20. Тертишник В. М. Концептуальні проблеми кримінального процесу сьогодення / В. М. Тертишник // Вісник Академії митної служби України. – Серія: "Право". – 2013. – № 2 (11). – С. 129–133.

21. Тертишник В. М. Кримінальний процес України. Загальна частина : підручник. Академічне видання / Тертишник В. М. – К. : Алерта, 2014. – 440 с.

22. Уваров В. Г. Застосування практики Європейського Суду з прав людини та норм міжнародно-правових актів в удосконаленні кримінального судочинства України : монографія / В. Г. Уваров ; за заг. ред. доктора юрид. наук В. М. Тертишника. – Дніпропетровськ, 2012. – 268 с.

23. Хахуцяк О. Ю. Речові докази у новому Кримінальному процесуальному кодексі України / О. Ю. Хахуцяк // Адвокат. – 2013. – № 6. – С. 46–48.

24. Шумило М. Є. Поняття "докази" у Кримінальному процесуальному кодексі України: спроба критичного переосмислення ідеології нормативної моделі / М. Є. Шумило // Вісник Верховного Суду України. – 2013. – № 2. – С. 40–48.

25. Яновська О. Змагальні засади процесу доказування в кримінальному провадженні / О. Яновська // Юридична Україна. – 2013. – № 8. – С. 77–82.

✧ ✧ ✧ ✧ ✧ ✧ ✧

УДК 340.12-049.5

Ю. С. Размєтаєва, кандидат юридичних наук,
асистент кафедри теорії держави і права
Національного юридичного університету
ім. Ярослава Мудрого

КІБЕРВІЙНА: ЗАГАЛЬНОТЕОРЕТИЧНІ АСПЕКТИ

Присвячено загальнотеоретичним аспектам кібервійни в інформаційному суспільстві. Розглянуто термінологічні питання та характеристики кібервійни, особливу увагу приділено російсько-українському протистоянню. Визначено та проаналізовано проблеми правового регулювання кібервійни на національному та міжнародному рівнях, застосування міжнародного права, права прав людини, транснаціональні тенденції кіберконфліктів.

Ключові слова: *кібервійна; кіберпростір; кіберзагроза; кібератака; правове регулювання; інформаційне суспільство*.

The article is devoted to cyberwar general theoretical aspects in the information society. The terminological issues and characteristics of cyberwar are considered, special attention is paid to the Russian-Ukrainian confrontation. Problems of legal regulation of cyberwar at national and international levels, the application of international law and human rights law, transnational cyber conflict trends are determined and analyzed.

Key words: *cyberwar; cyberspace; cyber threat; cyber attack; legal regulation; information society.*

Постановка проблеми. Суттєва особливість соціального розвитку на початку XXI ст. – підсилення впливу інформаційного середовища на особу, суспільство та державу. Наслідками науково-технічного прогресу, особливо у сфері інформаційних і комунікаційних технологій, стали зсуви у правовому полі, зокрема в питаннях правового регулювання,

прав людини, національних і міжнародних правовідносин, свободи та безпеки. Розв'язання проблеми інформаційних загроз, кіберзагроз і браку правових інструментів для запобігання їм ускладнюється непередбаченістю наслідків діяльності у кіберпросторі.

Аналіз останніх досліджень і публікацій. Труднощі починаються від самого визначення змісту термінів "кіберзагроза", "протистояння у кіберпросторі", "кібервійна". Як стверджують Дж. Андрес і С. Вінтерфілд, "визначити, що таке кібервійна, досить важко. Фактично, обидві дефініції – "кібер" і "війна" – є предметом дискусій"[*1,* 2]. Дійсно, ми бачимо приклади ураження систем національної та міжнародної безпеки, не пов'язані з військовими діями, такі як вірусні атаки чи доведення секретної інформації до широкого загалу. Це приклад гібридного конфлікту в Україні, коли одночасно ведуться і військові дії, і протистояння в інформаційній сфері та кіберпросторі.

Оскільки "кібербезпека охоплює апаратну й програмну інфраструктуру, що підтримується за допомогою національних і міжнародних стратегій та регулювання" [*2,* 23], для досягнення певного якісного рівня кібербезпеки слід мати національну та міжнародну стратегії кіберзахисту, а також ефективні механізми їх реалізації. Добре, якщо ці механізми працюють на відвернення кіберзагроз, однак іноді в їх розробці доводиться спиратися на події, які вже сталися чи відбуваються прямо зараз.

