УДК 327.8
DOI: https://doi.org/10.32782/2312-1815/2024-1-8

Михайло Савлюк
ORCID: 0009-0001-9870-8343

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті йдеться про перехід України від постіндустріального суспільства до інформаційного, що ставить перед країною нові виклики та загрози. Російська Федерація використовує в Україні гібридну війну, яка передбачає інформаційні атаки шляхом поширення неправдивої або частково правдивої інформації, маніпулювання фактами, сіяння паніки та розбрату. Метою роботи є дослідження алгоритму інформаційної атаки противника та розробка програми протидії агресору. Використані методи дослідження – аналіз, синтез, емпіричне пізнання та порівняння. За результатами дослідження було розроблено алгоритм визначення достовірності поширюваної інформації та виявлення інформаційних атак противника. Цей алгоритм допомагає відрізнити справжню інформацію від результату ворожих інформаційних операцій.

Ключові слова: *ІПСО, інформаційна безпека, кібербезпека, соціальні мережі пропаганда, інформаційні операції, війна, гібридна війна, історія, інформаційні атаки, національна безпека.*

Вступ. Уже понад півтора року як розгорнулася повномасштабна війна між та Російською Федерацією та Україною. Бойові дії тривають не тільки безпосередньо на полі бою, а й на інформаційному фронті – так звана гібридна війна. Ворог намагається знищити авторитет України на міжнародній арені, поширюючи інформацію, яка несе репутаційні ризики для України. Ворог щоразу, хвиля за хвилею, просуває все нові етапи своїх ІПСО, намагаючись посіяти зневіру серед українців і міжнародних партнерів України. Ворожа пропаганда й інформаційні атаки стосовно України розпочалися не 24 лютого 2022 року чи навесні 2014 року. Усе це має набагато довшу історію і почало діяти набагато швидше, ніж почалися безпосередні збройні зіткнення.

Мета та завдання. Метою роботи є визначення специфічних аспектів застосування інструментів ворожої пропаганди й інформаційних психологічних спеціальних операцій у контексті російської агресії, а також їхнього впливу на суспільство й пересічних громадян, політику та національну безпеку.

Відповідно до цієї мети були сформовані такі **завдання**:

– визначення категорії «інформаційна безпека»;

– дослідження історії інформаційної безпеки;

– з'ясування, якою має бути політика інформаційної безпеки держави;

– визначення інформаційної стратегії держави під час воєнного стану.

Методи дослідження. У рамках цієї наукової статті використовувалися такі методи дослідження, як аналіз, синтез, емпіричний метод і порівняння.

Аналіз останніх досліджень. Серед вітчизняних науковців, які б досліджували тему національної безпеки крізь призму інформаційної безпеки, насамперед слід відзначити Боднар І., Фурашева В., Архипова О. та Довганя О. Ці вітчизняні науковці наразі розробили досить ґрунтовний теоретичний аналіз проблем національної безпеки, проєктуючи її на інформаційне поле. Ними були визначені основні проблеми, структура та методи вивчення зазначеної проблематики.

Виклад основного матеріалу. Прихід до влади в Російській Федерації керівника авторитарного типу породив нові виклики та загрози для всього цивілізованого світу. Реваншистські

настрої та імперські погляди серед більшості населення, а особливо серед політичного та силового керівництва Росії, викликали черговий виток інформаційної війни, про яку вже почали забувати після завершення Холодної війни. У зв'язку зі стрімким розвитком інформаційних технологій і переходом більшості сучасних держав від постіндустральних до інформаційних суспільств стали можливими швидкі та надійні способи поширення інформації [1]. Цим не могли не скористатися авторитарні та тоталітарні режими, які намагаються протистояти так званому колективному Заходу. Зокрема, це стосується Російської Федерації, яка завдяки тому, що на світових ринках стрімко дорожчали ціни на енергоносії (зокрема, на нафту та газ), почала отримувати надприбутки до державного бюджету, але замість того щоб покращувати соціально-економічний стан своїх громадян і працювати над розвитком інфраструктури всередині власної країни, почала працювати над відновленням колишнього СРСР (нової країни в її територіальних межах).

