Сергєєва Д. Б.,
доктор юридичних наук, професор,
заслужений юрист України,
професор кафедри кримінального процесу та криміналістики
Навчально-наукового інституту права
Київського національного університету імені Тараса Шевченка,
адвокат
***ORCID ID**: 0000-0003-1005-7046*

Черниш Р. Ф.,
кандидат юридичних наук, доцент,
Національна академія Служби безпеки України
***ORCID ID:** 0000-0003-4176-7569*

DOI: *https://doi.org/10.17721/2413-5372.2022.3-4/148-157*

УДК 321.7:070.1

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ГЛОБАЛІЗАЦІЇ

«Колись інформація була нашою здобиччю,
тепер ми здобич інформації»
Ліна Костенко

Анотація. *У статті констатовано, що Україна стала об'єктом інформаційно-психологічних впливів, які реалізуються в ході відповідних операцій, внаслідок чого її інформаційна безпека опинилась під загрозою.*

Зазначено, що актуальність проблематики забезпечення державної безпеки України в інформаційній сфері зумовлена антиукраїнськими впливами, які пропагують ідеї сепаратизму, національної ворожнечі, насильства, що створює передумови до знищення національної ідентичності України та міжнаціональної злагоди, посягання на конституційний лад і територіальну цілісність держави у цілому.

*Зважаючи на викладене, **метою статті** є вироблення пропозицій щодо оптимізації шляхів забезпечення інформаційної безпеки України в умовах глобалізації.*

Виділено основні напрямки заходів щодо захисту національного інформаційного простору та забезпечення національної системи інформаційної безпеки України з врахуванням руйнівного інформаційного впливу країни-агресора на цільову аудиторію держави.

Стверджується, що зважаючи на динаміку розвитку суспільних відносин в інформаційній сфері, беручи до уваги необхідність реалізації ефективних заходів із протидії сучасним загрозам інформаційній безпеці, потребують удосконалення форми і методи захисту інформації, критичної інформаційної інфраструктури та інформаційно-психологічної безпеки громадян всіма без винятку європейськими країнами.

У заключній частині дослідження сформульовано пріоритетні заходи із забезпечення інформаційної безпеки України в умовах глобалізації.

Ключові слова: *інформаційна безпека, інформаційна війна, мережа Інтернет, глобалізація, забезпечення інформаційної безпеки.*

Постановка проблеми. Загальна оцінка проблем інформаційної безпеки, забезпечення безпеки телекомунікацій та протидія кіберзлочинності[1] є ключовими напрямками забезпечення національної безпеки України у контексті зміцнення міжнародної безпеки в умовах глобалізації. Світові процеси глобалізації, формування інформаційного співтовариства, впровадження нових інформаційних технологій підсилюють важливість такої складової національної безпеки держави, як інформаційна безпека, що характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх і внутрішніх загроз[2]. Щоб вистояти в таких умовах перед дезінформацією та маніпуляціями, які вміло застосовують, насамперед, російські ЗМІ, яка розповсюджується за допомогою соцмереж та інших комунікаційних каналів, кожній державі необхідна консолідація, довіра до влади, а з боку держави – широкомасштабна інформаційна політика швидкого реагування із застосуванням сучасних технологій. При цьому громадяни повинні правильно фільтрувати інформацію, критично мислити, аналізувати, звертати увагу на джерела інформації, власників медіа, оскільки в міру збільшення усвідомлення маніпуляція зменшується[3].

Аналіз останніх наукових досліджень та публікацій. Окремі аспекти окресленої проблематики досліджували такі науковці і практики як: П. Волошин, М. Гаврильців, М. Галамба, В. Горбулін, О. Довгань, І. Доронін, У. Ільницька, О. Зозуля, У. Коруц, О. Курбан, В. Ліпкан, Н. Марута, О. Мороз, А. Марущак, В. Пилипчук, М. Погорецький, В. Полевий, Г. Почепцов, Т. Ткачук та інші. Однак, багато з них продовжують залишатися дискусійними й потребують подальшої наукової розробки та реалізації як до законодавства так й у правозастосовну практику. Одним із таких є питання щодо вироблення пропозицій щодо оптимізації шляхів забезпечення інформаційної безпеки держави в умовах глобалізації, що і є **метою цієї статті**.

Виклад матеріалу дослідження та його основні результати. В інформаційній сфері слід виділити проблемні питання, які проявляються в умовах глобалізації. Зокрема: інформаційно-психологічний вплив індивідуальної та масової спрямованості; обмеження доступу споживачів до послуг, заснованих на інформаційно-телекомунікаційних технологіях; кіберзлочинність тощо.

