Айтек Бабаєва,
аспірантка Академії державного управління при
Президентові Азербайджанської Республіки

Роль принципів міжнародного права у формуванні
специфічних принципів сталого розвитку

У статті аналізується роль принципів міжнародного права у формуванні специфічних принципів сталого розвитку. Наголошується на загальній значущості основних принципів міжнародного права, низки принципів (повага прав людини і основних свобод, принцип співробітництва держав, принцип сумлінного виконання міжнародних зобов'язань, принцип суверенної рівності держав), а також нові принципи міжнародного права (принцип міжнародно-правового захисту навколишнього середовища, принцип колективної безпеки). Сталий розвиток тісно пов'язаний із правами людини і соціальними, економічними та екологічними цілями. Концепція сталого розвитку поєднує економічні, екологічні та соціальні пріоритети і може бути реалізована в контексті національно-правового застосування, що відображає міжнародно-правове регулювання. Це вимагає єдиного підходу до проблеми з міжнародно-правової точки зору, оскільки національно-правове регулювання залежить від ефективного виконання міжнародних норм.

Міжнародні суди вже посилаються на документи про сталий розвиток. Сталий розвиток був предметом обговорення національних судів, а низку положень в цих галузях було включено до конституцій держав. Окрім цього, зазначаються такі процеси як глобалізація, акцент на фактор прав людини, залежність безпеки кожної держави від системи міжнародної безпеки, швидко зростаюча роль міжнародних відносин і міжнародного права у внутрішніх справах і т. д., що представляють нові тенденції. Нарешті, специфічні принципи сталого розвитку (рівність і скорочення бідності; принцип відповідальності держав; принцип обережного ставлення до здоров'я людини, природних ресурсів й екосистем; принцип участі громадськості й доступу до інформації та правосуддя; принцип належного врядування; принцип інтеграції та взаємодії та ін.) тісно пов'язані та формуються на основі міжнародного права і прав людини.

Ключові слова: *сталий розвиток, права людини, суверенна рівність, співробітництво держав, міжнародні зобов'язання, специфічні принципи, міжнародні угоди, економічне співробітництво, охорона навколишнього середовища, відповідальність держав, міжнародне право.*

https://doi.org/10.31392/NPU-nc.series22.2021.30.12
УДК 351.746(477):007]:327.88

Вознюк Євгенія Василівна,
кандидат політичних наук, доцент,
кафедра міжнародних відносин і регіональних студій
Волинського національного університету імені Лесі Українки
vozniukjane.vippo@gmail.com; ORCID: 0000-0002-7828-7430

SWOT-АНАЛІЗ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Стан інформаційної безпеки держави є надзвичайно актуальним питанням як для інформаційного простору України, так і для усього світу, з огляду на постійне розширення спектру гібридних загроз. Метою статті є визначити сильні, слабкі сторони інформаційної безпеки України, дослідити наявні загрози та виокремити можливості подальшого їх усунення. У ході дослідження використано SWOT-аналіз - сукупно розглянуто сильні та слабкі сторони інформаційної війни і безпеки нашої держави (strengths and weaknesses), а також висвітлено усі існуючі її можливості та загрози (opportunities and threats). Детально розглянуто теоретико-методологічні основи дослідження питання інформаційної безпеки України. Виокремлено ключові поняття інформаційної безпеки, інформаційної війни, інформаційного тероризму. Висвітлено основні напрями діяльності в галузі інформаційної

безпеки, проаналізовано головні загрози, які спричиняють порушення категорій інформаційної безпеки. Проаналізовано типи інформаційних війн, їх компоненти та види. Охарактеризована мета та інструменти сучасних способів реалізації інформаційного або кібертероризму.

Зазначено, що на відміну від інформаційної війни, для інфотероризму характерна нерівність конфронтуючих сторін, що змушує слабку сторону використовувати такі методи й засоби, які б при використанні мінімальних зусиль змогли найбільше зашкодити іншій стороні конфлікту. Звідси захист інформації є важливою складовою частиною підтримання загалом національної безпеки країн.