На початку такої експансії, поки йшло відновлення російського військово-промислового комплексу, про якусь збройну агресію не йшлося. Проте наявні ресурси дали змогу російським пропагандистам розпочати роботу над створенням міфу про «вставання з колін» та історії про другу за силою армію світу. Насправді така робота принесла дуже хороші плоди, адже переважна більшість росіян, які пам'ятали голодні та холодні 90-ті роки (відразу після розпаду СРСР), у таку пропаганду охоче вірила. Така пропагандистська робота мала й успіх поза межами Російської Федерації. Адже за валюту куплялися публікації в провідних європейських і світових засобах масової інформації, що дало змогу поширювати пропагандистські матеріали про економічну могутність Росії та силу й непереможність російської армії.

Основною загрозою для національної безпеки є можливість впливу інших сил на інформаційну структуру країни, її інформаційні ресурси та суспільство загалом. Це вплив може бути спрямований на нав'язування державі інших цінностей, переконань, інтересів і рішень, які вигідні для інших сил [10]. Суть цієї загрози полягає в тому, щоб керувати поведінкою та розвитком країни у важливих сферах її суспільного та державного життя в напрямі, який вигідний іншим силам. Це може загрожувати суверенітету України в ключових галузях суспільного та державного життя, і ця загроза реалізується через інформаційні впливи. Стратегічне інформаційне протистояння є новим типом конфлікту, здатним вирішувати суперечності без застосування традиційних засобів ведення війни [3].

Отже, російська пропаганда почала впливати на інформаційну безпеку простих громадян. А з розвитком соціальних мереж і глобалізацією інформаційного простору російська пропаганда прийшла персонально до кожної людини, яка має акаунт у соціальних мережах. Це почало нести додаткові загрози для світової стабільності, адже, як ми бачили з початком повномасштабного вторгнення РФ до України (24 лютого 2022 року), усі світові найпрогресивніші розвідки давали Україні часу від трьох днів до двох тижнів. За їхніми розрахунками, російська армія мала б бути настільки високооснащеною та сильно тренованою, що Збройні сили України фактично не мали б шансів на опір загарбникам. Тому українській армії на початку не надавалися сучасні зразки озброєнь, які стоять на озброєнні армій країн НАТО. Командування НАТО побоювалося, що в разі стрімкого контрнаступу російської армії таке сучасне озброєння могло легко потрапити до рук російських, китайських та іранських інженерів, які б в подальшому могли відтворити такі сучасні зразки озброєння для своїх авторитарних режимів.

Із цього ми можемо побачити, що жертвами російської пропаганди та ІПСО стали не тільки пересічні громадяни, а й досвідчені офіцери світових розвідок, які так само повірили у міф про непереможність та силу «другої армії світу». Тож можна зробити висновки, що гібридні війни – це не вигадка, вони дійсно мають дуже важливий вплив на проведення бойових дій на лінії фронту. Інформаційна безпека є важливим фактором, що впливає на національну безпеку держави. А доступність і популярність соціальних мереж роблять вплив ворожої пропаганди

особливо дієвим. Тому для України, яка наразі перебуває у стані війни (у тому числі й гібридної) з Російською Федерацією, інформаційна безпека дорівнює національній безпеці, і нам треба навчитися її ефективно обороняти, маючи значно менші ресурси, ніж наш ворог [1].

Що таке інформаційна безпека. Інформаційна безпека є актуальною і важливою проблемою в сучасному світі, де інформація стала однією з найцінніших ресурсів. Ця стаття присвячена теоретико-методологічним засадам дослідження інформаційної безпеки, які допоможуть краще зрозуміти сутність цього поняття й визначити його відмінності від кібербезпеки [3].

Інформаційна безпека – це комплекс заходів, стратегій і політик, спрямованих на захист інформації від загроз, які можуть призвести до її втрати, руйнування або незаконного доступу (наразі ми бачимо, як ворог намагається активно втручатися в персональний (конфіденційний) простір українських споживачів інформації та активно впливати на нього своїми наративами та прихованою пропагандою) [1].

Це поняття містить декілька важливих аспектів:

1. Конфіденційність. Збереження конфіденційності інформації – це один із головних аспектів інформаційної безпеки. Інформація повинна бути доступною лише тим, кому вона потрібна, і не повинна потрапляти в руки несанкціонованих осіб (про що вказувалось вище).

