ISSN 2078–4333. Вісник Львівського університету. Серія міжнародні відносини. 2019. Випуск 46 С. 169–181
Visnyk of the Lviv University. Series International Relations. 2019. Issue 46. P. 169–181

УДК 327.5
DOI 10.30970/vir.2019.46.0.10362

ПОНЯТІЙНО–КАТЕГОРІАЛЬНІ ХАРАКТЕРИСТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Марія Копійка,

Інститут міжнародних відносин
Київського національного університету імені Тараса Шевченка,
вул. Юрія Іллєнка, 36/1, м. Київ, Україна, 04119, тел. 044 481 4437,
e-mail: kopiikams@gmail.com

Розглянуто понятійно-категоріальні характеристики інформаційної безпеки у міжнародно-політичному вимірі, враховуючи якісно нове бачення архітектури міжнародної безпеки в умовах подвійного використання інформаційно-комунікаційних технологій, спрямованого на маніпулювання інформацією, викривлення інформаційної реальності та деструктивного впливу соціальних комунікацій, що обумовлює необхідність поглибленого дослідження щодо тлумачення сучасного інструментарію інформаційного протиборства. Зокрема подальшого уточнення й міжнародно-правового закріплення потребують поняття «інформаційна безпека», «інформаційні загрози», «інформаційні озброєння», «інформаційні війни», оскільки уже існує досвід їх застосування, так і новітніх понять, таких як «мова ворожнечі», кліктивізм, хактивізм, тролінг, «фейки», бот-мережі, які стосуються інформаційно-психологічного впливу на мотивацію політичної поведінки сучасного суспільства. З'ясування ролі комунікативного інструментарію у сфері безпеки дозволило виокремити його характерні особливості та засоби використання міжнародними акторами для просування пріоритетних інтересів на міжнародній арені. Можливості інноваційних засобів протиборства, з авторського погляду, мають неоднозначні наслідки для інформаційної безпеки України, оскільки вони впливають на безпеку і оборону держави, демократизацію державного управління, вирішення кризових ситуацій, забезпечують протидію деструктивній пропаганді і водночас формують нові типи поляризації у суспільстві, а також спричиняють маргіналізацію окремих верств суспільства у сучасному розвитку країни. Зміна парадигми інформаційної безпеки зумовила і зміну чинників, базових для здійснення безпекової політики, та перегляд інструментарію для забезпечення інформаційного суверенітету та національних інтересів держави.

Ключові слова: інформаційна безпека; інформаційні загрози; «мова ворожнечі»; кліктивізм; хактивізм.

.

Актуальність дослідження зумовлена процесами трансформації системи міжнародної безпеки, зміною інформаційної парадигми безпекової політики, модернізацією інформаційних озброєнь та активізацією гібридних конфліктів з інноваційним інструментарієм інформаційного впливу, що створює нові підходи до понятійно-категоріального апарату інформаційної безпеки в умовах глобального інформаційного протиборства і забезпечення національних інтересів держав. Визначальними для дослідження стали наукові праці відомого американського політолога Дж. Ная–мол., одного з основних розробників концепту інформаційної безпеки, який виявив наявність широкого спектру інформаційних загроз, які за своїми характеристиками переважають можливості оборони суверенних держав, що викликає необхідність протидії таким загрозам на зовнішньому і внутрішньому рівні функціонування держави [1; 2; 3; 4].

Аналіз зарубіжних наукових теорій щодо інформаційної безпеки уможливив бачення сутності її основних понять і класифікації інформаційного інструментарію у безпековій сфері. Так, у фахових розвідках зазначається, що перші понятійні характеристики інформаційної безпеки було представлено у «Веселкових книгах»– серіях стандартів, опублікованих у США (1980–1990), серед яких виокремлюється розробка «Критерії оцінки надійних комп'ютерних систем» (*англ.* «Trusted Computer System Evaluation Criteria» TCSEC), де визначаються засоби, що мають бути включеними в комп'ютерну систему для безпечної обробки критичної інформації, тобто йшлося про технічні стандарти кібербезпеки для систем спеціального і військового призначення. Водночас у 1986 р. було розроблено загальні «Європейські критерії безпеки інформаційних технологій» (англ. Information Technology Security Evaluation Criteria (ITSEC)), якими було вперше введено поняття «адекватності засобів захисту» і значно розширено сферу їх застосування, враховуючи захист інформації від несанкціонованого доступу задля забезпечення конфіденційності та цілісності інформації, захисту її від несанкціонованої модифікації або знищення, а також для забезпечення працездатності систем щодо протидії загрозам відмови в обслуговуванні [5; 6].