Ключові слова: *інформаційна безпека, інформаційна війна, інформаційний тероризм, SWOT-аналіз, Україна, гібридні загрози.*

Вступ. На сучасному етапі розвитку український інформаційний простір не в змозі повноцінно протистояти гібридним загрозам з боку Російської Федерації, щоб донести цілісну картину та сучасну ситуацію для світової громадськості. Українські інформаційні джерела, доступні іноземними громадянам і жителям окупованих територій, подаються у вигляді фейкових новин російською мовою. Основна інформаційна пропаганда спрямована на міжнародну спільноту, внутрішню російську аудиторію та мешканців територій, де відбуваються воєнні дії (Донецька та Луганська області). Все це здійснює значний деструктивний вплив на інформаційну політику та безпеку України, що вимагає своєчасних та кардинальних рішень зі сторони влади та громадськості.

Метою статті є визначення сильних, слабких сторін інформаційної безпеки України, виокремлення можливостей подальшого її удосконалення, дослідження наявних загроз.

Аналіз останніх досліджень. Дослідженню інформаційної безпеки України присвячено праці таких вітчизняних вчених як В. Бурячок, Н. Карпчук, Н. Ніколаєнко, Н. Ротар, Н. Хома, Є. Тихомирова, А. Шуляк та ін. Значна частина публікацій присвячена аналізу поняття інформаційна безпека, визначенню можливих загроз, становленню нормативного забезпечення. Серед робіт, що присвячені цій тематиці, слід відзначити колективні монографії, підручники: «International and National Security: Politics, Information, Ecology, Economy» під редакцією А. Митко; «Інформаційна та кібербезпека: соціотехнічний аспект під загальною редакцією» В. Толубка.

Результати та дискусії. Розглянемо теоретико-методологічні основи дослідження інформаційної безпеки України. Ключовим поняттям є інформаційна безпека (ІБ), що сучасними вченими визначається як стан захищеності систем обробки й зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, унесення змін, ознайомлення, перевірки, запису чи знищення (у цьому значенні частіше використовують термін «захист інформації»). ІБ держави характеризується ступенем захищеності й, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості та ін.) стосовно небезпечних (дестабілізаційних, деструктивних, суперечних інтересам країни тощо) інформаційних впливів, причому як до впровадження, так і до вилучення інформації (Шуляк, 2019, с. 130).

Поняття інформаційної безпеки, на переконання учасних дослідників, є не лише безпекою технічних інформаційних систем чи безпекою інформації в чисельному або електронному вигляді, адже потрібно охопити усі аспекти захисту даних чи інформації, незалежно від їхньої форми. Проблему ІБ розглядають у таких основних аспектах: захист інформації, контроль за національним інформаційним простором, достатнє інформаційне забезпечення державних і недержавних органів, громадських, приватних організацій. У захисті інформації вбачається система заходів з недопущення несанкціонованого доступу до інформації, несанкціонованої її модифікації, втрати, знищення, порушення цілісності тощо.

Інформаційна безпека України – передбачений Конституцією захист політичних, державних, громадських інтересів країни, загальнолюдських і національних цінностей (Шуляк, 2019, с. 133):

1) дотримання вимог чинного законодавства щодо неприпустимості зловживань свободою ЗМІ, недопущення закликів до насильницької зміни конституційного ладу й захоплення влади, порушення територіальної цілісності держави, пропаганди війни, насилля, жорстокості, розпалювання расової, національної, релігійної ворожнечі, посягань на права та свободи людини, суспільства;

2) запобігання розміщенню відомостей, що становлять державну таємницю, чи відомостей з обмеженим доступом, а також текстових матеріалів, які переміщаються через державний кордон України (Шуляк, 2019, с. 133).

Інформаційна безпека охоплює й протидію технічним, маніпулятивним і психологічним впливам. Основним напрямом діяльності в цій галузі є збалансований захист конфіденційності, цілісності та доступності даних, також відомий як «Тріада ЦРУ», зберігаючи при цьому фокус на ефективній реалізації політики та відсутності суттєвої перешкоди продуктивності організації (Vetrov & Voznyuk, 2019, p. 35). Розглядаючи перелік інтересів ІБ щодо доступності інформації, відкритості інформаційних систем і новітніх інформаційних технологій як сучасних об’єктів вирішення безпекових питань, виокремлюємо такі основні категорії: доступність (можливість отримання будь-якої необхідної інформації за визначений проміжок часу); цілісність (отримання актуальної, несуперечливої інформації, а також визначення її надійності, захищеності від руйнування та несанкціонованого змінювання); конфіденційність (повна й цілковита захищеність від будь-якого несанкціонованого проникнення).

Головними загрозами, які негативно впливають на згадані раніше основи інформаційної системи, призводять до втрати інформації або її надійності, знищення чи збою функціонування, вважаємо: розголошення інформації, витік інформації, несанкціонований доступ до інформації (див. рис. 1.1).