Так, 21 лютого 2014 р. в Україні перемогла "революція гідності", яка почалася 21 листопада 2013 р. з нечисленного громадського протесту, який поступово, у відповідь на жорстокі й непропорційні дії публічної влади, перетворився на народний спротив режиму. Отже, 21 лютого багато українців сподівалися на швидкі та ефективні реформи, які відбувалися б за активної участі представників громадянського суспільства та підтримкі міжнародного співтовариства. Однак анексія Криму, діяльність незаконних збройних формувань, терористичні акти в Донецькій та Луганській областях, а також багато інших дій, що відбулися завдяки Російській Федерації або за її активної підтримки, майже поховали ці надії. І перед тим, як Російська Федерація дозволила собі прямі агресивні дії, була розв'язана інформаційна війна, частиною якої стали дії у кіберпросторі.

Хоча багато хто погодився би з думками про те, що "кібервійна поки не мала драматичних гуманітарних наслідків, і можна сподіватися, що такий стан справ не зміниться у майбутньому, потенціал для людських трагедій, проте, вже величезний та, ймовірно, збільшиться разом зі зростаючою залежністю від комп'ютерно-контрольованої системи підтримки повсякденного життя" [3], і про те, що загроза кібервійни перебільшена [*4,* 41–42], – все це не виглядає так оптимістично, коли ви перебуваєте у центрі подій. З іншого боку, звідси можна споглядати, як працюють чи не працюють правові доктрини та механізми у світлі інформаційної небезпеки й кіберзагроз, і порівняти теоретичні моделі з дійсністю.

Мета статті – загальнотеоретичне визначення сутності й особливостей кібервійни, зважаючи на українсько-російське протистояння та його наслідки для системи національної та міжнародної безпеки. Слід також розглянути деякі вразливі місця доктрини кібербезпеки і перспективи її розвитку.

Виклад основного матеріалу. Насамперед необхідно приділити увагу неоднозначній термінології, яка використовується у правовому регулюванні в умовах інформацйного суспільства. Оскільки налаштування глобальних мереж, комп'ютерна техніка, комунікаційні досягнення та інформатизація соціуму стали закономірними, нам потрібно визначитися з деякими універсальними характеристиками сучасного світу.

Зазначається, що "в різноманітті теорій і трактувань ймовірних шляхів розвитку людства в найближчому і подальшому майбутньому окрему групу становлять погляди на соціальний устрій як форму мережної або електронної спільноти з домінантою засобів масової інформації, інформаційних і мобільних технологій, Інтернету" [*5,* 55]. Таке суспільство, в якому більшість збирає, обробляє та використовує інформацію, що має ключовий характер, вважається інформаційним. Останнім часом поширюється також концепція суспіль-

ства мережного. Цей тип суспільства передбачає "популяризацію можливостей і переваг інформаційного суспільства, соціалізацію на основі спілкування, нові форми солідарності, поширення регіональних ініціатив, формування відкритого творчого співтовариства, що сприяє створенню інновацій" [*6,* 101].

На жаль, окрім переваг та можливостей, інформаційний і мережний типи суспільства містять нові складнопрогнозовані виклики та загрози. Приміром, під час президентських виборів в Україні відбулася атака російських спецслужб (хакерів) на сервер Центральної виборчої комісії. Як повідомив Голова Державної служби спеціального зв'язку та захисту інформації України В. Звєрєв, там мала з'явитися неправдива інформація про те, який кандидат набрав більшість голосів [7]. І хоча успішні дії з кібероборони запобігли цифровому втручанню, в російських ЗМІ не встигли поміняти заготовлену картинку та показали неправдиві результати, згідно з якими на виборах нібито переміг інший кандидат (Дмитро Ярош) [8]. Будь-хто міг перевірити таку інформацію хоча б за допомогою офіційного сайту Центральної виборчої комісії України, але багато людей зволіли повірити російській пропаганді, бо насіння впали у підготовлений грунт. Цей приклад, між іншим, показує, що поєднання методів інформаційної війни та кібервійни дає ефективніші результати, ніж окремі дії.