До вивчення концепту інформаційної безпеки у міжнародному вимірі зверталися такі відомі зарубіжні фахівці, як Р. Армітідж, Д. Арквілла, С. Бальді, Зб. Бжезинський, Дж. Гарстка, Е. Гельбштейн, Е. Говард, Й. Курбалія, М. Лібіцкі, У. Лінн, С. Манн, Д. Місслер, Дж. Най-мол., У. Оуенс, А. Себровскі, О. Тоффлер, Ф. Хоффман, Д. Шарп, Р. Шафранські, М. Шнайдер тощо, які визначили основні поняття інформаційної безпеки та її складових, розробили теорії інформаційного протиборства та використання інструментарію інформаційної безпеки у сфері міжнародної політики. Вітчизняні науковці А. Баровська, Р. Власенко, Л. Гнатюк, О. Гребініченко, О. Грицун, Д. Дубов, Є. Камінський, І. Коваль, Б. Кормич, О. Литвиненко, В. Ліпкан, Є. Макаренко, М. Ожеван, В. Петров, І. Погорська, Г. Почепцов, М. Рижков, Ю. Романчук, О. Соснін, Г. Яворська тощо досліджували понятійно-категоріальний апарат інформаційної безпеки, розглядаючи безпековий інструментарій у форматі його застосування в міжнародних відносинах. У вказаних наукових розвідках було

представлено сутнісні характеристики інформаційної безпеки, визначено специфіку підходів до проблеми інформаційної безпеки на глобальному, регіональному та національному рівнях функціонування політичних систем, проаналізовано інструментарій інформаційного протиборства.

Слід зазначити, що швидкоплинні зміни безпекового середовища і поява новітніх засобів інформаційного впливу наразі потребують систематизації і новітнього тлумачення понятійно-категоріальних характеристик інформаційної безпеки з огляду на їх еволюцію та інноваційні засоби використання в міжнародних відносинах, оскільки у науковому дискурсі присутні як ретроспективні, так проспективні розвідки щодо визначення як власне інформаційної безпеки, так і окремих її складових.

Мета статті полягає у дослідженні сучасного концепту інформаційної безпеки як важливого і ключового чинника взаємодії міжнародних акторів у глобальному середовищі.

Зазначимо, що теорія і практика міжнародного співробітництва у сфері інформаційної безпеки зумовила відповідну термінологію та зміст основних понять, зафіксованих в міжнародних документах ООН та її спеціалізованих установ, у документах регіональних організацій, в стратегіях національної безпеки провідних країн світу. Так, у Документі A/54/213 ГА ООН «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» було запропоновано для обговорення тлумачення поняття «інформаційна безпека», яке визначалося як «стан захищеності основних інтересів особистості, суспільства і держави в інформаційному просторі, включаючи інформаційно-телекомунікаційну інфраструктуру і власне інформацію щодо таких її властивостей як цілісність, об'єктивність доступність і конфіденційність», а також суміжних понять, таких як «інформаційна війна», «інформаційна зброя», «інформаційні загрози», «інформаційний тероризм», «інформаційна злочинність», «несанкціоноване втручання», «критично важливі структури», «міжнародна інформаційна безпека» тощо. При цьому поняття «міжнародна інформаційна безпека» визначалося як «стан міжнародних відносин, що виключає порушення світової стабільності і створення загрози для безпеки держав і міжнародного співтовариства в інформаційному просторі». Водночас упродовж сесій ГА ООН (2007–2013 рр., а також 2014–2019 рр.), держави-члени міжнародної організації інформували Генерального Секретаря ООН про свою позицію щодо власного розуміння інформаційної безпеки, заходів на національному рівні для зміцнення інформаційної безпеки і сприяння міжнародному співробітництву в цій сфері, щодо змісту відповідних стратегій, спрямованих на безпеку глобальних інформаційних і телекомунікаційних мереж та щодо забезпечення інформаційної безпеки на глобальному рівні. Відтак, на думку експертного співтовариства, узгодження та універсального тлумачення потребують базові поняття міжнародної інформаційної безпеки, що зумовлюють колізії у міжнародних відносинах [7; 8].

Розгляд наукових підходів до змісту цих понять засвідчив, що науковці, які використовують поняття «міжнародна кібербезпека», враховують лише

