правових документів в умовах російської агресії можуть істотно підвищити ефективність держави в досягненні захисту інформаційної безпеки. Зокрема, застосування інформаційних технологій може розширити можливості у забезпеченні обороноздатності країни. Активне використання інформаційних технологій допомагає Україні у веденні інформаційної боротьби з росією, досягненні стратегічних цілей та забезпеченні національної безпеки.

Метою статті є дослідження особливостей забезпечення інформаційної безпеки під час російсько-української війни, визначення її проблематики та вирішення завдань щодо подолань інформаційних загроз.

Аналіз дослідження проблеми. Інформаційна безпека в державній політиці в умовах конфліктів нині все більше вивчається в роботах вітчизняних науковців. Проблема ця знаходить своє відображення у різних аспектах в публікаціях вітчизняних дослідників, серед яких можна відзначити праці К.І. Бєлякова, М.І. Дзямулич, О.Д. Добрянської, А.М. Новицького, Г.В. Онкович, Н.Б. Новицької, О.О. Пунди, Т.Ю, Ткачука, Цимбалюка, О.О. Чеботарьова, М. Швець та інших. У їх дослідженнях основний акцент робиться на аспектах правового регулювання інформаційної політики, як важливої складової механізму державного управління у сфері суспільних відносин. У зв'язку з сучасними умовами війни в Україні, викликаної агресією рф, стає необхідним пошук нових засобів регулювання інформаційної сфери, що робить дане дослідження актуальним.

Результати

Інформація є неодмінною складовою життя людини, оскільки сама людина є своєрідною сукупністю інформації. Зародження життя становить собою об'єднання генетичних інформацій. Процес зростання людини полягає в накопиченні, використанні та обміні інформацією. Увесь життєвий шлях людини, як певної частини інформаційного соціуму, є неможливим поза межами інформаційного поля. Людина є джерелом, споживачем, носієм та передавачем інформації. Проте, незважаючи на те, що інформація є невіддільна в житті людини, небагато хто задумується над її сутністю, роллю та значенням. У звичайний час під «інформацією» більшість людей розуміє отримання відомостей, доступ до даних і розуміння своїх «інформаційних прав».

Умови життя в Україні примушують переглянути наше уявлення про інформаційну безпеку. Якщо до лютого 2022 року світ навколо нас здавався безпечним, то сучасні виклики створюють набагато більше загроз, ніж у звичайні часи. Вплив російської пропаганди відчутний не лише на окремих осіб чи групи, а й на цілі нації. Психологічний вплив реалізується через засоби масової інформації, при цьому в основі цього впливу лежать перцептивні та поверхневі методи. Сучасні обставини підтверджують, що часті

інформаційні атаки, використання ботів та створення фейкових матеріалів виявляються дієвими засобами для заплутування, залякування, маніпулювання та поширення паніки серед населення. Спеціально створені джерела інформації підсвідомо впливають на сприйняття інформації, змушуючи людей вірити в неї.

Інформаційне законодавство України вважається комплексом ратифікованих міжнародних договорів, законів та підзаконних нормативно-правових актів, їхня кількість перевищує 4,5 тисячі коштом оцінки правозахисників.

Права на інформацію громадянина закріплені в Конституції України.

У частині 1 статті 34 Конституції України визначено, що «Кожен має право вільно збирати, зберігати, використовувати і розповсюджувати інформацію усно, письмово або іншим чином – за власним вибором". Однак у частині 2 вказаної статті попереджає, що "здійснення цих прав може бути обмежене законом у інтересах національної безпеки, територіальної цілісності або громадського порядку для запобігання заворушенням або злочинам, для збереження здоров'я населення, для захисту репутації або прав інших осіб, для уникнення розголошення конфіденційної інформації або для підтримання авторитету та неупередженості правосуддя» [1].