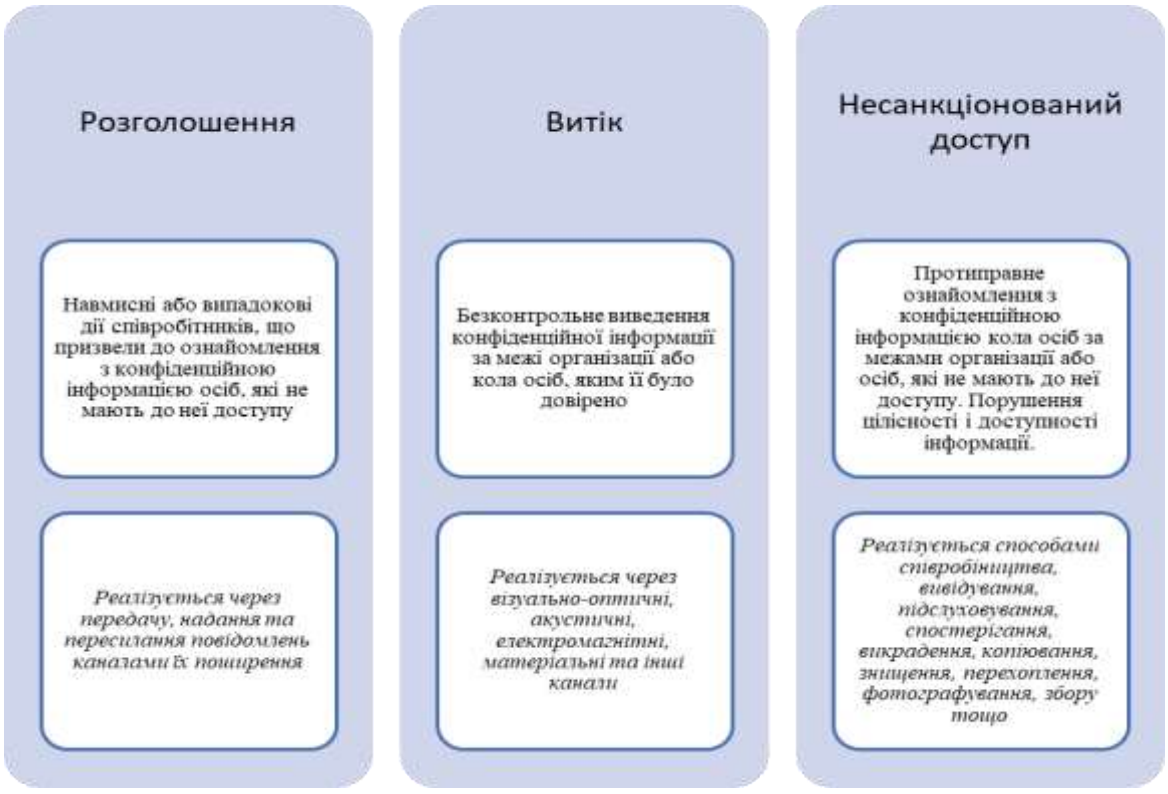

Рис. 1.1 *Головні загрози інформаційної безпеки**

*Побудовано за: (Бурячок та ін., 2015, с. 13).

Інформаційна війна та інформаційний тероризм є формами порушення інформаційної безпеки держави. Інформаційна війна – це тактичне та стратегічне використання інформації для отримання переваги. Вона може охоплювати кілька типів операцій і проводитися різними способами протягом десятиліть. Інформаційна війна також відома як кібернетична війна, електронна війна та кібернетична атака. Дан Куель з Національного університету оборони визначив інформаційну війну як «конфлікт або боротьбу між двома та більше групами в інформаційному середовищі» (цит. за Ничипорчук та Вознюк, 2018, с. 68).

Сучасна інформаційна війна містить такі компоненти: збір тактичної інформації, перевірка точності інформації, розповсюдження пропаганди та дезінформації для деморалізації або маніпулювання супротивником та громадськістю; підривання якості інформації супротивника. Можливі види інформаційної війни: використання вірусів або шкідливих програм для проведення кібератак; використання «дірок» в мережі; викрадення інформації через різні типи несанкціонованого доступу.