2. Цілісність. Цілісність інформації визначається її станом, у якому вона зберігається й передається. Інформація повинна залишатися незмінною та недоторканою щодо будь-яких вторгнень або маніпуляцій (наразі російською пропагандою активно застосовується політтехнологічний метод напівправди, коли кінцевому споживачу інформації подається тільки та частина інформації, яка вигідна агресору (але вона часто вирвана з основного контексту і втрачає свою цілісність).

3. Доступність. Інформація повинна бути доступною тим, хто має на це право і потребує її для виконання своїх обов'язків. Недоступність інформації може призвести до порушення роботи організацій і завдати шкоди їх діяльності (щодо російського медіаполя, то ми бачимо тут власне зворотну ситуацію, коли цілий ряд інформаційних ресурсів і популярних соціальних мереж перебувають під тривалою державною забороною (фактично введена цензура), через це кінцевий споживач перебуває в «інформаційній бульбашці» і може сприймати за чисту правду все, що йому подає державна пропагандистська машина).

Чим відрізняється інформаційна безпека від кібербезпеки. Інформаційна безпека та кібербезпека часто сприймаються як синоніми, але вони мають важливі відмінності. Кібербезпека – це підгалузь інформаційної безпеки, яка спеціалізується на захисті інформації в цифровому середовищі. У вказаній статті нас більше цікавитиме саме напрям інформаційної безпеки, адже саме завдяки «атакам» на особистий інформаційний простір відбувається вплив на споживачів, що в кінцевому підсумку може вплинути на національну безпеку держави [12].

Основні відмінності між цими поняттями такі:

– Сфера застосування. Інформаційна безпека охоплює захист інформації в будь-якому форматі, включно з паперовими документами та фізичними носіями інформації (що є дуже важливим для нашого дослідження). Кібербезпека, з іншого боку, стосується виключно цифрової інформації і потребує спеціалізованих засобів і технологій для її зламу [13].

– Загрози. Інформаційна безпека стосується загроз, які можуть бути як фізичного, так і цифрового характеру (що, власне, ми зараз і спостерігаємо в українському медіаполі). Кібербезпека здебільшого зосереджена на цифрових загрозах, таких як хакерські атаки, віруси й інші онлайн-загрози.

– Заходи. Для забезпечення інформаційної безпеки використовуються різноманітні заходи, включно з фізичними засобами безпеки, контролем доступу і політиками безпеки, а також постійний моніторинг, зокрема, з боку органів влади та фахівців спецслужб. Кібербезпека

вимагає спеціалізованих технологій, включно з файрволами, антивірусами і криптографічними рішеннями [12].

У цій частині ми розглянули теоретико-методологічні засади дослідження інформаційної безпеки, визначили сутність поняття інформаційної безпеки та відмінності від кібербезпеки. Важливо зазначити, що інформаційна безпека є складною та багатогранною проблемою, яка потребує комплексного підходу та постійного вдосконалення заходів з її забезпечення, адже розвиток інформаційного поля (зокрема, соціальних мереж) ніколи не стоїть на місці [5]. Соціальні платформи постійно розвиваються та збагачуються. І якщо 15 травня 2017 року, згідно з указом п'ятого Президента України, у рамках введення додаткових санкцій України щодо Росії було введено заборону на популярні російські соціальні мережі «Одноклассники» та «Вконтакті» (що істотно зменшило вплив російської пропаганди на українських споживачів інформації), то зараз виникають нові популярні соціальні мережі, такі як «Тік Ток» [11].

Ця популярна соціальна мережа теж несе певну загрозу, оскільки до її баз даних має доступ уряд Китаю, який опосередковано підтримує Росію (не запроваджує проти неї економічних санкцій через її агресію щодо України, а, навпаки, активно розвиває економічно-торгівельні відносини з нею). У США від початку зростання популярності цієї соцмережі військовим було заборонено мати там свої акаунти, бо це могло викликати, як наслідок, витік персональних даних і потрапляння їх до рук не дружніх до США розвідок і спецслужб. У 2023 році саме через цей аспект у деяких американських штатах вже введено повну заборону на використання «Тік Ток» [14]. В Україні на цей час такої заборони немає, а тому російська пропаганда має додаткове інформаційне поле для поширення своїх наративів.