Вимоги воєнного часу змусили законодавців ввести такі обмеження, хоча теоретично питання про можливі дії обговорювалося експертами раніше. З 2014 року стали популярними дослідження особливостей інформаційних відносин у гібридній війні, при цьому частина експертів передбачала необхідність готування до широкомасштабної війни та аналізу питань інформаційної безпеки. Так, у лютому 2017 року в ефірі радіо «Свобода» в інтерв'ю з Юрієм Костюченком, аналітиком з безпекових питань, виконавчим секретарем Комітету із системного аналізу Президії НАН України на тему: «Якою має бути інформаційна політика України в умовах війни?», було відзначено, що метою суспільства в умовах війни нового типу має бути виживання, успішне подолання конфліктного стану та власний розвиток у нових умовах, а стратегія інформаційної стійкості має бути спрямована на протидію впливам, які здійснюються на суспільство в рамках інформаційних війн, що є складовими війн нового типу" [2].

Також слід відзначити ряд нормативно-правових актів, що встановлюють основні принципи реалізації державної інформаційної політики. До них відноситься Закон України «Про доступ до публічної інформації», який регулює основи опублікування та розповсюдження конкретних категорій інформації в мережі Інтернет відповідальними за інформацію, а також права користувачів на активний та пасивний доступ до інформації [3]. Закон України «Про основні засади забезпечення кібербезпеки України» націлено на визначення юридичних та організаційних основ гарантування захисту інтересів особи, громадянина, суспільства, держави та національних інтересів у кіберпросторі, а також на основні цілі, напрямки та принципи державної політики у сфері кібербезпеки України [4]. Закон України «Про боротьбу з тероризмом» визначає обмеження стосовно поширення інформації, забороняючи через засоби масової інформації або інші засоби розповсюджувати інформацію, спрямовану на пропаганду або виправдання тероризму, містить висловлювання осіб, що чинять опір чи закликають до опору проведенню антитерористичної операції та інше [5].

На рівні нормативно-правового регулювання питання здійснення державної інформаційної політики в умовах війни врегульовані у таких законодавчих актах, як: указ Президента України від 24 лютого 2022 року №64/2022 «Про введення воєнного стану в Україні» [6], указ Президента України «Про рішення Ради національної безпеки й оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» [7].

Відповідно до останнього рішення, Рада національної безпеки й оборони України (далі - РНБО) прийняла рішення визнати, що у воєнний час пріоритетним завданням

національної безпеки є впровадження єдиної інформаційної політики. Це досягається шляхом об'єднання всіх загальнонаціональних телеканалів, які основним чином транслюють інформаційні та/або аналітичні програми на єдиній інформаційній платформі стратегічних комунікацій - цілодобовому інформаційному марафоні «Єдині новини #UAразом». Окрім того, важливим є наказ Головнокомандувача Збройних Сил України від 03 березня 2022 року №73 «Про організацію взаємодії між Збройними Силами України, іншими компонентами сил оборони та представниками засобів масової інформації під час дії правового режиму воєнного стану». [8].

В контексті впровадження ключових нормативно-правових актів в законодавчу базу важливо, щоб Україна в умовах російської агресії з метою захисту національної безпеки та захисту своїх інтересів продовжувала активно вирішувати питання міжнародного співробітництва щодо запобігання та протидії загрозам інформаційній безпеки.

В умовах інформаційного суспільства усі ситуації, що виникають, включають інформаційний аспект, який часто є визначальним у конкретному контексті. Наприклад, під час військового конфлікту, окрім безпосереднього застосування збройної сили, виявляється також інформаційна складова, яка є рівноцінною зброєю як для агресора, так і для захисника території. У період воєнних дій обидві сторони активно використовують інформаційну пропагандистську зброю (у контексті атак та оборони), і в результаті цього сформувалися різні терміни, такі як «інформаційна війна», «інформаційна агресія», «інформаційна операція», «інформаційний тероризм», «інформаційне протистояння» та інші.