Взаємовплив і протистояння на міждержавному рівні в счасному світі дедалі більше занурюються в кіберпростір. Так, порівняно недавно з'явився новий термін – "*cyber power*" (кібервлада, кіберміць). Він усебічно описує можливості держави у двох сферах – вчиняти дії та здійснювати вплив у кіберпросторі. Він складається з низки суттєвих чинників, що включають: можливості Інтернету та інформаційних технологій; можливості ІТ-індустрії; можливості Інтернет-ринку; вплив Інтернет-культури; можливості Інтернет-дипломатії/міжнародної політики; військову міць у кіберсфері; національні інтереси щодо участі у стратегії кіберпростору [*9,* 802–803]. Так само, як держава чи група союзних держав можуть нарощувати міць у сфері озброєння, вони заводять кіберзброю і кібервійська. Комп'ютерні віруси, приховані деталі обладнання, пристрої для стеження та запису – все це стає досить ефективною зброєю і має тяжкі наслідки застосування. Потенційно це призведе до нової "холодної війни", що потребуватиме механізмів взаємного стримування.

У XXI ст. приватні, публічні особи та держава все більше залежать від інформації й інформаційних технологій. Приватні особи покладаються на інформаційні технології у повсякденному житті (від читання стрічок новин до платіжних операцій). Функціонування громадянського суспільства також багато в чому залежить від технологій, особливо в частині контролю за публічною владою, прозорості та відкритості, ефективності спільних дій. Комп'ютерні мережі та системи широко використовуються державою в цивільних і військових цілях. Тому вразливість усіх елементів суспільства у світлі можливих кіберзагроз досить висока.

Класичні приклади можливих наслідків кібератак у сучасності – втручання до інфраструктури військових і цивільних об'єктів. І тут можливі різні варіанти розвитку подій, аж до руйнівних наслідків. Так, зазначається, що типовим прикладом можливої кібератаки, яка безпосередньо впливає на цивільних осіб, є вимикання електростанції шляхом повного вимикання, перевантаження або вимикання систем відмовостійкості, завдаючи шкоди обладнанню. Це потенційно може трапитися з будь-якою інфраструктурою, що підтримується за допомогою програмного забезпечення [*10,* 504]. Проте є і складніші випадки, коли ми не можемо точно сказати, наскільки серйозні руйнування відбулися. Це звучить трохи фантастично, але втручання у кіберпростір у майбутньому здатне вразити самі основи суспільства. Тим більше, що інформаційне й особливо мережне суспільство передбачає, що люди проводять багато часу в кіберпросторі. Важливий момент: межі цього кіберпростору не збігаються з кордонами, встановленими міжнародним правом.

Іншими досить розпливчатими термінами є кіберзагрози та кіберконфлікти. Конфлікт означає протистояння між сторонами, причому ними можуть бути і державні, і приват-

ні суб'єкти. "Конфлікт у кіберпросторі належить до дій, які вживають сторони для отримання переваги над супротивником у кіберпросторі за допомогою різноманітних технологічних інструментів і засобів, орієнтованих на людський чинник" [*11,* 515]. З цього погляду атака групи хакерів, що підтримують опозиційну політичну силу, на урядові сервери також може бути класифікована як кіберконфлікт.

Існує щонайменше три терміни, які найчастіше використовуються, коли йдеться про кіберзагрози, протистояння і конфлікти. Всі вони можуть позначати нові або змішані типи військового протистояння. Це інформаційна війна, мережна війна і кібервійна. Названі три терміни іноді вибудовують у логічний ряд у міру звуження змісту. Візуально їх можна подати як три сфери: найбільша – інформаційна війна, всередині неї – мережна, а всередині останньої – кібервійна. Однак фактично вони існують як три сфери, що перетинаються. Тому дії, скоєні, приміром, у ході кібервійни, тягнуть за собою або передбачають дії з арсеналу війни інформаційної.

Так, деякі автори пишуть, що "мережна війна належить до типів конфліктів (і злочинів), що розвиваються на рівні всього суспільства, включає заходи короткої традиційної війни". Вони стверджують, що кібервійна містить конфлікти між організованими збройними формуваннями, військовими, водночас мережна війна складається з Інтернет-конфлікту, який включає недержавних акторів [*12,* 194]. Думка з приводу несамостійного характеру кібервійни дуже поширена. Наприклад, Е. Гартцке вважає, що "найчастіше вона буде зустрічатися як додаток до звичайної війні або як своєрідні тимчасові заходи і значною мірою символічні зусилля з вираження невдоволення діями іноземного супротивника. Кібервійну найкраще обговорювати в цих контекстах не як самостійну або навіть альтернативну форму конфлікту, а як логічне продовження вже наявного в поєднанні з військовим протистоянням" [*4,* 73]. Однак таку думку з приводу кібервійни досить важко підтримати. Адже кібервійна може включати не тільки військових учасників і не завжди супроводжується відкритим збройним конфліктом. Насправді, її небезпека – в гнучкому і мінливому характері протистояння. Дійсно, держави більш успішно можуть здійснювати серйозні руйнування в кіберпросторі, і вони виявляються основними гравцями в полі міжнародної безпеки. Однак значення приватних суб'єктів зростає з кожним днем, і вони можуть негативно впливати не тільки на кіберпростір, але й на відносини між державами у сфері кібербезпеки.