Серед проявів інформаційної війни крайній – інформаційний тероризм. Це використання інформаційних технологій, засобів масової інформації, поширення інформації з метою цілеспрямованого впливу на обраний об'єкт, його дискредитація (Bondar, 2011, p. 128). У науковому вжитку є також ще одна його поширена назва – кібертероризм – використання комп'ютерних і телекомунікаційних технологій (особливо Інтернету) в терористичних цілях. Законодавство України визначає кібертероризм як терористичну діяльність, що здійснюється в кіберпросторі або з його використанням. Це вбивча атака, спрямована на залякування з метою досягнення політичних результатів або нанесення шкоди комп'ютерним мережам, особливо персональним комп'ютерам, підключеним до Інтернету, за допомогою таких засобів як комп'ютерні віруси (Vozniuk et al., 2018, p. 169**).**

На відміну від інформаційної війни, для інфотероризму характерна нерівність конфронтуючих сторін, що змушує слабку сторону використовувати такі методи й засоби, які б при використанні мінімальних зусиль змогли найбільше зашкодити іншій стороні конфлікту. Метою тероризму є залякування й деморалізація людства, а об'єктом такої діяльності є не ті, хто постраждали, а ті, хто залишився в живих. Інформаційній простір є ідеальним місцем для поширювання ідей тероризму, залучення до своєї діяльності все більше прибічників та для того, аби психологічно впливати на населення.

Захист інформації є важливою складовою частиною підтримання національної безпеки країн. Організація захисту інформації здійснюється за допомогою системи правових, організаційних та інженерно-технічних заходів. Реалізація організаційних та інженерно-технічних заходів є сутнісю процесів технічного захисту інформації. Правові заходи захисту інформації є базисом, на який спираються організаційні та інженерно-технічні заходи захисту інформації. Забезпечення інформаційної безпеки – це сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства й держави в інформації. Форми і способи забезпечення інформаційної безпеки разом складають інструмент протидії внутрішнім і зовнішнім кіберзагрозам. Серед форм забезпечення інформаційної безпеки виділяють:

- інформаційний патронат;
- інформаційне протиборство;
- інформаційну кооперацію.

Отже, інформаційна безпека покликана захищати інформаційні системи й інформацію. Сучасні науковці переконують, що саме інформація, інформаційні системи, а також інформаційні технології є об'єктами безпеки. Відтак серед ключових загроз, негативних впливів варто визначити витік, розголошення інформації, несанкціонований доступ до такої неї. Формами ж порушення кібербезпеки є інформаційні війни та тероризм.

Задля забезпечення системного підходу до вивчення інформаційної безпеки України скористаємось SWOT-аналізом, тобто сукупним розглядом сильних і слабких сторін інформаційної війни та безпеки нашої держави (strengths and weaknesses), а також висвітлимо усі існуючі її можливості та загрози (opportunities and threats).

Проаналізувавши *сильні сторони* інформаційної безпеки України, зазначаємо, що ми одні з перших почали протистояти інформаційній війні з боку Росії, поступово навчились протидіяти всьому інструментарію кремлівської «гібридної» атаки: психологічній війні; кібервійні; мережевій війні; ідеологічній війні. При цьому увесь світ згуртувався, підтримує і вчиться у нас. За підтримки трастового фонду НАТО створено Ситуаційні центри при СБУ та Державній службі спеціального зв'язку та захисту інформації України (ДССЗЗІ). Представники України регулярно беруть участь у міжнародному співробітництві з реагування на кіберінциденти. Постійно й активно залучають місцеві громадські організації у протистояння інформаційній війні з боку РФ.

З огляду на покращення нормативно-правової бази, виокремимо основні досягнення українського уряду – проведено ряд реформ; ратифіковано Конвенцію Ради Європи про кіберзлочинність (дата ратифікації – 07 вересня 2005 р., дата набрання чинності – 01 липня 2006 р.); посилено базовий Проект Закону України «Про Концепцію державної інформаційної політики» (від 13 жовтня 2010 р.) (Закон України, 2010), зокрема йдеться про єдиний національний інформаційний простір, утвердження інформаційного суверенітету України, розвиток інформаційного суспільства, забезпечення прав на свободу слова та вільний доступ до інформації, підтримку суспільної моралі та національних інформаційних ресурсів (Закон України, 2010); внесено зміни до Закону «Про інформацію» (з останніми змінами від 16 червня 2020 р.); удосконалено Стратегію кібербезпеки України (14 травня 2021 р., «Стратегія» від 27 січня 2016 р. визнана такою, що втратила чинність); а також прийнято «Доктрину інформаційної безпеки України» (від 25 лютого 2017 р.), яка визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері (Доктрина, 2017).