У війні між росією та Україною, росія використовує різноманітні інформаційні пастки та методи для досягнення своїх цілей. Ось кілька основних з них:

- *розповсюдження дезінформації та пропаганди:* росія активно застосовує стратегії дезінформації та пропаганди для впливу на громадську думку. Це охоплює поширення неправдивих новин, спотворення фактів, створення негативного враження про Україну та викривлення реальності. Російські медіа, такі як телеканали, радіостанції, вебсайт та соцмережі, є основними засобами для реалізації цих стратегій;
- *кібератаки*: росія використовує кібератаки з метою здобуття контролю над інформацією та системами в Україні. Це протиправні дії насамперед пов'язані із вторгненням у вебсайт, розповсюдженням шкідливих програм, кібершпигунством та кіберсаботажем. Кібератаки можуть призводити до перебоїв в роботі критичних інфраструктурних об'єктів, таких як енергетичні системи чи транспортні мережі, а також перешкоджати нормальному функціонуванню служб та агентств.

Використання соціальних мереж та інтернет-форумів росією для поширення пропагандистських наративів та маніпулювання громадською думкою є активною стратегією. Це включає створення фейкових акаунтів, ботів і автоматизованих систем, які ширять дезінформацію та створюють штучний образ підтримки власних позицій.

Кожен з вищезазначених термінів має конкретні аргументи та приклади, які взяті з досвіду російсько-української війни. Доведено, що задовго до відкритої агресії з боку росії, велася не тільки збройна підготовка, але й інформаційна, спрямована на психологічний вплив на населення обидвох країн. Пропаганда використовувала не інформацію, а дезінформацію, якій слід було ефективно протистояти шляхом організованої державної діяльності. Проте на той момент в Україні частина представників відповідних органів, які повинні були забезпечити належний інформаційний захист, виявилися російськими агентами, включаючи політичні сили в Верховній Раді України.

Додатково, перед повномасштабним вторгненням росія, окрім пропаганди та дезінформації, з метою впливу на зарубіжну аудиторію, часто використовувала так звану м'яку силу[3]. Наприклад, російська медична допомога Італії та Сербії під час пандемії Covid-19 може служити прикладом використання м'якої сили. Завданням було продемонструвати готовність росії допомагати та підтримувати ідею про нездатність європейських лідерів вирішити кризу в галузі охорони здоров'я, підкреслюючи важливість росії у міжнародному кризовому управлінні.

Саме ці чинники вказують на те, що протидія інформаційній агресії рф повинна включати не лише безперервне виправлення брехень та спростування фальшивих наративів, але й активне просування послідовного та позитивного дискурсу, базованого на правді та цінностях, що чітко відмежовують демократію від диктатури та демонструють привабливість проукраїнської моделі. Недостатнє реагування - це лише частина рішення, необхідні нові правила та власний проукраїнський дискурс, який, по суті, має стати частиною інформаційної війни проти рф, не лише в аспекті оборони, але й контрнаступу.

Розглянемо, які кроки вже було здійснено на другому році повномасштабної російської агресії, враховуючи парадокс: країна, на яку напали, повинна зробити більше, ніж агресор, щоб продемонструвати свою правоту.

Наразі всі ресурси України зосереджені на протистоянні ворогу, звільнення всіх територій та визначення шляхів відновлення економіки як у часи війни, так і після здобуття перемоги, а також на швидкій відбудові країни. Намагаємося не лише мінімізувати збитки та подолати руйнівні наслідки, але й класти фундамент для майбутнього, з метою забезпечити економічне зростання країни в період миру.

Основні компоненти цього фундаменту включають:

- здійснення інституційних реформ відповідно до стандартів Європи;
- інтеграція транспортної, енергетичної та соціальної інфраструктури в єдиний європейський ринок;
- створення сприятливого інвестиційного клімату для інвесторів та технологічних донорів;
- реконструкція міст на основі передових технологій дизайну та міського планування;
- оптимізація транспортних систем;
- активне відновлення соціального капіталу країни, розгляданого як здатність громадян до колективних дій для досягнення спільної мети;
- розвиток людського капіталу нового рівня, спрямованого на розширення економічних зв'язків в межах європейської економіки;
- консолідація зусиль у сфері вищої освіти для розвитку людського інтелекту та утворення партнерств з провідними зарубіжними освітніми та науковими установами [9, с. 49].