Щоб детально дослідити порушення та наслідки впливу на інформаційну безпеку, слід вивчити її історичну еволюцію від найдавніших часів і до тепер. Так ми зможемо краще зрозуміти ті виклики, з якими стикалась інформаційна безпека в різні епохи, і вивчити, як саме в ті чи інші часи протидіяли чи намагалися протидіяти інформаційним загрозам, які тоді виникали.

Для початку пропонується розглянути, як розвивалася та для чого створювалася інформаційна безпека від найдавніших часів і до XIX століття, оскільки цей період є відносно менш конфліктним, ніж інформаційні війни, які відбуваються в новітні часи.

Початки інформаційної безпеки. Започаткування інформаційної безпеки помічається ще в античній Греції та Римській імперії, де використовувалися методи шифрування для захисту секретної інформації. Наприклад, відомий шифр Скитала використовувався в античному Римі для шифрування повідомлень. Уже тоді люди зрозуміли, наскільки важливими для соціуму є інформаційна безпека й інформаційна гігієна [4].

Середньовіччя та Ренесанс. Середньовіччя відзначається використанням шифрувальних пристроїв, таких як шифратори та коди, для забезпечення безпеки дипломатичних спілкувань. Ренесансний період призвів до розвитку криптографії та поширення її в армії і державних структурах. В цю епоху ми бачимо створення уже чогось схожого на те, що є в сучасному світі та сучасних арміях.

Епоха промислової революції. З появою промислової революції зросла важливість захисту технічних і комерційних інформаційних ресурсів. Багато інноваційних методів і технологій було використано для захисту виробничих секретів та патентів. На цьому етапі ми бачимо заходи, якими людство користується і досі. Це, зокрема, патенти та захист банківської і комерційної таємниці. На цьому етапі людство все чіткіше починає розуміти переваги інформаційної гігієни й інформаційної безпеки, адже саме ці заходи допомагають сталому розвитку й економічному прогресу, до якого прагне все людство [7].

XIX століття. На початку XIX століття розвивалася телеграфія, що вимагала нових методів захисту інформації від небажаного втручань і посягань на конфіденційну передачу

інформаційних повідомлень. У 1854 році було створено кодекс, який став відомий як код Морзе для передачі повідомлень через телеграф.

Загальна тенденція розвитку інформаційної безпеки в цей період полягала в пошуку й застосуванні нових методів шифрування та зберігання інформації. Зокрема, бажання посилити інформаційну безпеку певною мірою спонукало людство до розвитку та прогресу, адже способи шифрування та передачі інформації, які виникали в попередні епохи, призвели до розвитку нових технологій і винаходів [12].

Інформаційна безпека у XX–XXI століттях. Далі слід розглянути період, який є значно коротшим у часі, ніж ті історичні періоди, які розглядалися вище. Але цей період тривалістю трохи менше півтора століття став найбільш інтенсивним відрізком часу стосовно розвитку та поширення інформаційних технологій і засобів для їх передавання на великі відстані та для масової аудиторії.

Ера кібернетики. XX століття відзначається різким розвитком науки, а саме комп'ютерів і кібернетики. Із цим розвитком з'явилися нові можливості для зберігання, обробки та передачі інформації, а також нові загрози для інформаційної безпеки. Кожен винахід у цій галузі ставав доступнішим і дешевшим для широкого загалу, що, зі свого боку, потягнуло за собою масові зловживання та використання їх у злочинних і протизаконних діях [12].

Важливим етапом стало створення Еніака – першого електронного комп'ютера, який використовувався для розшифрування різноманітних ворожих кодів під час кровопролитної Другої світової війни. Це відкриття вперше показало, що комп'ютери можуть бути використані як для захисту, так і для порушення інформаційної безпеки. Тобто інформаційне протистояння та боротьба за інформаційну безпеку вийшли на абсолютно новий рівень. Тож почали виникати нові виклики й загрози для інформаційної безпеки та належного поводження з конфіденційною інформацією для її розпорядників. Це знову ж таки сприяло стрімкому прогресу й розвитку всіх подальших інформаційних систем і способів поширення масової та конфіденційної інформації [7].