Реалії сьогодення свідчать, що Україна стала об'єктом інформаційно-психологічних впливів, операцій, війн внаслідок чого її інформаційна безпека опинилась під загрозою. Підтримуємо думку У. Ільницької про те, що: український інформаційний простір є незахищеним від зовнішніх негативних пропагандистсько-маніпулятивних впливів і стає об'єктом інформаційної експансії; у світовому медіапросторі відсутній український національний інформаційний продукт, що поширював би об'єктивну, неупереджену та актуальну інформацію про події в Україні. Як наслідок – світова громадськість відчуває брак інформації або отримує її з інших джерел, які часом дезінформують, надають викривлену, спотворену, неповну інформацію. Водночас проти України активно застосовується потужний медіа-ресурс, здійснюється експансія іноземних суб'єктів на ринку інформаційних послуг, активізуються негативні інформаційні впливи, спрямовані на викривлення реальності, заниження міжнародного іміджу держави; діяльність вітчизняних ЗМІ щодо систематичного,

[1] M Pohoretskyi, A Cherniak, D Serhieieva, R Chernysh & Z Toporetska (2022) 11 (53) Detection and proof of cybercrime *Amazonia Investiga* 259–269.

[2] Характеристика становища інформаційної безпеки України. <https://vuzlit.com/1137657/harakteristika _ stanovischa_informatsiynoyi_bezpeki_ukrayini> дата звернення 01.12.2022.

[3] О Зозуля, Фейк як інструмент інформаційної війни. Юридична газета – онлайн версія <https://yur-gazeta.com/publications/practice/inshe/feyk-yak-instrument-informaciynoyi-viyni.html> дата звернення 01.12.2022.

об'єктивного висвітлення фактів, подій та явищ є недостатньо ефективною та позбавлена стратегічного планування; інформаційно-комунікативна політика України у сфері національної безпеки потребує невідкладного перегляду та удосконалення[1].

Актуальність проблематики забезпечення державної безпеки України в інформаційній сфері зумовлена антиукраїнськими впливами, які пропагують ідеї сепаратизму, національної ворожнечі, насильства, що створює передумови до знищення національної ідентичності України та міжнаціональної злагоди, посягання на конституційний лад і територіальну цілісність держави у цілому.

Враховуючи руйнівний інформаційний вплив країни-агресора на цільову аудиторію України та інших країн, можна виділити такі основні напрямки заходів щодо захисту національного інформаційного простору та забезпечення національної системи інформаційної безпеки України:

– удосконалення правового регулювання в галузі інформаційної державної політики, яке визначало б взаємодію спеціальних служб та правоохоронних органів України з органами місцевого самоврядування, іншими державними органами та установами;

– створення єдиного міжвідомчого координаційного органу, який би керував, координував і контролював заходи інформаційної безпеки, наприклад, його можна створити як міжвідомчу комісію при РНБО України;

– розробити систему всебічного моніторингу популярних аудіовізуальних і друкованих ЗМІ, а також популярних Інтернет-ресурсів;

– заохочувати подальші комплексні дослідження у галузі інформаційної безпеки[2].

У процесі забезпечення державної безпеки України в інформаційній сфері П. Волошин та Н. Марута звертають увагу на необхідність запобігання погіршенню психічного здоров'я і психологічного благополуччя численних верств населення, яке потребує системної спеціалізованої медико-психологічної допомоги[3]. Таке погіршення стало результатом негативного впливу на суспільство загроз інформаційній та національній безпеці з боку рф. Україна дедалі частіше стає об'єктом інформаційної агресії, а тому пропаганда війни як один із її елементів спричинила подібні негативні наслідки. Ця точка зору підтверджується у працях О. Олішевського, який відмічає, що інформаційні загрози та пропаганда війни впливають, в першу чергу, на свідомість і психологічний стан людини, але їх наслідки є значно системнішими[4]. Вочевидь, йдеться про те, що, впливаючи негативним чином на свідомість людини та на суспільну свідомість у цілому засобами пропаганди війни, відбувається деформація суспільного сприйняття ролі держави, зростання стійкого переконання неспроможності держави захистити власний суверенітет та забезпечити національну безпеку та безпекове середовище. Це призводить до нових форм реалізації злочинної діяльності з пропаганди війни, яка, трансформуючись, може зберігати цілі та засоби, але зміст діяльності виходить за межі можливостей її кваліфікації як кримінально-караного діяння. У такому випадку явно протиправна та суспільно небезпечна діяльність ви-

[1] У Ільницька Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам (2016) 2 (1) *Політичні науки* <http://science.lp. edu.ua/sites/default/files/Papers/ilnicka_0.pdf> дата звернення 01.12.2022.