Інтеграція сучасних інформаційних технологій у бізнес-процеси на всіх рівнях при формуванні глобальної цифрової економіки відображає загальну тенденцію, що виникла перед війною [10, с. 5]. Ця тенденція обумовлена тим, що сучасні інформаційні та цифрові технології:

- дозволяють організаціям оптимізувати свої процеси, зменшити витрати та підвищити ефективність;

[3] М'яка сила (англ. *soft power* — можна перекласти *м'яка сила, м'яка влада, м'яка міць*) — концепція, розвинена Джозефом Наєм для опису можливості отримати бажане через кооптацію (співробітництво) і привабливість на відміну від «твердої сили», тобто застосування примусових заходів або прямої оплати.

- відкривають нові можливості для інновацій, такі як розробка нових технологічних продуктів і послуг, вихід на нові ринки, розроблення нових бізнес-моделей на регіональному та національному рівні;
- забезпечують перехід від аграрно-сировинної до технологічної економіки, що включає спектр ключових напрямків науково-технічного прогресу, включаючи підвищення сфери безпеки та обороноздатності, розвиток високотехнологічного сектору виробництва продукції з доданою вартістю. Це, в свою чергу, дозволяє Україні в майбутньому зробити технологічний стрибок і подолати технологічний розрив з країнами, що входять до технологічного ядра [11].

Крім того, галузь інформаційних технологій продемонструвала свою стійкість під час війни. Згідно з опитуванням провідних українських ІТ-компаній, в цьому секторі бізнесу вдалося зберегти кадровий потенціал та уникнути втрат, оскільки тут працюють близько 285 тисяч спеціалістів. ІТ-сфера швидко адаптувалася до умов воєнного стану, здійснивши релокацію персоналу та забезпечивши безперебійність робочого процесу через створення безпечних умов праці для ІТ-спеціалістів. Крім того, було вжито заходів для забезпечення постійного доступу до електроенергії та Інтернету, зокрема, використовуючи послуги Старлінку та генераторів [12].

У той самий період загальна тенденція до скорочення кадрового складу, яку відзначають світові лідери ІТ-індустрії через зменшення активного використання Інтернет-послуг, викликана нестабільністю світової економіки, також вплинула на українські компанії. У 2022 році наймання фахівців у сфері ІТ в Україні зменшилося на близько 13%, що вказує на перше зменшення кількості прийнятих на роботу протягом останніх десяти років.

Станом на 1 січня 2023 року обсяг сплати податків та зборів ІТ-бізнесом до зведеного бюджету України склав 32,2 млрд гривень, що є на 4,4 млрд гривень або 16% більше порівняно з попереднім роком. Також відзначається зростання кількості фізичних осіб-підприємців, які є платниками податків за ІТ-КВЕД [13]. Завдяки здатності утримувати темпи росту, ІТ-бізнес відіграє ключову роль у збереженні та створенні робочих місць, підтримці економіки та внесенні в військові потреби. Також він бере активну участь в реалізації гуманітарних проєктів під час війни та є стратегічно важливим у процесі національної та регіональної відбудови країни.

Щодо прогнозу для інформаційної сфери після завершення війни, можна розглядати конкретні заходи для посилення захисту державного інформаційного простору.

Як свідчить зарубіжна інформацію, російська пропаганда поки що залишається ефективною зброєю[4]. У цьому контексті Україна досліджується як об'єкт впливу такої дезінформації і як вона взаємодіє з цим явищем для власного захисту. В такому випадку, Україні слід чітко усвідомлювати свою геополітичну важливість у майбутньому, адаптуватися до можливих країн-агресорів у сфері інформаційного простору. Треба створити стійку основу, яка була б недоступною для ворожих пропагандистських впливів… Важливо розкрити справжній зміст агресивної політики росії, а також надавати методичні рекомендації з протистояння цій агресії [14].