Кібернетична ера. У другій половині XX століття і на початку XXI століття інформаційна безпека стала викликати все більший інтерес через поширення комп'ютерів, Інтернету та цифрових технологій. Кіберзагрози, такі як хакерські атаки, віруси та фішинг, стали повсюдними явищами. Вони стали новими викликами для розпорядників інформації та правоохоронних органів. Різноманітні розробки й винаходи зловмисників ніколи не залишаються на місці та постійно розвиваються [15]. Злочинці щоразу вигадують нові способи поширення фейкових і неправдивих новин або ж намагаються видурити конфіденційну банківську інформацію, щоб отримати із цього фінансовий зиск.

Саме на цей час припадає розквіт інформаційних воєн, поширення пропаганди та створення спеціальних підрозділів приватних фірм або ж підрозділів армій світу (так званих ботоферм). Основним завданням таких підрозділів є саме поширення неправдивої інформації та потрібних їхньому керівництву наративів. Такі заходи допомагають деморалізувати противника та пришвидшують перемогу [12].

На замовлення урядів створюються інформаційні ресурси (такі як інформаційні вебсайти чи телеканали) або ж навіть цілі соціальні мережі, які в подальшому дають змогу військовим розвідкам і спецслужбам цих держав конфіденційно отримувати персональну інформацію про зареєстрованих користувачів [15].

Такі виклики майже миттєво зумовлюють створення протидії. Однією з таких важливих подій в історії інформаційної безпеки стало створення стандарту криптографічного захисту інформації – шифру AES. Цей стандарт став основою для захисту важливої інформації на державному й корпоративному рівнях.

XXI століття також відзначається розробкою та впровадженням стратегій і політик інформаційної безпеки на рівні держав та організацій. Наразі це є один з основних чинників,

який у подальшому може впливати на стабільну національну безпеку та боротися з викликами й загрозами, які оточують людство в сучасному інформаційному та кібернетичному глобалізованому світі [7].

Із цього можна зробити цілий ряд висновків, які в подальшому допоможуть більш конкретно зрозуміти суть досліджуваної проблематики. Історія інформаційної безпеки свідчить про постійний розвиток і адаптацію заходів і методів для захисту інформації протягом століть. Від античних методів шифрування до сучасних кіберзаходів – інформаційна безпека завжди залишалася актуальною та важливою проблемою. Вона ніколи не стоїть на місці, і на нові виклики завжди потрібно шукати якусь протидію [1]. А оскільки прогрес і людство не стоять на місці, то на кожен їхній винахід знаходяться ті негативні сили, які намагаються це використати на свою не зовсім законну користь.

Далі пропонується розглянути те, що на сучасному етапі повинна мати кожна держава та поважна установа, йдеться про політику інформаційної безпеки.

Інформаційна безпека є важливим елементом сучасного світу, особливо в контексті збільшення обсягу інформації та швидкості її передачі. Політика інформаційної безпеки є ключовим аспектом управління цією проблемою [8]. Далі розглядатимемо політику інформаційної безпеки держави та її особливості в умовах війни, а саме вивчатимемо алгоритм дій для протидії ворожим інформаційним атакам.

Політика інформаційної безпеки держави – це сукупність стратегій, методів і механізмів, спрямованих на захист національних інформаційних ресурсів і забезпечення їх надійності та цілісності. Вона передбачає такі аспекти:

Створення інфраструктури інформаційної безпеки. Держава повинна розробити інфраструктуру та мати висококваліфікованих фахівців для зберігання, обробки та передачі інформації з врахуванням сучасних вимог щодо безпеки [6].

Законодавство та регулювання. Для забезпечення інформаційної безпеки держава повинна приймати та застосовувати відповідне законодавство, включно із законами про кібербезпеку, захист персональних даних та іншими нормативними актами. Це повинен бути сукупний кодекс сучасних законів (про які два десятиліття тому навіть ніхто б і не думав), завдяки якому можна якісно регулювати інформаційне поле держави [5].