технічний її аспект, підкреслюючи проблему захисту цілісності, доступності та конфіденційності самої інформації, інформаційно-комунікаційних технологій, інформаційних систем, доступності та цілісності глобальних мереж та критично важливої інфраструктури. Програмним з питань кібербезпеки вважається виступ в Університеті Перд'ю тодішнього кандидата в президенти США Б. Обами 16 липня 2008 р., в якому він наголосив, що саме кібербезпека є складовою національної оборонної стратегії, оскільки після 11 вересня 2001 р. ситуація в сфері міжнародної безпеки і на північноамериканському континенті докорінно змінилася з огляду на появу нових видів загроз, до яких відносять і кібернетичну загрозу. Визначаючи пріоритетність кібербезпеки у XXI ст., Б. Обама за свого президенства сприяв реалізації національної політики кібербезпеки, залучав до розробки нових стандартів і рішень з проблем інформаційної безпеки як державні структури, так і академічні кола й приватних фахівців, враховуючи, що комп'ютерні мережі та інфраструктура є стратегічними активами країни, від захищеності яких залежить безпека ефективного державного управління та життєдіяльність американського суспільства. Варто підкреслити, що у стратегічному плані Б. Обами з кібербезпеки йшлося не лише про заходи превентивно-оборонного характеру, але й про наступальну «інформаційну зброю» – перехоплення повідомлень на лінях зв'язку включно з Інтернетом, руйнування чужих інформаційних систем, протидію зовнішнім інформаційно-психологічним впливам. Оскільки план вважався конфіденційним, у відкриту пресу потрапляли лише окремі його фрагменти. Принциповою новизною ініціативи кібербезпеки стала мілітаризація питань інформаційної безпеки, що означало залучення до програми обороноздатності держави такої військової структури, як Національна агенція безпеки, а реалізацію програми кібербезпеки було запропоновано компаніям Lockheed Martin, Boeing, Raytheon, Symantec і Mcafee, що є основними партнерами Пентагону, які надають необхідні ресурси для розгортання діяльності у відносно нових напрямах забезпечення національної безпеки США. Крім того, тодішній президент США підтримав фінансування низки дослідницьких проектів з розробки нових технологій і засобів інформаційної безпеки зі створюваного 5-мільярдного фонду, спрямованого саме на реалізацію нової стратегії національної безпеки держави [9].

Інші фахівці, які розглядають поняття «міжнародна інформаційна безпека», враховують змістовну та технічну характеристики інформаційної безпеки, включаючи до тлумачення поняття засоби психологічного впливу та поширення негативного контенту. Фактично «міжнародна інформаційна безпека» визначається як «взаємодія акторів міжнародних відносин з операцій підтримання миру та захисту міжнародного інформаційного середовища, глобальної комунікаційної інфраструктури та суспільної свідомості світової спільноти від реальних і потенційних інформаційно-психологічних і кібернетичних загроз; як стан міжнародних відносин, що виключає порушення міжнародної стабільності і створення загрози для безпеки держав і світового співтовариства в інформаційному просторі» [10].

Згідно із зазначеним визначенням розглядалася концепція «м'якої сили» Дж. Ная–мол., в межах якої для підтримки національних інтересів США в міжнародних відносинах було віднесено не лише політичну ідеологію, зовнішню політику, суспільні цінності, а й інформаційно-технологічну потугу держави. У науковій праці «Покликання до лідерства. Природа американської потуги, що змінюється» (1990) Дж. Най зазначав, що абсолютна перевага США полягає не тільки у показниках військової сили й економічної могутності, а й у несиловому впливі на міжнародні відносини. Крім того, у науковій праці авторства Дж. Ная та У. Оуенса «Головна сила Америки – її інформаційні можливості» було запропоновано концепцію «інформаційної парасолі» для країн світу, враховуючи домінуючу роль США у розробці і використанні стратегічних засобів комунікації й інформаційних технологій та у політиці стримування й нейтралізації традиційних воєнних загроз і нових видів озброєнь [11; 12].

Складовою категорією міжнародної інформаційної безпеки вважається поняття «інформаційні загрози», яке тлумачиться як «інформаційно-технологічні, інформаційно-комунікаційні, інформаційно-психологічні інструменти, що створюють небезпеку для інтересів акторів міжнародних відносин у світовому інформаційному просторі і реалізуються через порушення інфраструктури, вільного обігу інформації, неправомірність використання інформаційних ресурсів». На погляд дослідників міжнародної інформаційної безпеки, «інформаційні загрози стосуються всього людства в цілому, кожного регіону, кожної держави, тобто мають глобальний характер; ці загрози виступають як потенційний чинник конфліктогенності та асиметрії інформаційного розвитку світу; проблеми протидії інформаційним загрозам потребують для свого вирішення постійного міжнародного співробітництва, максимальних об'єднаних зусиль світової спільноти, оскільки невирішеність цих проблем створює загрозу для системи підтримання миру і стабільності». Відповідно виділяються інформаційні загрози для критично важливих сфер життєдіяльності держави і суспільства військово-політичного, соціально-економічного, науково-технологічного, суспільно-культурного, терористичного та злочинного характеру, тобто як протиправні дії, спрямовані на руйнування життєво важливих інфраструктур, систем управління державою, морального стану суспільства та війська, порушення прав людини [13; 14].