Одним із пріоритетних завдань країни є забезпечення інформаційної безпеки, яка виступає основою національної безпеки у світлі розвитку цивілізації та інформаційних технологій. У процесі цивілізаційного прогресу інформація набуває ключового значення у веденні інформаційних конфліктів. Таким чином, інформаційна безпека означає

[4] За даними міністерства фінансів рф, з січня до березня 2022 року росія виділила на фінансування державних ЗМІ 17,4 млрд рублів (з них 11,9 млрд – під час бойових дій у березні). Це у 3,2 рази більше, ніж за аналогічний період минулого року. А до кінця року цифра може сягнути мільярда доларів США.

ступінь захищеності держави від зовнішніх загроз, її здатність ефективно протистояти інформаційним атакам і виступає важливою складовою національної безпеки.

У сучасних умовах ведення конфліктів, інформаційна зброя визнається значущим ресурсом. Таким чином, система інформаційної безпеки в Україні повинна ґрунтуватися на спільних діях державних інституцій та структур громадянського суспільства. Зростає важливість розвитку інформаційної культури суспільства як ключового елемента для захисту населення від впливу інформаційної війни, яку проводить ворог.

Отже, ключові напрямки, які повинна враховувати державна політика з питань захисту інформації, включають:

- оцінка внутрішніх і зовнішніх загроз національній інформаційній безпеці;
- впровадження та удосконалення системи моніторингу, яка охоплює спостереження, збір, обробку, збереження та аналіз інформації про стан інформаційної безпеки країни;
- підвищення рівня інформаційної культури серед населення;
- зміцнення міжнародного співробітництва у галузі інформаційних правовідносин;
- вдосконалення нормативно-правової бази, спрямованої на забезпечення національної інформаційної безпеки та стабільності.

У забезпеченні захисту інформаційної безпеки активною її складовою виступає кібербезпека. Законом України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року, кібербезпека визначається як «захищеність ключових інтересів людини та громадянина, суспільства та держави під час використання кіберпростору, що забезпечує сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, а також своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі» [4]. Погоджуючись з О. Косіловою, можна відзначити, що на сьогодні існують конкретні загрози для інформаційної безпеки, які мають міжнародний характер. До них вчена включає інформаційний тероризм, комп'ютерну злочинність, інформаційні війни, використання інформаційної зброї, маніпулювання громадською думкою та інші аспекти [15, с. 45].

Аналізуючи аспекти інформаційної безпеки України у контексті глобалізації, О. Косілова приходить до висновку, що для запобігання та нейтралізації загроз інформаційній безпеці країни важливо на рівні держави систематично розробляти та вдосконалювати нормативно-правову базу. Також слід активно підвищувати науковий потенціал у сферах інформатизації, телекомунікацій та зв'язку, а також удосконалювати систему захисту вітчизняної інформаційної інфраструктури. Важливо вдосконалювати форми та методи активної протидії інформаційно-психологічним операціям, спрямованим на позбавлення країни обороноздатності, а також моделі превентивного інформаційного впливу та захисту інформаційного суверенітету [15, с. 46].

Проводячи аналіз інформаційної безпеки та культури в сучасному інформаційному суспільстві, О. Панченко та Л. Панченко висунули авторський підхід до розуміння інформаційної безпеки. За їхньою думкою, це визначається як стан інформаційного середовища, що забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, захист інформації, а також захист суб'єктів від негативного впливу інформації [16, с. 34].

У ситуації інформаційної війни, під час якої поширюється велика кількість фейків, важливо, щоб суспільство мало відповідний рівень медіакультури та медіаграмотності. Медіакультура суспільства у науковій літературі описується як:

- «сукупність інформаційно-комунікативних засобів, матеріальних та інтелектуальних цінностей, що вироблені людством у процесі культурно-історичного розвитку» [17];