Розвиток і підтримка кадрів. Держава має забезпечити підготовку та підтримку висококваліфікованих фахівців у сфері інформаційної безпеки, зокрема кіберспеціалістів та аналітиків. Такі люди мають першими виявляти загрози інформаційній безпеці держави (навіть, якщо вони носять прихований характер). Вони повинні бути вмотивованими, навченими та мати відповідне обладнання й забезпечення (як фінансове, так і технічне), щоб на високому рівні конкурувати з опонентами [4].

Міжнародне співробітництво. Здійснення політики інформаційної безпеки також передбачає співпрацю з іншими країнами та міжнародними організаціями для обміну інформацією і спільної боротьби з кіберзагрозами та сучасними інформаційними викликами [8]. Така співпраця дасть змогу попереджувати небезпечні ситуації та навіть війни (як це сталося 24 лютого 2022 року в Україні та 7 жовтня 2023 року в Ізраїлі), «оскільки попереджений, значить озброєний».

Створення культури інформаційної безпеки. Політика інформаційної безпеки повинна сприяти формуванню свідомого підходу до безпеки інформації серед громадян та організацій, адже «не стільки небезпечний ворог, як дурень з ініціативою». Інформаційна політика держави має також бути спрямована на освіту населення поводження з інформацією, зокрема в соціальних мережах [4], адже сьогодні соцмережами користується чимало людей похилого віку й осіб без відповідної освіти, які запросто підхоплюють і поширюють ворожі наративи.

На завершення пропонується розглянути актуальну проблематику для сучасного стану України, а саме політику інформаційної безпеки держави під час війни та воєнного стану.

В умовах війни політика інформаційної безпеки набуває особливо важливого та критичного значення, оскільки інформація може бути використана відверто або приховано для досягнення військових і політичних цілей. Нижче розглянемо основні аспекти політики інформаційної безпеки держави під час війни.

Кібервійна. У сучасних конфліктах інформаційна безпека стає одним з основних аспектів бойових дій, оскільки так звані хакерські атаки можуть істотно впливати на роботу критичної інфраструктури держави, роботу транспорту, освітнього процесу й інших не менш важливих для перемоги компонентів. Держава повинна бути готовою до відповіді на ворожі кібератаки та захист своєї критичної інфраструктури [7]. Коли якісно «контратакувати» й «оборонятися» на кіберполі, то противник може відмовитися від своїх планів у цьому напрямі. І всі свої сили залучатиме до відбиття саме «кіберконтратак».

Пропаганда та психологічна війна. Інформація може бути використана для маніпулювання громадською думкою та зміни ставлення до війни. Ворог у доступний спосіб може поширювати власні наративи та пропаганду і, використовуючи політтехнології та психологічні маніпуляції, домогтися того, що громадяни держави, яка піддається нападу, самостійно поширюватимуть таку неправдиву та відверту дезінформацію серед власних друзів (це стосується власне соціальних мереж і пліток). Така робота буде відвертим підіграванням ворогу та його спецслужбам. Держава повинна мати стратегію протидії таким впливам і розвивати контрпропаганду. Для цього потрібна відповідна стратегія та кваліфіковані фахівці з досвідом роботи в інформаційному полі [6].

Захист інформації. У військових операціях держава повинна забезпечити захист конфіденційної інформації від ворожих розвідувальних дій. Конфіденційність і захист такої інформації сприятиме успішним наступальним і контрнаступальним операціям [2]. Саме так, як це було з контрнаступом Збройних сил України на харківському напрямку восени 2022 року (що дало змогу звільнити значну частину окупованих територій) чи успішною атакою на Кримський міст восени того ж року (завдяки чому вдалося порушити логістичні ворожі ланцюжки на півдні України).

Міжнародне співробітництво. Під час війни міжнародне співробітництво в галузі інформаційної безпеки набуває важливого значення для обміну розвідувальною інформацією та координації заходів. Така співпраця є особливо корисною, коли держава істотно поступається ворогам у плані технічного та матеріального забезпечення. І якщо мати добрі стосунки з іноземними державами, у яких є сучасне обладнання й оснащення, то це буде важливим фактором у протидії ворогові [2].