Позитивно розцінюємо і реалізацію основних положень Будапештської конвенції, за умовами якої українські правоохоронці активно співпрацюють із представниками Ради Європи щодо ефективного забезпечення високого рівня протидії та розслідування кіберзлочинів. Зазначається, що кіберполіція спільно з іншими органами виконавчої влади проводить роботу з комітетами Верховної Ради України щодо приведення українського законодавства у відповідність до європейського (Рада Європи, 2020).

До сильних аспектів також віднесемо запровадження посади інформаційного омбудсмена, а також цілковите дотримання умов міжнародних домовленостей, а саме не застосування сили чи погрози силою у відповідь на провокації РФ. До переваг належить також можливість на самовизначення усіх народів, національних меншин і релігійних конфесій, що проживають на території України у всіх сферах життя і діяльності. Серед іншого варто також згадати створення сайтів, посібників та навчальних матеріалів, покликаних виявляти фейкові матеріали, протистояти негативним наративам.

Досліджуючи питання *слабких сторін* розвитку інформаційної безпеки України, варто розпочати із технічної, технологічної не готовності та надзвичайно застарілого обладнання не лише в державних органах влади. Більшість українських компаній все ще загалом не готові до нових хвиль кібератак, зокрема і з організаційних позицій, не наймають відповідних фахівців. Тривале й тісне попереднє співробітництві з РФ не давало можливості ефективному протистоянню з огляду на «відкритість» усіх існуючих систем захисту.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (5 липня 1994 р.) (Закон України, 2020) та низка нормативних документів про технічний захист інформації суттєво застаріли, а обов'язковість впровадження так званої Комплексної системи захисту інформації («Що таке КСЗІ», н.д.) органами державної влади, об'єктами критичної інфраструктури та приватними компаніями, які хочуть надавати послуги державним органам, відкидає нас назад.

Серед слабких сторін також відсутність централізованого управління силами реагування на кіберінциденти на загальнодержавному рівні, а також те, що національна система кібербезпеки обмежується переважно участю в ній силових органів (Нацполіція,

СБУ, Держспецзв'язок тощо). Все ще недостатньо ефективна система кіберрозвідки (більш відома на заході як Threat Intelligence).

Україна досі нерідко осмислюється як буферна зона поміркованого впливу, «балансу сил». Однак на перетині енергетичних, газових і дипломатичних шляхів країна все ж стала випробовувальним театром інтенсивного впливу «чорної» пропаганди, фейкових новин, що призвело до соціальної конфронтації, політичної нестабільності. Українці легко піддаються ініціюванню конфлікту, низькою є зокрема й поінформованість населення тимчасово окупованих територій, де інфогігієна не на належному рівні.

Виокремлюючи основні *загрози* інформаційні безпеці України, наголошуємо й на розвитку нових видів війни, або удосконалення старих (гібридна війна, асиметрична війна, е-джихад, iWar); новітніх засобах впливу, зброї; гібридних загрозах; посиленні новітніх компонентів гібридної війни – «мутація пристосованості» – війна свідомості.

Наступною важливою складовою є утворення сформованими «державними структурами суверенного утворення», тобто незаконними військовими регіональними формуваннями, які відділилися, військами центральної влади і найбільш активними прибічниками центру – також незаконними військовими формуваннями, які управляються місцевою адміністрацією ворожою до новоутвореного «уряду» відокремленої території. Шляхом поширення подвійних цінностей для українських громадян, значно загострюючи ворожнечу між західними та східними регіонами, спричиняють велику кількість локальних конфліктів.

Щодо міжнародного впливу на загальну ситуацію в країні, то варто наголосити на суперечностях між сучасними світовими центрами сили щодо конфлікту на території України та шляхів його вирішення, а також порушення гарантій безпеки з боку українських «захисників» на міжнародній арені та й втрата українським політикумом іміджу надійного і передбачуваного партнера на міжнародній дипломатичній арені не на останньому місці.

Зрештою, у зв'язку зі значним поширенням пандемії багато галузей знову працюють онлайн і відповідно масованість кібератак посилюється, а кількість зростає. Сьогодні кожен громадянин є суб'єктом кіберпростору, наприклад мобільний телефон або ж будь який інший гаджет, що має вихід в Інтернет, вразливий перед щоденними атаками, серед яких розповсюдженим є розсилання фішингових листів зі сумнівними пропозиціями. В цьому аспекті варто згадати і про «тюремну кіберактивність», яка за останній два роки отримала передові позиції внутрішнього пошуку протидії та боротьби.