До категорій міжнародної інформаційної безпеки відносять також поняття «інформаційні озброєння», яке тлумачиться як «комплекс технічних та інших заходів, методів і технологій, спрямованих на встановлення контролю над інформаційними структурами потенційного супротивника, втручання у роботу його систем управління, інформаційних мереж та комунікацій з метою руйнування або модифікації даних, дезінформації, поширення інформації спеціального призначення у системах формування громадської думки і прийняття рішень, а також як сукупність засобів впливу на свідомість і психологічний стан політичних і військових структур, спецслужб та населення для протидії можливим інформаційним впливам іншої сторони». У науковий обіг поняття «інформаційні озброєння було уведено Р. Шафранскі, який у

дослідженні «Теорія інформаційної війни. Готуючись до 2020 року» підкреслював їх суттєві відмінності від фізичних озброєнь, оскільки засоби ведення інформаційної війни можуть бути використані як проти зовнішніх, так і проти внутрішніх противників. Інформаційні озброєння, на думку Р.Шафранскі, за своєю природою є асиметричними, їх можна замаскувати під інші види деструктивних інформаційних впливів, а нарощування воєнно-інформаційного потенціалу можна видати за «наслідки науково-технічного прогресу» [15].

Поняття «інформаційні війни» також вважається категоріальною характеристикою міжнародної інформаційної безпеки і тлумачиться як «форма міждержавного протиборства, яка реалізується з використанням інформаційного впливу на системи управління різного призначення інших держав, а також на політичну владу і суспільство в цілому, на інфраструктуру і засоби масової комунікації для досягнення переваг з одночасним захистом національної інформаційної сфери від аналогічних дій». Проблема еволюції війни в інформаційному суспільстві з'ясовується у роботі О. Тоффлера та Х. Тоффлер «Війна і антивійна: виживання в XXI столітті», в якій стверджується, що «нації ведуть війну таким же чином, яким вони створюють багатства», тому для кожної хвилі розвитку цивілізації характерним є свій особливий тип війни. Типовим прикладом ведення війн нового покоління, зазначається у науковій праці, була операція США проти Іраку, в якій «американські війська поєднали досягнення інформаційної, радіоелектронної і власне збройної боротьби з використанням новітньої авіаційної та ракетної техніки» [16].

Авторський підхід до сучасної інформаційної війни представлено у науковій праці А. Себровскі і Дж. Гарстки «Мережно-центрована війна: її походження та майбутнє», в якій підкреслюється, що в умовах глобалізації і розвитку інформаційних технологій з'являються нові форми протиборства, які дозволяють перейти до більш швидкоплинної й ефективної форми боротьби, для якої характерні інформаційна перевага військ, більш високий рівень усвідомлення і більш глибоке розуміння ситуації на полі бою через впровадження нових систем управління і комп'ютерного моделювання, що позбавляє противника можливості вдаватися до будь-яких дій у відповідь і введення його у стан шоку за допомогою інноваційних інформаційних озброєнь [17].

Важливим для понятійно-категоріальних характеристик міжнародної інформаційної безпеки є поняття «гібридна війна», що уведено в науковий обіг американським дослідником Ф. Хоффманом і тлумачиться як «сучасний тип конфлікту, який передбачає поєднання різних способів та типів ведення війни». Гібридні війни визначаються як мультимодальні, оскільки передбачають поєднання класичних методів ведення війни з використанням регулярних військових сил та спеціальних підрозділів і некласичних методів з використанням нерегулярних сил, різноманітного типу збройних формувань, з підтримкою внутрішніх конфліктів, спротиву, опозиції, протестних рухів, із застосуванням методів економічного впливу, дипломатичних механізмів, терористичних атак та кримінального хаосу, а також методів і прийомів

інформаційного протиборства, пропаганди та кібервійни. Гібридні війни як форма інформаційного протиборства передбачають використання можливостей інформаційних озброєнь на окремих територіях з метою організації внутрішнього конфлікту між опозиційними силами (політичні, сепаратистські, міжнаціональні конфлікти) і трансформації національного управління [18; 19].

Поняття «міжнародний інформаційний тероризм» у форматі міжнародної інформаційної безпеки розуміється як «використання телекомунікаційних та інформаційних систем і ресурсів та вплив на такі системи і ресурси в міжнародному інформаційному просторі в терористичних цілях». Терористичні угруповання, зазначається у численних наукових дослідженнях, вдаються до більш досконалих, видовищних і жорстоких засобів інформаційно-психологічного впливу через використання ресурсів національних і глобальних медіа, що досягається здійсненням активної інформаційно–пропагандистської діяльності шляхом значного поширення інформації та дезінформації про руйнівні наслідки терористичних акцій, про загрози подальшого здійснення актів тероризму без вказівки конкретного об'єкта, про нанесення терористичних ударів по особливо важливим для життєдіяльності суспільства і безпеки населення об'єктам з метою залякування населення, деморалізації правоохоронних органів, державних посадовців, конкретних політичних супротивників. За своїми масштабами і дієвістю інформаційно-пропагандистські акції терористичних угруповань, до яких відносять Аум Шінрікьо (Японія), Хамас (Палестина), Хезболлах (Ліван), Аль-Каїду (Пакистан), ІДІЛ (Ірак), Талібан (Афганістан) тощо, відіграють значну роль в загальній структурі терористичної діяльності, що потребує створення ефективної системи антитерористичної контрпропаганди [20].