[2] М Гаврильців, Інформаційна безпека держави в системі національної безпеки України (2020) 2 *Юридичний науковий електронний журнал* 200–203 <http://lsej.org.ua/2_2020/54.pdf> дата звернення 01.12.2022.

[3] П Волошин, Н Марута, Стратегія охорони психічного здоров'я населення України: сучасні можливості та перешкоди (2015) 23 (1) *Український вісник психоневрології* 5–11 <http://nbuv.gov.ua/UJRN/Uvp_2015_23_1_3.f> дата звернення 01.12.2022.

[4] О Олішевський, Заходи протидії пропаганді війни в Україні (2018) 1 (1) *Национальный юридический журнал: теория и практика* 155–160.

падає за межі можливостей кримінального переслідування[1].

Одним з основоположних напрямків забезпечення глобальної інформаційної безпеки є підготовка і прийняття міжнародно-правових актів, спрямованих на усунення термінологічної невизначеності в сфері інформаційної безпеки. При цьому важливим елементом є визначення міжнародно-правового статусу інформаційного та кіберпростору, а також нормативно-правове закріплення юрисдикції держав щодо національних складових цього простору (за аналогією з повітряним, водним простором держав) і подальшим врегулюванням питань, пов'язаних з кібервійною, кіберагресіями, тощо. Ключовим напрямком нормотворчої діяльності у цій сфері є також впровадження уніфікованого поняття «кіберзлочинності», а також чіткої систематизації відповідних діянь[2,3]. Інші можливі заходи, які могли б бути прийняті міжнародним співтовариством для зміцнення інформаційної безпеки на глобальному рівні, можуть включати гармонізацію нормативно-правової бази в сфері захисту інформації, розробку узгоджених критеріїв і методів оцінки ефективності систем і засобів забезпечення інформаційної безпеки, взаємне визнання сертифікатів продукції в сфері захисту інформації, розширення взаємодії при вирішенні науково-технічних і правових питань забезпечення безпеки інформації. При цьому зміцнення взаємодії правоохоронних органів держав щодо запобігання комп'ютерним злочинам, застосування юридичної відповідальності є необхідною умовою успішної взаємодії на даному напрямку. Правове регулювання формування єдиного інформаційного простору України має сприяти гармонійному розвитку інформаційних ресурсів, інформаційних послуг та інформаційного продукту в країні. Важливість проблеми розвитку законодавства у галузі інформації та інформаційної безпеки, формування інформаційного суспільства визначається тим, що закони цієї сфери суттєво впливають на законодавче регулювання відносин у всіх сферах життя.

З огляду на викладене, з метою протидії інформаційній агресії, фахівцями пропонується створення єдиного комунікаційного центру, аналогічного за функціями та завданнями відповідного структурного підрозділу НАТО.

У 2014 році в Латвії було створено Центр стратегічних комунікацій НАТО (NATO Strategic Communications Centre of Excellence), серед завдань якого – забезпечити адекватну відповідь на спроби інших країн вплинути на інформаційний простір членів НАТО. Центр має опікуватися питаннями «гібридної війни»[4].

Реалії сьогодення свідчать, що ефективним засобом посилення власних спроможностей у сфері координації інформаційних потоків стає залучення до активної співпраці волонтерів. Волонтерський рух в мережі Інтернет став одним із засобів протидії російській інформаційній агресії проти України.

Серед українських волонтерських проектів, що діють як допоміжні віртуальні ресурси в інформаційно-психологічній війні з російськими агресорами та сепаратистськими рухами, можна виділити Inform Napalm, «Інформаційний спротив» та центр «Миротворець». Зазначені мережеві проекти є яскравим прикладом того, як за допомогою належним чином розбудованої інформаційної мережі та системи роботи можна ефективно забезпечувати та ре-

[1] У Коруц, Запобігання та протидія пропаганді війни та інформаційним загрозам в Україні (2020) 2 (38) *Публічне право* 80–87.

[2] М Погорецький, В Шеломенцев, Поняття кіберпростору як середовища вчинення злочинів (2009) 2 *Інформаційна безпека людини, суспільства, держави* 77–81.

[3] М Погорецький, В Шеломенцев, Кіберзлочини: до визначення поняття (2012) 8 *Вісник прокуратури* 2012 № 8 89–96.

[4] В Горбулін, Гібридна війна як ключовий інструмент російської геостратегії реваншу <http://gazeta.dt.ua/internal/gibridna-viyna-yak-klyuchoviy-instrument-rosiyskoyi-geostrategiyi-revanshu-_.html> дата звернення 01.12.2022.

зультативно супроводжувати офлайн-процеси.