- «здатність соціуму ефективно використовувати медіа-ресурси й застосовувати передові інформаційні технології» [18];
- «сукупність інформаційно-комунікаційних засобів, що функціонують у суспільстві, знакових систем, елементів культури комунікації, пошуку, збору, виробництва і передачі інформації, а також культури її сприймання соціальними групами та соціумом у цілому. На особистісному рівні медіа-культура означає здатність людини ефективно взаємодіяти з мас-медіа, адекватно поводитися в інформаційному середовищі» [19];
- - тип або підсистема культури інформаційного суспільств, функціями якої є: інформативна; комунікативна; нормативна, або ідеологічна; релаксійна, або розважальна; креативна; інтеграційна; посередницка. Медіакультурі притаманне використання продуктів медіа в будь-якій сфері життєдіяльності, відсутність територіальних кордонів, одночасний синтез сприйняття усіма органами чуття, формування принципово іншого типу мислення, інтерактивного сприйняття та принципово інші взаємини автора і читача, виробника і споживача» [20].

З метою опанування навиків медіаграмотності громадянам слід навчатися не панікувати перед перевіркою інформації, розрізняти правду від брехні та розпізнавати ботів у соціальних мережах. Для досягнення цієї мети повинні активно працювати державні органи, освітні заклади, журналісти, громадські організації та інші. Наприклад, під час ракетного удару по житловому будинку в Одесі, який призвів до загибелі вісьмох людей та поранення вісімнадцятьох, російські агресори намагалися уникнути відповідальності за цю трагедію, спочатку розповсюджуючи фейк про атаку на військовий об'єкт. Після викриття цього фейку атака зухвало перетворилася на напад на нафтобазу. Однак подальша публікація фотографій з місця події розкрила цю брехню.

Згодом, російські пропагандисти придумали новий фейк, що житловий будинок став жертвою українських протиповітряних ракет. Але цей ворожий фейк також був спростований фотографією будинку з характерними пошкодженнями від ракетних ударів. Подібні фейки кремлівською пропагандою також використовувалися після терористичних атак у Харкові, Києві, Вінниці, Кременчуці, Дніпрі та інших містах.

Для того, щоб ворожа брехня не впливала негативно на населення, важливо ретельно викривати всі фейки, які запускаються в український інформаційний простір. Це дозволить громадянам отримувати не лише правдиву інформацію, але і відчувати підтримку від влади, яка тісно взаємодіє з ними.

Як ми вже зазначали, істинність є основним інструментом протистояння ворожим фейкам, і цю правду перевіряють і розповсюджують журналісти. Керівник відділу ЮНЕСКО зі свободи висловлення та безпеки журналістів, Гільєрмо Канела, визначив мужність українських журналістів, які, ризикуючи своїм життям, освітлюють події війни: «Наша головна мета - висловлення солідарності тим професіоналам, які висвітлюють жахіття, що коїть росія у вашій державі. Такою акцією ми хочемо захистити вас. Через символічне «журналістське віконце» весь світ має змогу бачити біль, через який проходить Україна через російську окупацію» [21]. Журналісти в свою чергу розповіли про труднощі, з якими їм доводилося зіткнутися, такі як викрадення, втрата обладнання, фінансові труднощі та інші.

За даними Моніторингу російських злочинів проти журналістів та медіа, що здійснює Інститут масової інформації, «за два роки та два місяці з початку повномасштабного вторгнення Росія скоїла 589 злочинів проти журналістів та медіа в Україні. З них: вбито – 76 (10 – загинуло під час виконання редакційного завдання); 14 – зникло безвісті; 25 – викрадено; 34 – поранено; 19 – обстрілів телевеж; 42 – обстрілів журналістів; 19 – захоплень та нападів на редакції медіа; 29 – вимкнень українського

радіомовлення та трансляція російської пропаганди; 69 – переслідування журналістів, погроз, залякувань; 78 – кіберзлочинів [22].

З кінця березня Інститут масової інформації (IMI) реєстрував отримання погроз на електронні адреси редакцій українських медіа та журналістів. Листи-погрози надходили з російської пошти mail.ru та підписувалися різними користувачами. У листах погрожували журналістам допитами, тортурами, ув'язненням, а пізніше почали надсилати навіть віршовані загрози. Ці листи отримали редакції «Європейської правди», «Главкому», «Апострофу», «Крим.Реалії», а також декілька волинських та запорізьких медіа.