Говорячи про *можливості* покращення інформаційної безпеки України необхідно почати з активізації та посилення міжнародного співробітництва з НАТО, ОБСЄ, ЄС, ООН в усіх сферах, також про можливість самим відстоювати власні позиції та інтереси на міжнародних переговорах, форматах співпраці і в міжнародних судах. Продовжуємо активно застосовувати європейські і міжнародні стандарти у сфері кібербезпеки, розвивати роботу спеціальних органів, які здатні ефективно взаємодіяти з відповідними органами ЄС і НАТО, коли іноземні спеціалісти постійно залучають українців до спільних навчань / тренінгів.

Серед можливих сценаріїв розглядаємо і повернення окупованих територій до складу України не силовими засобами (Мінські домовленості, Нормандська 4, Кримська платформа, Люблінський трикутник), для яких українська ситуація є свого роду «тренувальним майданчиком» по відбиттю гібридних загроз та інноваційною сферою розробки необхідних технологій і видів протистояння гібридним загрозам.

Серед потенційних можливостей покращення інформаційної безпеки України варто відзначити запровадження Центру кіберзахисту (установи, яка безперервно займається захистом державних інформаційних ресурсів), а також функціонування єдиної у нашій державі команди CERT-UA, яка є членом міжнародного форуму FIRST і постійно здійснює обмін інформацією з усіма міжнародними партнерами (Голова Держспецзв'язку, 2021).

Висновки. Отже, стан розвитку інформаційної безпеки в Україні перебуває у стані реформування та удосконалення. Розглянувши сильні та слабкі сторони, а також визначивши загрози і проаналізувавши можливості, можемо стверджувати, що основні переваги

інформаційної безпеки на стороні української держави у сфері оновлення нормативно-правової, технічної та професійної сфер. Тісне міжнародне співробітництво з ЄС та НАТО у сфері кібербезпеки, а також по відбиттю гібридних загроз призведе до повної цифровізації / диджиталізації, подолання корупції в країні, духовної і політичної єдності українського народу, а також бажання захистити не лише себе, а й свою державу від іноземного інформаційного впливу.

На нашу думку, **подальші дослідження** варто зосередити, зокрема на комплексному підході до визначення гібридних загроз та вдосконаленні усіх сучасних можливостей щодо забезпечення інформаційної безпеки України.

ВИКОРИСТАНІ ДЖЕРЕЛА:

1. Доктрина інформаційної безпеки України (2017) https://zakon.rada.gov.ua/laws/show/47/2017#Text/

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (2020) https://zakon.rada.gov.ua/laws/show/ 80/94-%D0%B2%D1%80#Text.

3. Закону України «Про Концепцію державної інформаційної політики» (2011) https://zakon.rada.gov.ua/laws/show/2897-VI#Text.

4. Закону України «Про Концепцію державної інформаційної політики» (2010) https://ips.ligazakon.net/document/LF5LF00A?an=15.

5. Толубко, В. (Ред.) (2015) *Інформаційна та кібербезпека : соціотехнічний аспект : підручник*. Київ: ДУТ. 288 с.

6. Ничипорчук, Н. та Вознюк, Є. (2018) Секрет успіху США у сфері інформаційної безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії. №1(3).* С. 66-71.

7. *Рада Європи готова до співпраці з Україною для імплементації Будапештської конвенції про кіберзлочинність* (2020) https://ua.interfax.com.ua/news/general/638709.html.

8. Шуляк, А. (2019) Інформаційна безпека. А. М. Шуляк (Ред.) *Глосарій : навч. енцикл.слов.-довід. із питань інформ. безпеки*. (130-133) Київ: МПБП «Гордон».

9. *Що таке комплексна система захисту інформації (КСЗІ)* http://altersign.com.ua/korysna-informacija/pobudova-kszi/shcho-take-kompleks na-systema-zahystu-informaciji-kszi.

10. *90% кібератак в Україні пов'язані з РФ і хакерськими групами, які фінансує російська влада – голова Держспецзв'язку* (2021) https://armyinform.com.ua/2021/06/90-kiberatak-v-ukrayini-povyazani-z-rf-i-hakerskymy-grupamy-yaki-finansuye-rosijska-vlada-golova-derzhspeczzvyazku/.