Практично всі вказані вище проекти діють за схемою роботи OSINT (Open Source Intelligence) – розвідувальної практики, яка передбачає пошук, вибір та збирання інформації, отриманої з відкритих джерел.

Важливою складовою такої роботи є системний аналіз наявної інформації з відповідною оцінкою та висновками, що дозволяють зрозуміти логіку та передбачити дії противника. Одним із базових правил цієї практики є те, що близько 90% необхідної для аналізу та прийняття відповідних рішень інформації перебуває у відкритих джерелах.

До таких джерел відносять: традиційні ЗМІ (газети, журнали, радіо, телебачення); інтернет-видання, що відносяться до ЗМІ (новинні сайти та портали, інтернет-ресурси профільних структур); акаунти та віртуальні майданчики у соціальних мережах; офіційні звіти державних структур; публічні заяви політиків і держслужбовців; спостереження – радіомоніторинг, використання загальнодоступних даних, аерофотозйомок (наприклад, Google Earth); професійні та академічні звіти, конференції, доповіді, статті; звіти та виступи в ЗМІ окремих незалежних експертів та експертних груп[1].

Щоб захиститися від інформаційної війни, необхідно також застосовувати методики, які використовує противник: знати його інфраструктуру, знищувати її; забезпечувати належний захист інформації; попереджувати введення викривленої інформації в поток правдивих фактів і даних; протидіяти спростуванню, запереченню та знищенню інформації і вчасно та якісно реагувати на всі прояви війни. У науковій літературі та політичній практиці така протидія отримала назву «асиметрична стратегія», яка в сучасних умовах означає постійний, активний системний тиск на вразливі місця супротивника, здатність організовувати свою діяльність і мислити відмінним від опонента способом задля максимізації власних переваг і використання вразливих місць, захоплення ініціативи чи забезпечення простору для маневрування»[2,3].

За цих умов, зацікавленим суб'єктам необхідно докладати додаткових зусиль у формуванні багатоспектрального інформаційного поля яке має бути в рази більшим і переконливішим дезінформаційне поле. Одночасно необхідно враховувати, що мінімум протягом п'ятнадцяти останніх років одним із завдань російської пропаганди було атрофувати вміння аудиторії об'єктивно мислити, аналізувати і задавати питання. Тому, боротьбу з дезінформацією не потрібно зводити лише до моніторингу та фактчекінгу. На нашу думку, є три обов'язкові складові, які нейтралізують дезінформаційну діяльність: блокування, створення альтернативи та розвиток медіаграмотності.

В сучасних умовах важливо звертати увагу на медіаграмотність в Україні. Суспільство живе в добу інформації, яка поволі перетворюється в добу дезінформації. Зважаючи на інформаційний простір, який надає можливість оперативного донесення інформації до користувача, необхідно вміти фільтрувати та грамотно визначати, що є важливим, а що ні, у що варто вірити, а що краще перевірити. Тому людині життєво необхідні критичне мислення і компетентність, що означає навички із перевірки сумнівної інформації. На національному рівні існує потреба забезпечення захисту національного інформаційного простору через ухвалення дієвих нормативно-правових

[1] О Курбан, Гібридна війна: сили спецопераций та соціальні мережі <http://ua.racurs.ua/1064-gibrydna-viyna-syly-specoperaciy-ta-socialni-mereji?articlevolist_page=339> дата звернення 01.12.2022.

[2] В Горбатенко, Асиметрична стратегія як відповідь на виклики системі європейської безпеки (2016) 6 *Studia Politologica Ucraino-Polona* Житомир Київ-Краків 61–67.

[3] Стратегія і тактика гібридних війн в контексті військової агресії Росії проти України (2014) 24 Борисфен Інтел <http://bintel.com.ua/uk/article/print/gibrid-war/> дата звернення 01.12.2022.

актів, спрямованих на захист інформації в інформаційно-комунікаційних системах. Потреба в цьому зумовлена поширенням інтернет-послуг, їх доступністю для надто великої кількості користувачів. Це пов'язано також і з тим, що останніми роками виробляється багато досить досконалих засобів безконтрольного зняття та поширення інформації. Робиться це й за допомогою новітніх інформаційних технологій, що потужно розвиваються і вдосконалюються[1].