Останнім часом до категорій міжнародної інформаційної безпеки включають такі поняття, як «мова ворожнечі» (англ. Hate speech), «кліктивізм» (англ. Clicktivism), хактивізм (англ. Hacktivism), «гостра сила» (англ. Sharp power). «Мову ворожнечі» тлумачать як «практику агресивних висловлювань, в яких принижуються чи дискредитуються представники суспільства за різними ознаками – політичними, расовими, релігійними, гендерними, соціальними, культурними». На думку політолога з Портландського університету (США) В. Кертіса, типова «мова ворожнечі» вважається викликом для сучасних ліберальних суспільств, які підтримують свободу слова і соціальну рівність, оскільки «агресивні висловлювання пов'язані з пропагандою негативних стереотипів і спрямовані на розпалювання ненависті і насильства між окремими групами та спільнотами». З огляду на проблему нетолерантного ставлення спільнот європейських країн до масового притоку мігрантів, в ЄС було започатковано Європейську програму боротьби з «мовою ворожнечі», якою вважаються всі форми самовираження, що включають «поширення, провокування, стимулювання або виправдання расової ненависті, ксенофобії, антисемітизму або інших видів ненависті на підставі нетерпимості, включаючи нетерпимість у вигляді агресивного націоналізму чи етноцентризму, дискримінації або ворожнечі щодо меншин, мігрантів і осіб з емігрантським

корінням». Крім того, у рамках програми боротьби з «мовою ворожнечі» в мережі Інтернет найбільші ІТ–компанії Facebook, Twitter, YouTube і Microsoft підписали кодекс, який зобов'язує їх запобігати поширенню «мови ворожнечі», відстежувати появу в соціальних мережах висловлювань, що розпалюють ненависть, і протягом 24 годин видаляти їх [22; 22].

На теренах України «мова ворожнечі» створює атмосферу агресії в окупованому Криму, яка «спрямована насамперед проти українців загалом – як людей, так і політичної спільноти, проти кримських татар, мусульман, мігрантів, а також активістів Євромайдану». Аналіз проросійських мас-медіа в Криму свідчить про 718 прикладів поширення «мови ворожнечі», причому 479 з них було знайдено у новинах російських телеканалів, спрямованих проти українців взагалі або тих, хто проживає в контрольованій урядом Україні. Водночас засоби масової інформації та веб–сайти неправомірних кримських «державних органів» заохочували використання «мови ворожнечі» до національних і етнічних груп (виявлено 36 таких груп) і мешканців певних територій [23]. Експерти зазначають, що масове використання «мови ворожнечі» в інформаційному просторі України грубо порушує українські та міжнародні норми права і журналістські стандарти. Інформацію про поширення «мови ворожнечі» в Криму, зазначається у дослідженнях, можна використати як доказ у Міжнародному суді ООН для підтвердження етнічної дискримінації, пропаганди насильства з використанням адміністративних, фінансових та інших ресурсів РФ і окупаційної влади для законного переслідування і пропорційно покарання [24]. Українські експерти звертають увагу, що в Кримінальному кодексі країни є статті про наклеп, про образу честі, гідності і ділової репутації, які також можуть бути використані в боротьбі проти «мови ворожнечі». Наразі розширення української інформаційно–комунікативної присутності в інформаційному середовищі держави та у свідомості спільноти тимчасово окупованих територій може зумовити зміцнення національної ідентичності та взаєморозуміння політичної влади з населенням Криму та Сходу України.