Зважаючи на те, що гарантування доступу до інформації визнається одним із ключових прав особистості, українські владні структури повинні забезпечити безперешкодний доступ до неї. В такому випадку в умовах російської агресії сама влада стає отримувачем вигод, оскільки правдива інформація сприяє збільшенню довіри українського суспільства та світової спільноти до неї. Особисті інтереси в інформаційній сфері містять реалізацію конституційних прав людини та громадянина на отримання в законний спосіб інформації, використання інформації для розвитку фізичної, духовної та інтелектуальної сфер життя, а також захист інформації, яка гарантує особисту безпеку.

Особливо актуальним на сьогодення є зміцнення ефективної системи стратегічних комунікацій, яке призначене для забезпечення ефективної інформаційної взаємодії між органами державної влади, місцевим самоврядуванням і суспільством у кризових ситуаціях та для зміцнення позитивного іміджу України. Згідно з Доктриною НАТО, стратегічні комунікації розглядаються як «скоординоване і відповідне використання комунікативних можливостей НАТО: публічної дипломатії, зв’язків з громадськістю, PR-служби збройних сил, інформаційних і психологічних операцій для підтримки політики Альянсу та заходів, спрямованих на досягнення цілей НАТО. Стратегічну комунікацію, за словами колишнього речника Міністерства оборони США Роберта Гастінгса-мол., можна визначити як «синхронізацію образів, дій та слів для досягнення бажаного ефекту» [23].

Отже, якщо говорити про стратегічні комунікації як систему внутрішніх і зовнішніх комунікацій, то важливим елементом цієї системи є зв’язки з громадськістю. На наш погляд, в умовах війни органи публічної влади проявляють високий рівень інформаційної взаємодії із суспільством. Достовірні та чіткі виступи Президента України перед парламентами іноземних держав та міжнародними організаціями, інформація від центральних органів публічного управління, голів обласних військових адміністрацій, спрямовані на висвітлення поточної ситуації у російській агресії та надання звітів про свою діяльність, стали актуальними та бажаними для громадян.

Щодо створення іміджу України у російській агресії, як сфери впливу зовнішніх комунікацій, слід зазначити, що зміцнення позитивного іміджу України є необхідним з урахуванням його впливу на міжнародний, політичний, економічний та культурний розвиток країни. Оскільки успішність у зміцненні іміджу держави залежить від ефективності відповідної інформаційної діяльності, особлива роль у цьому спрямуванні повинна надаватися органам публічного управління, що відповідають за зв’язки з громадськістю, засобами масової інформації та іншими структурами громадянського суспільства.

Висновки

Події в ході російсько-української війни викликали загострення та прискорення процесів формування державної інформаційної політики. В рамках інформаційної політики під час війни застосовуються комплекс заходів нормативно-правового, організаційного, контрольного та іншого характеру. Ці заходи спрямовані на

забезпечення дотримання принципів свободи засобів масової інформації та забезпечення балансу між інтересами суспільства та держави в умовах збройної російської агресії.

Загалом слід відзначити, що підвищення рівня вірогідності та надійності інформації, ефективне використання інформаційних ресурсів під час війни, а також оптимальне використання зовнішніх та внутрішніх інформаційних каналів сприяють покращенню якості публічних управлінських рішень. Це, загалом, зміцнює стійкість політичної та військової системи, забезпечує стабільність соціально-політичного розвитку в умовах російської агресії та сприяє перемозі України на полі бою.

Отже, інформаційна безпека в контексті російсько-української війни виступає як важлива складова національної безпеки та міжнародного правопорядку. Подальші дослідження та вдосконалення законодавства в цій сфері є необхідними для ефективної протидії сучасним російським загрозам та забезпечення стабільності у вітчизняному інформаційному просторі.