Наприклад, в українсько-російському протистоянні наочно видно брак використання інформаційно-комунікаційних технологій з боку держави України. Приватні особи, що об'єдналися в громадські ініціативи за допомогою Інтернету і через мережі особистих комунікацій, найуспішніше борються проти інформаційних атак. Вони також здійснюють кібератаки, виводять з ладу кібертехнології супротивника, знищують або підміняють інформацію, розміщену на російських офіційних сайтах або ресурсах проросійських терористів, а також зламують особисті блоги і пошту публічних діячів.

Як видно, багато з цих дій виходять за межі закону. Виникає питання, чи може кібервійна вписуватися у правове поле? У сучасному світі, в якому значну роль у житті держави та її безпеці відіграють кіберпростір та інформація, не можна оминути увагою ті загрози, які пов'язані із застосуванням відповідних технологій. О. Мережко пропонує у зв'язку з цим проект Конвенції про заборону використання кібервійни в глобальній інформаційній мережі інформаційних та обчислювальних ресурсів (Інтернеті). Він визначає кібервійну як "використання Інтернету і пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній та інформаційній безпеці та суверенітету іншої держави" [13].

На наш погляд, кібервійна може бути визначена як протистояння у кіберпросторі, яке ведеться за допомогою комп'ютерних технологій з метою завдати шкоди супротивнику. Кібервійна ведеться переважно державними суб'єктами за участю приватних і може супроводжувати збройний чи інший конфлікт між ними.

Інформаційні технології, особливо кібертехнології, розширюють спектр можливого і виводять уявлення про наслідки і, зокрема, спричинену шкоду за межі традиційних уявлень про війну. Поширена думка, що кібероперації проводяться онлайн, але ефект мають офлайн. І хоча точний ефект визначити важко, зауважимо, що саме комп'ютерні технології дають можливість досягати результату на величезній відстані за малий проміжок часу.

Н. Мельцер дає коротке визначення терміна кібервійна як такого, що "належить до війни, що проводиться в кіберпросторі за допомогою кіберзасобів і методів" [3]. Але що таке кіберзасоби і методи? Фактично, єдиний метод, наявність якого не викликає сумнівів, – кібератака. "Кібератака являє собою навмисну діяльність зі зміни, пошкодження, руйнування і знищення комп'ютерних систем або мереж, що використовуються супротивником, або інформації та/або резидентних програм у них, або таких, що транслюються через ці системи або мережі. Така діяльність може також впливати на об'єкти, підключені до цих систем або мереж" [*11,* 518–519]. "Вузька дефініція кібератаки, призначена для привертання уваги до унікальності загрози, яка походить від кібертехнологій, визначає її як будь-які дії, вжиті для підриву функціонування комп'ютерної мережі в політичних цілях або для впливу на національну безпеку" [*14,* 826].

Кібератака – це пряме втручання до комп'ютерних мереж супротивника. Воно може бути досить "брутальним", спрямованим на знищення або блокування частини інфраструктури або інформації. Втручання може бути більш "ніжним" і витонченим, коли інформація повністю або частково змінюється.

Іноді втручання до комп'ютерних мереж супротивника називають також кібероперацією. "Кібероперації – це операції, спрямовані проти або вчинені за допомогою комп'ютера або комп'ютерних систем через потік даних […] різноманітні "цілі" в реальному світі можуть бути знищені, змінені (уражені) або зруйновані, такі як індустрія, інфраструктура, телекомунікації чи фінансова система. Кібероперації проводяться за допомогою програмного забезпечення, обладнання або за допомогою комбінації програмного забезпечення та персоналу" [*10,* 503]. В. Бут стверджує, що "кібероперації мають розглядатись як кібератаки. Важливе питання, однак, те, що операція може бути розпочата на значній відстані як у просторі, так і в часі від того місця і часу, де і коли відбудуться руйнівні наслідки" [*15,* 587].