Важливим напрямом забезпечення державної безпеки в інформаційній сфері є створення інформаційно-психологічних підрозділів для забезпечення психологічної безпеки особистості, суспільства, держави. Їх основне завдання – розробка і здійснення стратегічних та оперативних заходів із попередження і нейтралізації негативного інформаційно-психологічного впливу на державному, регіональному і місцевому рівнях. Зростання впливу інформаційних чинників, що обумовлено інформатизацією суспільства, об'єктивно вимагає ефективного функціонування системи інформаційно-психологічного забезпечення національної безпеки, об'єктами впливу якої мають бути інформаційно-психологічне середовище суспільства, інформаційні ресурси, психіка і поведінка політичної еліти, системи формування суспільної свідомості й думки та прийняття політичних рішень. Така система забезпечить захист психіки різних соціальних груп від деструктивного інформаційно-психологічного впливу, протидіятиме спробам маніпулювати процесами сприйняття інформації з метою відстоювання національних інтересів України в інформаційному просторі. Політика цілеспрямованого впливу на суспільну думку передбачає знання настроїв широких народних мас, реального стану справ. Постійний моніторинг ставлення українського суспільства до найважливіших проблем національної безпеки дасть змогу захистити психіку населення від негативного інформаційно-психологічного впливу[2].

На сьогодні вчені Німеччини розробили чіткі рекомендації із забезпечення інформаційно-психологічної безпеки особистості, які сприяють запобіганню або нейтралізувати негативний вплив ІПВ в маскомунікаційних (отримання інформації через ЗМІ), контакт-комунікаційних (отримання інформації під час масових видовищних заходів, на мітингах, зборах та ін.) і міжособистісних (отримання інформації у процесі спілкування з людьми, під час бесід, зустрічей тощо) ситуаціях, зокрема:

1. «Відхід» – збільшення дистанції, переривання контакту, вихід за межі досяжності інформаційного впливу. Дії в різних інформаційних ситуаціях можуть бути такими:

– відключення певних каналів ЗМІ (дратівливого каналу телебачення, вихід з інтернету та ін.), відмова від перегляду (прослуховування) конкретних теле- та радіопрограм;

– відмова від читання деяких газет, статей, рубрик та ін.;

– вихід з місць проведення масових видовищних заходів: театру, концертного залу, кінотеатру, мітингів, зборів тощо;

– зміна неприємної теми бесіди, прагнення не загострювати міжособистісні відносини під час бесіди (обхід «слизьких тем», «гострих кутів» та ін.), ухилення від зустрічей з тими, хто є джерелом неприємних переживань, переривання під різними приводами зустрічей, бесід. У деяких випадках захист може виразитися в різкій формі – «вигнанні» або «ігноруванні». У разі використання способу «вигнання» засіб або джерело негативного інформаційного впливу виганяється (або витісняється) з інформаційного середовища (відмова від корис-

[1] Б Калініченко, Інформаційна війна: чинники ескалації і засоби протидії (Київ, 2020) 294.

[2] В Хорошко, Ю Хохлачова, Д Чирков, Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України № 387/2015 (Київ, ПВП «Задруга», 2013) 12–19.

тування телевізором або комп'ютером, відвідування театральних постановок або концертів та ін.). «Ігнорування» передбачає несприйняття інформації, яка ускладнює або перешкоджає певній діяльності людини, може спровокувати конфлікт, викликати негативні емоції.

2. «Блокування» – контроль інформаційного впливу, виставляння психологічних бар'єрів, захист психіки від зовнішнього негативного інформаційного впливу. Дії, що виконуються при «блокуванні»:

– критичне сприйняття інформації;

– емоційне відчуження (сприйняття негативної інформації «без емоцій»);

– збільшення міжособистісного простору – «зони спілкування» під час бесіди;

– використання «психологічних бар'єрів» (приниження джерела інформації, внутрішнє висміювання, розвінчання авторитету, несерйозне сприйняття інформації, недовіра, настороженість, неуважність, відволікання і перемикання уваги на інші об'єкти, не пов'язані з вмістом інформаційного впливу та ін.).

3. «Управління» – контроль процесу інформаційного впливу, вплив на його характеристики і джерело. Виконувані дії:

– використання зворотного зв'язку (участь в опитуваннях щодо рейтингу популярності певних каналів або програм телебачення, популярності періодичних видань та ін.);

– висловлювання у видовищних заходах свого ставлення до подій (несхвалення, невдоволення особами, що виступають);

– використання в бесіді принципу «своїх не ображають», для чого варто: продемонструвати бажання стати другом, членом однієї спільності; послабити або дестабілізувати активність співрозмовника несподіваним відволіканням (наприклад, зробити комплімент, висловити співчуття) та ін.

4. «Затаювання» – контроль своєї реакції на зовнішній інформаційний вплив. Виконувані дії:

– відстрочка своїх реакцій, поспішних висновків і оцінок, затримка або відмова від дій і вчинків, спричинених інформаційним впливом (наприклад, у разі перебування в натовпі, щоб не піддатися «ефекту натовпу», психічному зараженню і не допустити вчинків, про які потім можна буде шкодувати);

– маскування, приховування почуттів, проявів емоцій та ін.[1]

На нашу думку, до переліку розроблених німецькими вченими рекомендацій доцільно додати «перевтілювання», яке можна застосовувати в усіх чотирьох визначених ними ситуаціях.