Список використаних джерел

1. Конституція України: Основний Закон України від 28 червня 1996 р. № 254к/96-ВР.URL:https://zakon.rada.gov.ua/laws/ show/ 254%D0%BA/ 96- % D0%B2%D1%80#Text.
2. Штогрін І. Якою має бути інформаційна політика України в умовах війни? 28 лютого 2017. URL: https://www. radiosvoboda.org/a/28338927.html
3. Про доступ до публічної інформації : Закон України від 13 січня 2011 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19/.
5. Про боротьбу з тероризмом : Закон України від 20 березня 2003 р. № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15.
6. Про введення воєнного стану в Україні : Указ Президента України від 24 лютого 2022 року №64/2022 URL: https://www.president.gov.ua/documents/642022-41397/.
7. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України URL: https://www.president.gov.ua/documents/1522022-41761.
8. Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану : Наказ Головнокомандувача Збройних Сил України від 03 березня 2022 року №73. URL.https://www.mil.gov.ua/content/mou_orders/nakaz_73_050322.pdf?fbclid=IwAR3BFiXuFblkYZgRCWVYGHffTJhtmhBbQXAEVE7KZMR00Q_i6gz SslnkFg.
9. Сіденко С.В. Пріоритети й чинники інноваційної політики: досвід окремих країн Східної Азії і стратегічні імперативи для післявоєнної відбудови України. Економіка України. 2022. № 11. С. 47–75.
10. Дзямулич М.І., Шматковська Т.О. Вплив сучасних інформаційних систем і технологій на формування цифрової економіки. Економічний форум. 2022. № 2. С. 3–8.
11. Чеботарьов О.О. Формування інноваційних пріоритетів в системі виробничого менеджменту в умовах цифровізації. Ефективна економіка. 2023. № 3. URL: https://nayka.com.ua/index. php/ee/article/view/1316/1326.
12. Некрасов В. ІТ-галузь допоможе Україні вистояти у війні: опитування найбільших гравців. URL: https://www.epravda.com. ua/publications/2022/03/18/684265/.

13. Оновлені дані: IT – єдина експортна галузь в Україні, що зростає. URL: https://itukraine.org.ua/.
14. Ткаченко О. «Інформаційний Рамштайн» – початок єдиного інформаційного фронту країн-союзників» URL: http://surl.li/mnhep.
15. Косілова О. І. Інформаційна безпека України в умовах глобалізації. Правова інформатика. 2010. No 3(27). С.22–28.
16. Панченко О. А., Панченко Л. В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві. Правова інформатика. 2015. No 2(46). С.32–38.
17. Масол Л.М. Медіа-культура / Масол Людмила Михайлівна // Енциклопедія освіти /Акад. пед. наук України; головний ред. В.Г.Кремень. К.: Юнірком Інтер, 2008. 1040 с.
18. Онкович Г.В. Медіалогія та її складові / Онкович Ганна Володимирівна. 2009. URL: franko.lviv.ua.
19. Концепція впровадження медіа-освіти в Україні / Схвалено постановою Президії Національної академії педагогічних наук України 20 травня 2010 року, протокол № 1-7/6-150. URL: telekritika.uaю.
20. Лисинюк М.В., Голобородько О.О. Медіакультура: сутнісні особливості і функції. URL: http://issues-culture-knukim.pp.ua/article/ view/221042/221508.
21. В Україну передали засоби захисту для українських ЗМІ. URL: https://chasdiy.org/society/v-ukrainu-peredaly-zasoby-zakhystu-dlia-ukrainskykh-zmi-foto.html
22. 589 злочинів скоїла рф проти медіа та журналістів за два роки й два місяці повномасштабної війни. URL: https://imi.org.ua/monitorings/589-zlochyniv-vchynyla-rf-proty-media-ta-zhurnalistiv-za-dva-roky-i-dva-misyatsi-povnomasshtabnoyi-i60890.
23. Сутність явища «стратегічні комунікації». https://er.nau.edu.ua/bitstream/NAU/53949/5/05_%D0%A1% D0% A2%D0%9A_%D0%9B.pdf.