11. Bondar, Yu. (2011) Freedom of speech as a factor in information security. *The Actual problems of international relations. International Information Security : Contemporary Concepts and Practices. Issue 102 (Part I).* Kyiv. 127-129

12. Vetrov, K. & Voznyuk, Y. (2019) Information Terrorism as a Modern Threat for Information Security of European States. *Міжнародні відносини, суспільні комунікації та регіональні* студії. №1(5). 34-42.

13. Vozniuk E. (2018) *Information Terrorism as a Modern Dynamic Part of International Terrorism A. Mytko (Ed.)* [Collective monograph] International and National Security: Politics, Information, Ecology, Economy. Kyiv: MPBP «Hordon».

REFERENCES:

1. *Doktryna informatsiinoi bezpeky Ukrainy* [Doctrine of Information Security of Ukraine] (2017) https://zakon.rada.gov.ua/laws/show/47/2017#Text/. [in Ukrainian].

2. *Zakon Ukrainy «Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh»* [«On Information Protection in Information and Telecommunication Systems»] (2020) https://zakon.rada.gov.ua/laws/show/ 80/94-%D0%B2%D1%80#Text. [in Ukrainian].

3. *Zakon Ukrainy «Pro Kontseptsiiu derzhavnoi informatsiinoi polityky»* [«On the Concept of the State Information Policy»] (2011) https://zakon.rada.gov.ua/laws/show/2897-VI#Text. [in Ukrainian].

4. *Zakon Ukrainy «Pro Kontseptsiiu derzhavnoi informatsiinoi polityky»* [«On the Concept of the State Information Policy»] (2010) https://ips.ligazakon.net/document/LF5LF00A?an=15. [in Ukrainian].

5. Tolubko, V. (Red.) (2015) *Informatsiina ta kiberbezpeka : sotsiotekhnichnyi aspekt: pidruchnyk.* [Information and Cybersecurity: Socio-Technical Aspect: textbook]. Kyiv: DUT. 288 s. [in Ukrainian].

6. Nychyporchuk, N. ta Vozniuk, Ye. (2018) *Sekret uspikhu SShA u sferi informatsiinoi bezpeky.* [The Secret of US Success in the Field of Information Security]. Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii. №1(3). S. 66-71. [in Ukrainian].

7. *Rada Yevropy hotova do spivpratsi z Ukrainoiu dlia implementatsii Budapeshtskoi konventsii pro kiberzlochynnist* [Council of Europe is Ready to Work with Ukraine to Implement Budapest Cybercrime Convention] (2020) https://ua.interfax.com.ua/news/general/638709.html. [in Ukrainian].

8. Shuliak, A. (2019) *Informatsiina bezpeka.* [Information security]. A. M. Shuliak (Red.) Hlosarii: navch. entsykl.slov.-dovid. iz pytan inform. bezpeky. (130-133) Kyiv: MPBP «Hordon». [in Ukrainian].

9. *Shcho take kompleksna systema zakhystu informatsii (KSZI)* [What is a Comprehensive Information Security System] http://altersign.com.ua/korysna-informacija/ pobudova-kszi/shcho-take-kompleks na-systema-zahystu-informaciji-kszi. [in Ukrainian].

10. *90% kiberatak v Ukraini pov'iazani z RF i khakerskymy hrupamy, yaki finansuie rosiiska vlada – holova Derzhspetszv'iazku* [90% of Cyber Attacks in Ukraine are Related to Russia and Hacker Groups Funded by the Russian Government – the Head of the State Special Service] (2021) https://armyinform.com.ua/2021/06/90-kiberatak-v-ukrayini-povyazani-z-rf-i-hakerskymy-grupamy-yaki-finansuye-rosijska-vlada-golova-derzhspeczzvyazku/. [in Ukrainian].

11. Bondar, Yu. (2011) Freedom of speech as a factor in information security. *The Actual problems of international relations. International Information Security: Contemporary Concepts and Practices. Issue 102 (Part I).* Kyiv. 127-129

12. Vetrov, K. & Voznyuk, Y. (2019) *Information Terrorism as a Modern Threat for Information Security of European States.* Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii. №1(5). 34-42.

13. Vozniuk E. (2018) *Information Terrorism as a Modern Dynamic Part of International Terrorism* A. Mytko (Ed.) [Collective monograph] International and National Security: Politics, Information, Ecology, Economy. Kyiv: MPBP «Hordon».