Гуманітарні аспекти. Держава повинна також враховувати гуманітарні аспекти інформаційної безпеки, забезпечуючи доступ до гуманітарної інформації та дотримання прав людини під час конфлікту. На жаль, відкритістю джерел гуманітарної інформації може скористатися ворог, щоб створювати провокації та поширювати небезпечну для всіх громадян дезінформацію.

Політика інформаційної безпеки держави є важливим інструментом управління інформаційними ресурсами й забезпечення національної безпеки в сучасному світі. Вона має враховувати як нормальні умови, так і специфічні аспекти під час війни, щоб забезпечити надійний захист інформації та інтересів держави. На жаль, на сучасному етапі політика інформаційної безпеки України не є на досконалому рівні, що викликає загрози та напади з боку ворога [5].

Саме розробка й дослідження наявної проблематики має всебічно сприяти покращенню інформаційної безпеки нашої держави. Написання та створення методичних інформаційних

посібників для спецслужб і пересічних громадян має стати наріжним каменем в роботі з витіснення ворожих наративів і ворожої пропаганди з українського інформаційного поля [4]. Люди повинні навчитися вирізняти ворожі потоки інформації серед тих численних повідомлень, які їх оточують. Особливо це стосується користувачів соціальних мереж, адже саме там зустрічаються величезні масиви неперевіреної та невідфільтрованої інформації. А це, зі свого боку, зміцнить бойовий дух армії та всіх громадян і наблизить перемогу України.

Література:

1. Архипов О. Є., Архипова Є. О. Особливості розуміння понять «інформаційна безпека» та «безпека інформації». *Інформаційні технології та безпека: основи забезпечення інформаційної безпеки (ІТБ-2014): Матеріали XIV Міжнародної науково-практичної конференції*. Київ : ІПРІ НАН України, 2014. С. 18–30.

2. Богданович В. Ю., Ворович Б. О., Марко Є. І. Інформаційна безпека як основа воєнної безпеки держави та суспільства. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,* 2018. № 3, с. 44–48.

3. Боднар І. Р. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation,* 2014. № 1, с. 68–75.

4. Булаєв В. П. Теоретико-методологічні засади дослідження адміністративно-правового регулювання діяльності інформаційних служб системи МВС України. Laws and Administrative Measures on Information Services of the Ministry of Internal Affairs of Ukraine. 2018.

5. Довгань О. Д., Ткачук Т. Ю. Система інформаційної безпеки України: онтологічні виміри. Інформація і право. № 1 (24). 2018. С. 89–103.

6. Колгатин А. Г. Інформаційна безпека в системах відкритої освіти. *Освітні технології та суспільство*. 2014. Т. 17, № 1. С. 417–425.

7. Лисенко Сергій. Історія досліджень інформаційної безпеки як об'єкта правовідносин. *Supremația Dreptului*. № 2 (2016), с. 34–44.

8. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України. *Політичний менеджмент.* 2008.

9. Рішення РНБО України від 28 квітня 2017 року. URL: https://zakon.rada.gov.ua/laws/show/n0004525-17#Text.

10. Троянський О. А. Інформаційна безпека в Україні: сучасний стан та перспективи розвитку. 2021.

11. Указ Президента України № 133/2017. URL: https://www.president.gov.ua/documents/1332017-21850

12. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право,* 2012. № 2 (5), с. 162–169.

13. Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and national security*. Potomac Books, Inc., 2009.

14. Kumar, Anilesh. State nationalism or popular nationalism? Analysing media coverage of TikTok ban on mainstream Indian TV news channels. *Media Asia*, 2023. P 1–17.

15. Miller, Daniel, et al. *How the world changed social media*. UCL press, 2016.

References:

1. Arkhipov, O. E., & Arkhipova, Ye. O. (2014). Osoblyvosti rozuminnia poniat "informatsiina bezpeka" ta "bezpekainformatsii" [Features of Understanding the Notions of "Information Security" and "Security of Information"]. *Information Technologies and Security: Basics of Ensuring Information Security (ITS-2014): Proceedings of the XIV International Scientific and Practical Conference.* Kyiv: IEP NAPS of Ukraine. P. 18–30 [in Ukrainian].