Проте, на нашу думку, кібероперації належать до методів, що можуть передбачати кібератаки, кіберстеження, кіберпроникнення або кібервтручання. "Кібервтручання є навмисною діяльністю, спрямованою на проникнення до комп'ютерних систем чи мереж, використовуваних супротивником, з метою отримання інформації, що міститься там або передається через ці системи та мережі. Кіберпроникнення не прагнуть порушити нормальне функціонування комп'ютерної системи або мережі з погляду користувача" [*11,* 518–519]. Кіберпроникнення, таким чином, виглядає як збереження комп'ютерних систем супротивника та інформації у незайманому стані. Якщо атакуючі дії до якоїсь міри видимі, то дії зі стеження спрямовані на те, щоб якомога довше залишатися непомітними. Слід звернути увагу й на те, що склад учасників для кібератак і кіберпроникнень може бути різним. Якщо перші можуть досить успішно провести приватні суб'єкти, то другі частіше спираються на можливості держави.

Г. Лін пропонує два варіанти класифікації засобів кібервійни: "Інструменти і методи конфлікту в кіберпросторі доцільно розділити на інструменти, що базуються на технологіях, і методи, які зосереджуються на людині. Наступальні інструменти та методики дозволяють стороні супротивника зробити щось небажане. Захисні засоби і методи спрямовані на запобігання цьому" [*11,* 517].

На наш погляд, можна запропонувати таку класифікацію, яка ґрунтується на характері діяльності, здійснюваної в ході кібервійни. Методи кібервійни можна умовно розділити на відкриті (кібератаки і кібероборона) і приховані (кіберспостереження, кіберпастки і засідки).

У дійсності, ніхто не уявляє собі потенційних форм і небезпеки методів та засобів кібервійни повністю. Однак у них є й позитивний бік, що наочно продемонструвало українсько-російське протистояння. Насамперед це демонстраційна, доказова сторона (приміром, супутникові знімки, інші зображення або відео з геолокацією), що ефективно підкріплює традиційні засоби доказування. Важливо, що спеціальні знання не завжди потрібні для того, щоб користуватися інформаційними технологіями. Багато людей не мають уявлення про те, як інформаційні технології працюють, але можуть зробити красномовну фотографію.

Проблема в тому, що перевагами, які дають кіберзасоби, потрібно навчитися правильно користуватися. У випадку України ми зіткнулися з тим, що стратегія національної безпеки, і особливо кібербезпеки, не спрацювала в момент різкого збільшення загрози. Крім того, суттєві деталі російсько-українського протистояння – "психологічна" складова конфлікту і взаємопроникнення кіберпростору, в тому числі за рахунок мовного середовища.

Зараз Україна стоїть перед вибором у сфері національної безпеки. Одна із серйозних стратегічних проблем полягає у балансі між свободою та безпекою. Як справедливо зауважив А. Томкінс, у розробці антитерористичного законодавства, яке б відповідало вимогам прав людини, інтереси "безпеки" та "свободи" перебувають у напруженні один з одним [*16,* 215]. На одній шальці терезів для України перебуває прагнення до відкритості суспільства, демократії, презумпція відкритості інформації, ефективний контроль уряду з боку громадянського суспільства, питання участі, доступу та прозорості у діяльності публічної влади. На іншій – прагнення посилити національну безпеку, запобігти внутрішнім та зовнішнім загрозам і радикалізація суспільства, що потребує адекватної відповіді на агресію та саботаж.

Питання правового регулювання кібервійни досить дискусійні не тільки для національного, але й для міжнародного права. Найбільш прийнятні варіанти пов'язані з можливістю застосування Статуту ООН, міжнародного гуманітарного права та права прав людини.