Поняття «кліктивізм» увійшло до Оксфордського словника у 2011 р. і тлумачиться як «використання соціальних медіа та інших інтернет-методів для просування будь-якої діяльності чи процесу» [25]. Зростання впливу соціальних та інших цифрових засобів масової інформації призвело до того, що громадські організації використовують Інтернет для проведення передвиборної агітації, а тому обмежують кліктивізм виключно просуванням кандидатів або партій, а також програм діяльності таких організацій. На думку дослідників, кліктивізм не є виключно підтримкою або просуванням діяльності громадських організацій в мережі Інтернет. Скоріше йдеться про форми підтримки в соціальних мережах таких заходів, як організація протестів (Єгипет, 2011 р.); сприяння бойкоту (бойкот цілих продуктів); підписання петицій (клопотання про морські заповідники від Грінпіс та на сайті Avaaz); хактивізм (робота Google з Say Now, щоб обійти цензуру Twitter в Єгипті); краудфандінг (kiva.org або kickstarter); онлайн пародія і сатира (Yes Men style пародії на Koch Industries); бомбардування Google (кампанія Сантома у Dan Savage) в обхід відключень

новин/інформування людей (протести Gezi Park). Показником підвищеного інтересу до он–лайн активності кліктивістів є сервіс Change.org, створений 2006 р. випускниками Стенфордського університету, що об'єднав 17 млн користувачів для створення он–лайн петицій. Одним з відомих значних досягнень цього сервісу було задоволення петиції щодо скасування запланованої щомісячної комісії в розмірі п'яти доларів США на користь Bank of America. Тобто, йшлося про те, що для прояву власної громадянської позиції потрібен майже один клік – звідки й започатковано поняття – «кліктивізм». Сучасна дослідниця кліктивізму Е. Говард зазначає, що з розвитком соціальних мереж «кліктивізм» безпосередньо впливає на політиків і стає прототипом прямої «електронної» демократії, оскільки Інтернет і блогосфера наразі відіграють вирішальну роль у політичному та соціальному житті світового співтовариства. Так, масові виступи проти влади в Тунісі, Єгипті, Бахрейні та Лівії координувалися за допомогою соціальних мереж. Водночас влада, прагнучи дезорганізувати протестувальників, перекривала доступ до Фейсбука, Твітера, а подекуди до мережі Інтернет загалом. До країн, в яких було використано Інтернет для протестів проти уряду, відносять також Іран, Ємен, Алжир, Марокко, Саудівську Аравію, Молдову, Грузію й Україну [26].

Поняття «хактівізм», що тлумачиться як «використання комп'ютерів та комп'ютерних мереж для просування політичних ідей, свободи слова, захисту прав людини і забезпечення свободи інформації», було введено учасником «Omega» медіаорганізації Cult of the Dead Cow. Філософія хактівізму ґрунтується на ідеї про високу ефективність використання інформаційних технологій в протестному русі і, зокрема, в акціях громадянської непокори. Серед відомих угруповань хактивістів, які визначають себе політично вмотивованими, діють Anonymous, Chaos Computer Club, Cult of the Dead Cow, Projet Chanology, Telecomix, LulzSec [27]. За свідченням директора з досліджень і розвідки однієї з найбільших світових телекомунікаційних компаній Verizon В.Бейкера, щорічний аналіз витоку даних виявив різке зростання політично вмотивованих атак хактивістів, зокрема за участю хакерського угруповання Anonymous та її технічних підрозділів Antisec і LulzSec. Викрадення даних стало інструментом політичного протесту, зазначає В. Бейкер, проти якого складно розробити відповідний захист, оскільки в кожному конкретному випадку хактивісти використовують спеціально розроблені методи і тактику [28].

Деякі дослідники хактивізму, зокрема С. Балді, Д. Кунерт, Е. Гельбштейн, Е. Говард, Й. Курбалія, виділяють три групи хактивістів за методами використання технологій у кіберпросторі: 1) для поширення інформації, 2) для створення труднощів у роботі інтернет-мереж, 3) для злому та руйнування кіберсистем (поширення вірусів, створення фейкових сайтів). Інша група дослідників підкреслює мирні цілі та засоби хактивістів, коли йдеться про відмінності хактивізму від кібертероризму, оскільки хактівізм, на їхній погляд, просуває ідеї або протести проти несправедливих законів та організацій. Дослідники Е. Гудрам і М. Меніон визначають хакерські атаки, здійснені в політичних цілях, як соціально обумовлені і етично виправдані, бо такі дії, на їх