Безпосередній спосіб впливу інформації на свідомість означає апелювання до переконань людей, звернення до їхнього розуму із застосуванням раціональних аргументів, логіки. При цьому суб'єкт інформаційного впливу, звертаючись до розуму людей, неодмінно враховує реальну обстановку, суспільно-політичну ситуацію, розстановку сил, інтереси людей, що склалися на даний момент у тому чи іншому середовищі.

У процесі організації протидії деструктивним інформаційним впливам (як складової забезпечення інформаційної безпеки України), необхідно враховувати, що маніпулювання свідомістю за допомогою інформації передбачає наявність зворотного зв'язку[2]. Інформаційний вплив може бути нівельований, якщо суб'єкт маніпуляції не врахує динаміку зрушень у свідомості населення, а також вірогідність виникнення непередбачуваних ситуацій.

У розвинених демократичних країнах елементи маніпуляційного впливу застосовуються при безперервному урахуванні громадської думки. При цьому функціонує цілісна система опитувань, активізується спілкування депутатів різних рівнів з виборцями, підвищується увага до з'ясування настроїв конкретних груп населення. Це дозволяє вносити ко-

[1] V Levickij, Information-Psychological Security of the Person Partner Vash partner v Germanii 2007 № 6 (117) <http://www.partner-inform.de/ partner/detail/2007/6/272/2445> дата звернення 01.12.2022.

[2] Р Черниш, Організаційні та правові методи протидії маніпулюванню свідомістю громадян у соціальних мережах (2020) 3–4 *Вісник кримінального судочинства* 168–177.

ративи у пропаганду, реагувати на прояви неузгодженості між офіційною ідеологією та суспільною свідомістю.

На думку О. Мороз, для того, щоб протидіяти російській інформаційній ескалації в Україні необхідно:

– підвищити ефективність політики інформаційної безпеки в галузі оборони, вдосконалити організацію функціонування і посилити відповідні структури держави;

– перешкоджати маніпулятивним технологіям супротивника, які застосовують для впливу на суспільну свідомість;

– вдосконалювати методи протидії інформаційним впливам і захисту державних інформаційних ресурсів[1, 2, 3].

Погоджуючись із наведеним, зазначаємо, що із вказаною метою необхідно оптимізувати інформаційно-методичне забезпечення, в т.ч. визначення найбільш ефективних методів протидії деструктивним інформаційним впливам[4]. Зокрема, припускаючи, який саме комплекс заходів буде використовувати потенційний супротивник у ході військового конфлікту, терористичної або іншої протиправної акції, необхідно застосовувати такі засоби, які дозволяють блокувати його можливості, в тому числі: навмисне введення супротивника в оману щодо передбачуваних заходів і способів протидії загрозам національній безпеці; знищення засобів зв'язку й інформаційних систем супротивника; внесення умисних викривлень у роботу інформаційних систем супротивника; виявлення точок підтримки супротивника і їх знищення; одержання конфіденційної інформації про наміри супротивника і використання цих відомостей для формування стратегій захисту; використання засобів морально-психологічного пригнічення військ супротивника або інших засобів психологічного характеру, спрямованих на зміну ціннісних орієнтирів цільової аудиторії тощо.

Висновки. Підсумовуючи вищевикладене констатуймо, що пріоритетні заходи із забезпечення інформаційної безпеки України в умовах глобалізації повинні включати:

– визначення складу, послідовності та процедури складання законопроектів і нормативно-правових актів з питань інформаційної безпеки, протидії екстремізму та тероризму, а також механізмів їх реалізації (правовий супровід);

– розробку державної цільової науково-технічної програми інформаційної безпеки, створення інформаційної бази, спрямованої на реалізацію концепції інформаційної безпеки України (науково-технічне забезпечення);

– розробку організаційної структури системи інформаційної безпеки України;

– створення вітчизняної системи експертної оцінки інформації про наявність екстремістської складової (організаційна підтримка);

– забезпечення реальних потреб системи інформаційної безпеки в кадрових, матеріально-технічних та фінансових ресурсах (ресурсне забезпечення).

REFERENCES

BIBLIOGRAPHY

ARTICLES

1. Pohoretskyi M, Cherniak A, Serhieieva D, Chernysh R, & Toporetska Z (2022) 11 (53) Detection and proof of cybercrime. Amazonia Investiga [Detection and proof of cybercrime Amazonia Investiga] 259–269 [in Ukrainian].

[1] О Мороз, Боротьба за правду Як мій дядько переміг брехню (2020) 160.