2. Bohdanovych, V. Yu., Vorovych, B. O., & Marko, Ye. I. (2018). Informatsiina bezpeka yak osnova voiennoi bezpeky derzhavy ta suspilstva [Information Security as the Basis of State and Society Military Security]. *Collection of Scientific Papers of the Center for Military-Strategic Research of the Ivan Chernyakhovsky National Defense University of Ukraine*, 3. P. 44–48 [in Ukrainian].

3. Bodnar, I. R. (2014). Informatsiina bezpeka yak osnova natsionalnoi bezpeky [Information Security as the Basis of National Security]. *Mechanism of Economic Regulation*, 1. P. 68–75 [in Ukrainian].

4. Bulayev, V. P. (2018). Teoretyko-metodolohichni zasady doslidzhennia administratyvno-pravovoho rehuliuvannia diialnosti informatsiinykh sluzhb systemy MVS Ukrainy [Theoretical and Methodological Foundations of Research on Administrative and Legal Regulation of the Activities of Information Services in the Ministry of Internal Affairs of Ukraine]. *Laws and Administrative Measures on Information Services of the Ministry of Internal Affairs of Ukraine* [in Ukrainian].

5. Dovhan, O. D., & Tkachuk, T. Yu. (2018). Systema informatsiinoi bezpeky Ukrainy: ontolohichni vymiry [The Information Security System of Ukraine: Ontological Aspects]. *Information and Law,* 1 (24). P. 89–103 [in Ukrainian].

6. Kolhatin, A. G. (2014). Information Security in Open Education Systems [Informatsiina bezpeka v systemakh vidkrytoi osvity]. *Educational Technologies and Society*, 17.1. P. 417–425 [in Ukrainian].

7. Lysenko, S. (2016). Istoriia doslidzhen informatsiinoi bezpeky yak obiekta pravovidnosyn [The History of Research on Information Security as an Object of Legal Relations]. *Supremacy of Law,* 2. P. 34–44 [in Ukrainian].

8. Ostroukhov, V., Petryk, V. (2008). Do problemy zabezpechennia informatsiinoi bezpeky Ukrainy [On the Issue of Ensuring Information Security of Ukraine]. *Political Management* [in Ukrainian].

9. Verkhovna Rada of Ukraine (2017). Resolution of the National Security and Defense Council of Ukraine, April 28, 2017. Retrieved from https://zakon.rada.gov.ua/laws/show/n0004525-17#Text [in Ukrainian].

10. Troyansky, O. A. (2021). "Information Security in Ukraine: Current State and Development Prospects" [in Ukrainian].

11. Decree of the President of Ukraine No. 133/2017. Retrieved from https://www.president.gov.ua/documents/1332017-21850 [in Ukrainian].

12. Furashev, V. M. (2012). Kiberprostir ta informatsiinyi prostir, kiberbezpeka ta informatsiina bezpeka: sutnist, vyznachennia, vidminnosti [Cyberspace and Information Space, Cybersecurity and Information Security: Essence, Definitions, Differences]. *Information and Law,* 2 (5). P. 162–169 [in Ukrainian].

13. Kramer, Franklin D., Stuart H. Starr, Larry K. Wentz, eds. (2009). Cyberpower and National Security. *Potomac Books,* Inc.

14. Kumar, Anilesh. (2023). State Nationalism or Popular Nationalism? Analyzing Media Coverage of the TikTok Ban on Mainstream Indian TV News Channels. *Media Asia*. P. 1–17.

15. Miller, Daniel, et al. (2016). How the World Changed Social Media. UCL Press.

Mykhailo Savlyuk. Theoretical and methodological basis of information security research

The article discusses Ukraine's transition from a post-industrial society to an information society, which poses new challenges and threats to the country. The Russian Federation is using hybrid warfare in Ukraine, which includes information attacks by spreading false or partially true information, manipulating facts, and sowing panic and discord. The purpose of the study is to investigate the algorithm of the enemy's information attack and to develop a programme of counteraction to the aggressor. The research methods used are analysis, synthesis, empirical knowledge and comparison. The study resulted in the development of an algorithm for determining the reliability of disseminated information and detecting enemy information attacks. This algorithm helps to distinguish genuine information from the result of enemy information operations.

Key words: *IPSO, information security, cybersecurity, social media propaganda, information operations, war, hybrid warfare, history, information attacks, national security.*