думку, не завдають шкоди комп'ютерним системам і не приносять матеріальної вигоди хактивістам. Зважаючи на відсутність нормативної та етичної бази, у політичному дискурсі ведуться суперечки про те, наскільки виправданими є акти громадянської непокори хактивістів в мережі та про межі політичного протесту в мережі Інтернет. Так, хакери використовували мережі для засудження військових дій як Югославії, так і НАТО шляхом порушення роботи урядових комп'ютерів і отримання контролю над сайтами. У 1999 р. газета Los Angeles Times писала, що Косовський конфлікт перетворив кіберпростір в нематеріальну військову зону, де «битва за розуми і серця» ведеться за допомогою електронних зображень, групових поштових розсилок і хакерських нападів [30]. Характеризуючи протестні дії в соціальних мережах, Е. Пратканіс, професор Каліфорнійського університету Санта Крус, зазначав: «…те, що ви бачите зараз – це тільки перша хвиля того, що дуже скоро стане важливим, високоорганізованим інструментом у старій традиції пропаганди військового часу… це повинно, якщо вже не принесло, то принести занепокоєння військовим стратегам» [31]. Наразі вважається, що хактивізм вплинув на міжнародну безпеку і правове середовище, оскільки, здійснюючи атаки з території однієї держави проти іншої, хакери залишаються нерозкритими і не можуть бути притягнутими до відповідальності. Водночас активна діяльність хакерських організацій призвела до того, що держави прагнуть зміцнити інтернет–інфраструктури та впровадити стратегії захисту від кіберзагроз. На міжнародному рівні кілька країн, включаючи США, об'єднали зусилля щодо укладення у сфері кібербезпеки взаємних угод про юридичну допомогу, екстрадиції, розмежування розвідувальних повноважень, уніфікації законів таким чином, щоб хакери могли переслідуватися в судовому порядку навіть у випадку транскордонного нападу, практично у межах захисту міжнародної інформаційної безпеки.

Загалом, зазначається у науковому дискурсі, підходи дослідників до концепту інформаційної безпеки «враховують інформаційну парадигму глобального розвитку, яка є відображенням нових закономірностей формування сучасної системи міжнародних відносин і відповідно потребує новацій щодо забезпечення міжнародного миру і стабільності та досягнення переваг в інформаційному протиборстві».

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Nye J. Jr.* Soft Power. The Means to Success in World Politics / Joseph S. Nye. – New York : Public Affairs, 2004. – 192 p.

2. *Nye J. Jr.* Get Smart. Combining Hard and Soft Power [Electronic resource] / Joseph Nye // Foreign Affairs. – 2009. – Volume 88, № 4. – Access mode : http://www.foreignaffairs.com/articles/65163/joseph-s-nye-jr/get-.

3. *Nye J.S.* A smarter, more secure America. Report of the CSIS Commission on Smart Power [Electronic resource] / Craig Cohen, Joseph S. Nye, Richard Armitage. – Access mode : http://csis.org/publication/smarter-more-secure-america.

4. *Nye J. Jr.* How Sharp Power Threatens Soft Power. Retrieved from [Electronic resource]. – Access mode : https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power.

5. Trusted Computer System Evaluation Criteria [Electronic resource]. – Access mode : https:// src. nist. gov/ csrc/ media/ publications/ conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs- papers/ dod85.pdf.

6. Information TechnologySecurity EvaluationCriteria (ITSEC) [Electronic resource]. – Access mode : https:// www.ssi .gouv.fr/ uploads/2015/ 01/ITSEC-uk.pdf.

7. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Доклад Генерального секретаря ООН 10 августа 1999 г. [Электронный ресурс] Организация Объединенных наций // Режим доступа : https://digitallibrary.un.org/record/286090/files/A_54_213-RU.pdf.

8. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности Документ A/68/98 [Электронный ресурс]. – Режим доступа : http:// un.org.

9. Barack Obama's speech at the University of Purdue (July 16, 2008) [Electronic resource]. - Access mode : http://www.cfr.org/publication/16807/barack_obamas_speech_at_the_university_of_purdue.html.

10. *Gompert D.C.* National Security in the Information Age [Electronic resource] / D. C. Gompert. – Published by RAND Santa Monica, CA. – Access mode : http://www.rand.org/pubs/reprints/RP736.html.

11. *Nye J. S.* Bound to Lead: The Changing Nature of American Power / Joseph S. Nye. – New York : Basic Books, 1990. – 336 p.

12. *Nye J. S., Owens W. Jr.* America's Informational edgel Strategy and force planning / Faculty, National Security Decision Making Department, Naval War College. – 460 p.

13. *Brzezinski Z.* Between Two Ages: America's Role in the Technetronic Era / Zbigniew Brzezinski. – New York : The Viking Press, 1970. – 123 p.

14. *Макаренко Є. А.* Інформаційні чинники міжнародної політики безпеки / Є. А. Макаренко// Міжнародні інформаційні відносини. – Київ : Наша культура і наука, 2002. – С. 269–318.

15. *Shafransky R. A.* Theory of Information Warfare. Preparing for 2020. – Airpower Journal, 1995, Spring, P. 37–43.

16. *Toffler A. and H. Toffler*. War and Anti–War: Survival at the Dawn of the 21st Century / A. Toffler, H. A. Toffler. – Boston : Grand Central Publishing, 1995. – 370 p

17. *Cebrovski A., Garstka J.* Network–Centric Warfare: Its Origin and Future [Electronic resource] / A. Cebrovski, J. Garstka // Proceedings. – 1998. – January. – Access mode : http://www.kinection.com/ncoic/ncw_origin_future.pdf.