[2] О Мороз, Нація овочів (2020) 288.

[3] О Мороз, Як не стати овочем Інструкція з виживання в інфопросторі (2021) 208.

[4] Р Черниш, М Ігнатюк, О Заріцький, Протидія деструктивному інформаційному впливу в Україні: правові та організаційні аспекти (2022) 1 *Юридичний науковий електронний журнал* <http://www.lsej.org.ua/index.php/arkhiv-nomeriv?id=146> дата звернення 01.12.2022.

2. Pohoretskyi M, Shelomentsev V, Poniattia kiberprostoru yak seredovyshcha vchynennia zlochyniv. Informatsiina bezpeka liudyny, suspilstva, derzhavy [The concept of cyberspace as an environment for committing crimes] (2009) 2 77–81 [in Ukrainian].

3. Pohoretskyi M, Shelomentsev V, Kiberzlochyny: do vyznachennia poniattia [Cybercrimes: to define the concept] (2012) 8 Visnyk prokuratury. 89–96 [in Ukrainian].

4. Zozulia O, Feik yak instrument informatsiinoi viiny [Fake as a tool of information warfare] Yurydychna hazeta – onlain versiia <https://yur-gazeta.com/publications/practice/inshe/feyk-yak-instrument--informaciynoyi-viyni.html> data zvernennia 01.12.2022 [in Ukrainian].

5. Ilnytska U, Informatsiina bezpeka Ukrainy: suchasni vyklyky, zahrozy ta mekhanizmy protydii nehatyvnym informatsiino-psykholohichnym vplyvam [Information security of Ukraine: modern challenges, threats and countermeasures against negative information and psychological influences] (2016) 2 (1) *Politychni nauky* <http://science.lp.edu.ua/sites/default/ files/Papers/ilnicka_0.pdf> data zvernennia 01.12.2022 [in Ukrainian].

6. Havryltsiv M, Informatsiina bezpeka derzhavy v systemi natsionalnoi bezpeky Ukrainy [Information security of the state in the national security system of Ukraine] (2020) 2 *Yurydychnyi naukovyi elektronnyi zhurnal* <http://lsej.org.ua/2_2020/54.pdf> data zvernennia 01.12.2022 [in Ukrainian].

7. Chernysh R F, Orhanizatsiini ta pravovi metody protydii manipuliuvanniu svidomistiu hromadian u sotsialnykh merezhakh [Organizational and legal methods of counteracting the manipulation of citizens' consciousness in social networks] (2020) 3–4 *Visnyk kryminalnoho sudochynstva* 168–177 [in Ukrainian].

8. Voloshyn P, Maruta N, Stratehiia okhorony psykhichnoho zdorov'ia naselennia Ukrainy: suchasni mozhlyvosti ta pereshkody [Strategy for protecting the mental health of the population of Ukraine: modern opportunities and obstacles] (2015) 23 (1) Ukrainskyi visnyk psykhonevrolohii 5–11. <http://nbuv.gov.ua/UJRN/Uvp_2015_23_1_3> data zvernennia 01.12.2022 [in Ukrainian].

9. Olishevskyi O, Zakhody protydii propahandi viiny v Ukraini [Measures to Counter War Propaganda in Ukraine] (2018) 1 (1) *Natsyonalnыi yurydycheskyi zhurnal: teoryia y praktyka* 155–160 data zvernennia 01.12.2022 [in Ukrainian].

10. Chernysh R F, Ihnatiuk M V, Zaritskyi O Iu, Protydiia destruktyvnomu informatsiinomu vplyvu v Ukraini: pravovi ta orhanizatsiini aspekty [Countering destructive information influence in Ukraine: legal and organizational aspects] (2022) 1 Yurydychnyi naukovyi elektronnyi zhurnal <http://www.lsej.org.ua/index.php/arkhiv-nomeriv?id=146> data zvernennia 01.12.2022 [in Ukrainian].

11. Koruts U, Zapobihannia ta protydiia propahandi viiny ta informatsiinym zahrozam v Ukraini [Prevention and Countering War Propaganda and Informational Threats in Ukraine] (2020) 2 (38) *Publichne pravo* 80–87 [in Ukrainian].

12. Horbatenko V, Asymetrychna stratehiia yak vidpovid na vyklyky systemi yevropeiskoi bezpeky [Asymmetric Strategy as a Response to Challenges to the European Security System] (2016) 6 *Studia Politologica Ucraino-Polona* ZhytomyrKyiv-Krakiv 61–67 [in Ukrainian].