Yevheniia Vozniuk,
Ph.D. in Political Sciences, Associate Professor,
Associate Professor of the Department for International Affairs and Regional Studies,
Faculty of International Relations, Lesya Ukrainka Volyn National University

Swot-analysis of the State of Ukraine's Information Security

The condition of the state information security is an extremely important issue for the information space of Ukraine and for the whole world, as of the constant hybrid threats range expansion. The purpose of the article is to identify the strengths and weaknesses of Ukraine's information security, explore the existing threats, and identify opportunities for their further elimination. The study used SWOT-analysis - collectively considered the strengths and weaknesses of information warfare and security of our state, as well as highlighting all its existing opportunities and threats. In conclusion, it can be noted that the theoretical and methodological foundations of the study of Ukraine's information security are considered in detail. The key concepts of information security, information warfare, information terrorism are singled out. The main directions of activity in the field of information security are covered, the main threats that

cause violations of information security categories are analyzed. Types of information wars, their components, and types are analyzed. The purpose and tools of modern ways of realization of information or cyberterrorism are characterized.

It is noted that, unlike information warfare, infoterorism is characterized by inequality of the opposing parties, which forces the weak side to use such methods and means that could use the least effort to do the most harm to the other side of the conflict. Hence, we state that information protection is an important part of maintaining the overall national security of countries.

Keywords: *information security, information war, information terrorism, SWOT-analysis, Ukraine. hybrid threats.*

https://doi.org/10.31392/NPU-nc.series22.2021.30.13
УДК 351.746

Волянюк Ольга Ярославівна,
кандидат політичних наук, доцент,
Національний педагогічний університет імені М. П. Драгоманова
volyanyuk@ukr.net; ORCID 0000-0002-1606-7416

«ПОСТПРАВДА»: БЕЗПЕКОВІ ВИКЛИКИ, НАУКОВІ ДИСКУСІЇ, ПОЛІТИЧНИЙ СЛЕНГ

Від здатності суспільства розпізнавати реальне й уявне залежать політичний розвиток і політична стабільність, міжнародна та національна безпека загалом. У статті акцентується увага на змісті поняття «постправда» – такій інтерпретації явищ / відносин / процесів (зокрема й суспільно-політичних), що не відповідає дійсності або частково спотворює її. Постістинне (постправдиве) у політичному житті свідчить про зниження уваги до фактів при окресленні стратегій політики, певну «девальвацію» першоджерел при прийнятті політичних рішень, кризу довіри на шляху розвитку демократії, миру, безпечного світу. Це інструмент політичної боротьби та сучасних воєн. Суперечливий зміст поняття, на думку авторки, потребує якісного політологічного осмислення. Проблематику проаналізовано у структурі категоріального апарату політичної науки, громадсько-політичного сленгу, а також актуальних суспільно-політичних, безпекових викликів.

Якісно роз'яснити зміст і сучасні виклики постправди допомогли міждисциплінарні підходи та методи. Опрацьовані політологічні словники та енциклопедії, офіційні документи, матеріали популярних сайтів, умовні «рейтинги» часто вживаних слів. Ретроспективний аналіз, зокрема відсилання до радянської історії дозволили з'ясувати окремі чинники поширених деформацій у розумінні феномену правди суспільством. Загалом постправдива політика характеризується як маніпулювання базовими знаннями про історію та політику, як спрощення, посилення емоційних компонентів політичних ідеологій. Це загроза порозумінню, ефективному обміну політичною інформацією, політичній соціалізації. Це випробування спільноти на грамотність і витривалість. У статті не йдеться про запровадження нового наукового поняття, але акцентується на відповідальності інтелектуального середовища перед постправдивими обставинами сучасності.

Ключові слова: *постправда, безпека, політична реальність, дезінформація, оруеллізм, політична ідеологія, політична комунікація, (само)виправдання.*

Вступ. Поява та резонанс у публічному дискурсі категорії «постправда» спонукає більшість наук, які вивчають соціум, переглянути окремі підходи та концепти. Розуміння політичних відносин і процесів не обмежується тільки вивченням формальних правил і процедур, або номінальним переліком усіх зацікавлених суб'єктів, стейкхолдерів, чи встановленням лінійних причинно-наслідкових зв'язків. Розуміння політики – це також розпізнавання у ній реальних і вигаданих сюжетів, інфоприводів і штучно маргіналізованих