18. *Hoffman F.* Hybrid vs Compound War [Electronic resource] / Frank G. Hoffman // Small Wars Journal. – 2009. – October. – Access mode : http://smallwarsjournal.com/blog/journal/docs–temp/189–hoffman.pdf.

19. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. / за заг. ред. А. Баровської – Київ : НІСД, 2016. – 109 с.

20. Network Technologies for Networked Terrorists. Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations [Electronic resource] /

B. W. Don, D.R. Frelinger, S. Gerwehr, E. Landree, B.A. Jackson. – Published by RAND Santa Monica, CA. – Access mode : http:/ /www. rand. org/ pubs/technical_reports/TR454.html.

21. *Curtis W. M.* Hate speech [Electronic resource]. – Access mode : https://www.britannica. com/topic/hate-speech.

22. Hate speech and violence [Electronic resource]. – Access mode : https://www.coe.int/en/web/european-commission-against-racism-and-intolerance/hate-speech-and-violence.

23. Hate Speech in the Media Landscape of Crimea: An Information and Analytical Report on the Spread of Hate Speech on the Territory of the Crimean Peninsula (March 2014 – July 2017) / under the general editorship of I. Sedova and T. Pechonchyk. – Kyiv, 2018. – 40 p.

24. *Coynash H.* Russia uses hate speech to stir up fear and hatred of Ukrainians in occupied Crimea [Electronic resource]. – Режим доступу: http:// khpg. org/en/ index. php? id=1522717595

25. Clicktivism [Electronic resource]. – Access mode : https:// en.oxforddictionaries. com/ definition/clicktivism.

26. *Howard E.* How 'clicktivism' has changed the face of political campaigns [Electronic resource]. – Access mode : https://www.theguardian.com/society/2014/sep/24/clicktivism-changed-political-campaigns-38-degrees-change.

27. *McCormick T. Hacktivism: A* Short History [Electronic resource]. – Access mode : https://foreignpolicy.com/author/ty-mccormick/.

28. Ідейні хакери крадуть більше даних, ніж кіберзлочинці – дослідження [Електронний ресурс]. – Режим доступу : https:// www.bbc.com/ ukrainian/ science/ 2012/03/ 120322 _hacktivism_ko.

29. *Baldi S., Gelbstein E., Kurbalija J.* Hacktivism, cyber-terrorism and cyberwar: the activities of the uncivil [Electronic resource]. – Access mode : https:/ /baldi. diplomacy. edu/italy/isl/Hacktivism.pdf.

30. *Kuhnert D.* Hacktivism in the 2019 Political Landscape: An infosec consultant's response to Reuters' piece on Beto O'Rourke [Electronic resource]. – Access mode : https://dev.to/kuhnertdm/hacktivism-in-the-2019-political-landscape-an-infosec-consultants-response-to-reuters-piece-on-beto-orourke-1m03.

31. *Pratkanis, A. R., & Aronson, E.* Age of Propaganda: The Everyday Use and Abuse of Persuasion Holt Paperbacks, 2001. – 432 p. – P. 171.

Стаття надійшла до редколегії 10.04.2019
Прийнята до друку 20.04.2019

CONCEPTUAL CATEGORIES OF INFORMATION SECURITY

Maria Kopiika

Institute of International Relations,
Taras Shevchenko National University of Kyiv,
36/1, Y. Illienka Str., Kyiv, Ukraine, 04119, tel.044 481 4437,
e-mail:kopiikams@gmail.com

The article deals with the conceptual and categorical characteristics of information security in the international political dimension, taking into account a qualitatively new vision of the architecture of international security in the conditions of dual-use of information and communication technologies, directed manipulation of information, distortion of information reality and destructive influence of social communications that determine the necessity of research on the interpretation of modern information confrontation tools. In particular, further refinement and international legal support require the definitions of «information security», «information threats», «information weapons», «information wars», because already existed experience of their using, as well as a new concepts such as «hate speech», clicktivism, hacktivism, trolling, fakes, botnets that relate to information and psychological influence on the motivation of political behavior in modern society. Explaining the role of communication tools in security

has allowed to distinguish its specific using features and means by international actors for promoting priority interests in the international arena. Possibilities of innovative means of confrontation, from the author's viewpoint, have ambiguous consequences for the information security of Ukraine, as they affect the security and defence of the state, democratization of public administration, solution of crisis, provide counteraction to destructive propaganda and at the same time form new types of polarization in society, as well as the marginalization of some societies groups in the modern development of the country. The changes in the information security paradigm have also led to a change in the factors, underlying security policy implementation, and a revision of tools for ensuring information sovereignty and national interests of the state.

***Key words**:* information security; information threats; «hate speech»; clicktivism; hacktivism.