13. V Levickij, Information-Psychological Security of the Person Partner Vash partner v Germanii [Information-Psychological Security of the Person Partner Vash partner v Germanii] 2007 6 (117) <http://www.partner-inform.de/ partner/detail/2007/6/272/2445> data zvernennia 01.12.2022. [in Ukrainian].

14. Stratehiia i taktyka hibrydnykh viin v konteksti viiskovoi ahresii Rosii proty Ukrainy [Strategy and tactics of hybrid wars in the context of Russia's military aggression against Ukraine] (2014) 24 Borysfen Intel <http://bintel.com.ua/uk/article/print/gibrid-war/> data zvernennia 01.12.2022 [in Ukrainian].

BOOKS

15. Moroz O, *Borotba za pravdu Yak mii diadko peremih brekhniu* [The Struggle for Truth How My Uncle Overcame Lies] (2020) 160 [in Ukrainian].

16. Moroz O, *Natsiia ovochiv* [Nation of Vegetables] (2020) 288 [in Ukrainian].

17. Moroz O, *Yak ne staty ovochem Instruktsiia z vyzhyvannia v infoprostori* [How not to become a vegetable. Instructions for survival in the infospace] (2021) 208 [in Ukrainian].

18. Kalinichenko B M, *Informatsiina viina: chynnyky eskalatsii i zasoby protydii* [Information War: Escalation Factors and Countermeasures] (Kyiv, 2020) 294 [in Ukrainian].

WEBSITES

19. Kharakterystyka stanovyshcha informatsiinoi bezpeky Ukrainy [Characterization of the situation of information security of Ukraine] <https://vuzlit.com/1137657/harakteristika _stanovischa_informatsiynoyi_bezpeki_ukrayini> data zvernennia 01.12.2022 [in Ukrainian].

20. Horbulin V, Hibrydna viina yak kliuchovyi instrument rosiiskoi heostratehii revanshu [Hybrid war as a key instrument of the Russian geostrategy of revenge] <http://gazeta.dt.ua/internal/gibridna-viyna-yak-klyuchoviy-instrument-rosiyskoyi-geostrategiyi-revanshu-_.html> data zvernennia 01.12.2022 [in Ukrainian].

21. Kurban O, Hibrydna viina: syly spetsoperatsii ta sotsialni merezhi [Hybrid War: Special Operations Forces and Social Networks] <http://ua.racurs.ua/1064-gibrydna-viyna-syly-specoperaciy-ta-socialni--mereji?articlevolist_page =339> data zvernennia 01.12.2022 [in Ukrainian].

22. Khoroshko V O, Khokhlachova Yu Ye, Chyrkov D V, Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 roku «Pro Stratehiiu natsionalnoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy № 387/2015 [On the decision of the National Security and Defense Council of Ukraine dated May 6, 2015 «On the National Security Strategy of Ukraine»: Decree of the President of Ukraine No. 387/201] (Kyiv, PVP «Zadruha», 2013) 12–19 [in Ukrainian].

Serhieieva D. B.
Doctor of Law, Professor,
Honored lawyer of Ukraine,
Professor of the Department of Criminal Procedure and Forensics
Educational and Scientific Institute of Law
Taras Shevchenko National University of Kyiv, attorney
***ORCID ID**: 0000-0003-1005-7046*

Chernysh R. F.,
Candidate of Law, Associate Professor,
National Academy of Security Service of Ukraine
***ORCID ID:** 0000-0003-4176-7569*

DOI: *https://doi.org/10.17721/2413-5372.2022.3-4/148-157*

ENSURING INFORMATION SECURITY OF UKRAINE IN THE CONDITIONS OF GLOBALIZATION

Annotation. *The article states that Ukraine has become the object of informational and psychological influences, operations, and wars, as a result of which its information security is under threat.*

It is noted that the relevance of the issue of ensuring Ukraine's state security in the information sphere is due to anti-Ukrainian influences that promote the ideas of separatism, violence, and national enmity, which creates prerequisites for the destruction of the national identity of Ukraine, the destruction of inter-ethnic harmony, encroachment on the constitutional order and territorial integrity of the state.

Taking into account the above, ***the purpose of the article*** *is to develop proposals for optimizing ways to ensure information security of Ukraine in conditions of globalization.*

The main directions of measures to protect the national information space and ensure the national information security system of Ukraine are highlighted, taking into account the destructive informational influence of the aggressor country on the target audience of the state.

It is argued that, taking into account the dynamics of the development of social relations in the information sphere, taking into account the need to implement effective measures to counter modern threats to information security, the form and methods of protecting information, critical information infrastructure and information and psychological security of citizens need to be improved by all European countries without exception.

In the final part of the study, priority measures to ensure information security of Ukraine in the conditions of globalization are formulated.

Key words: *information security, information war, the Internet, globalization, ensuring information security.*