Опора на згаданий Статут базується на тому, що ООН зосереджена на підтримці міжнародного миру і безпеки. Вона може вживати ефективні колективні заходи для запобігання та усунення загрози миру і придушення актів агресії або інших порушень миру та проводити мирними засобами відповідно до принципів справедливості й міжнародного права залагодження або розв'язання міжнародних суперечок чи ситуацій, які можуть призвести до порушення миру (Стаття 1). Рада Безпеки ООН визначає існування будь-якої загрози миру, будь-якого порушення миру або акту агресії та здійснює рекомендації або вирішує те, яких заходів слід ужити для підтримки або відновлення міжнародного миру і безпеки (Стаття 39) [17]. Можна було б припустити, що до кібервійни застосовуються правила використання збройної сили, які містять два дозволених варіанти – санкціонування цього Радою Безпеки ООН відповідно до Статті 42 або реалізація невід'ємного права на індивідуальну або колективну самооборону, якщо відбудеться збройний напад згідно зі Статтею 51 [17]. Однак тут виникає низка проблем, пов'язаних з тим, що Статут ООН не описує кіберзагрози або кібероборону як неприпустимі дії або допустимі заходи безпеки, що не дивно, адже він був створений до появи подібних речей. Крім того, є проблеми з визначенням збройної сили і агресії як таких, тому що сам Статут містить надто загальні й дещо суперечливі формулювання.

Документи Генеральної Асамблеї ООН щодо кібербезпеки не додають ясності, навіть такі спеціальні резолюції, як "Створення глобальної культури кібербезпеки і захист найважливіших інформаційних інфраструктур" чи "Створення глобальної культури кібербезпеки й оцінка національних зусиль із захисту найважливіших інформаційних інфраструктур" [18; 19]. До того ж, як іноді зазначається, "ці резолюції є розпливчатими і не потребують будь-яких конкретних дій з боку держав – членів ООН" [*14,* 860].

Застосування міжнародного гуманітарного права у справі кібервійни також пов'язане із серйозними труднощами. По-перше, це кваліфікація кібервійни як такої, що досягає рівня воєних дій. По-друге, поява гібридних форм воєнних дій. По-третє, стирання граней між цивільними та військовими особами у кіберконфлікті. По-четверте, труднощі з визначен-

ням шкоди для цивільного населення. Можливо, рішення лежить у сфері інтерпретації положень Женевських конвенцій і протоколів до них, особливо в частині невибіркової зброї, заподіяння надмірного збитку і страждань. Але, як і у випадку зі Статутом ООН, міжнародне гуманітарне право не встигає змінюватися так швидко, як інформаційно-комунікаційні технології та кіберпростір. Крім того, як пише К. Дроге, "невизначеність і плутанина у застосовності міжнародного гуманітарного права до кібервійни може бути наслідком різних розумінь самого поняття кібервійни, які варіюються від кібероперацій, здійснюваних у контексті збройних конфліктів, до кримінальної кібердіяльності всіх видів" [*20,* 536]. Тобто самі інтерпретації терміна "кібервійна" можуть ускладнити застосування міжнародного гуманітарного права.

У застосуванні до кібервійни права прав людини можна окреслити три варіанти. Перший ґрунтується на такому фундаментальному праві, як свобода вираження думки (*right to freedom of opinion and expression*). Другий випливає з комплексу прав, які тісно пов'язані з інформацією та успішна реалізація котрих залежить від неї (наприклад, право на приватність, право брати участь в управлінні державою). Третій показує непряме обмеження прав людини в разі прямих важких наслідків кібератак (наприклад, право на життя і здоров'я). Але в усіх цих випадках важливо встановити причинно-наслідкові зв'язки між діями у рамках кібервійни й обмеженням прав людини.

Загальна декларація прав людини вказує на особливий характер права на свободу вираження думки. Крім безпосереднього закріплення в ст. 19, воно згадується у преамбулі у формулюванні "свобода слова і переконань" [21]. Фундаментальний характер цього права виражається також у тому, що воно охоплює широкий спектр можливостей: право мати думку і дотримуватися її, право висловлювати і поширювати думку або утримуватись від цього (наприклад, не ділитися відомою людині інформацією та її оцінкою). Інформаційно-комунікаційні технології багато значать для можливості виражати різноманітні думки, проте під час кібервійни вони можуть легко вразити головні опори реалізації цього права – свободу слова і преси. Методи кібервійни впливають на думки окремих людей і груп, що також може бути визнано втручанням у здійснення названого права.

Ключова проблема для права на свободу вираження поглядів в умовах кібервійни та інформаційної війни полягає у межах допустимого втручання держави до сфери його реалізації. Приміром, в Україні є групи проросійських хакерів, які зламують урядові сайти, та ЗМІ, що ведуть пропаганду і розпалюють міжнаціональну ворожнечу. Чи має держава використовувати для них особливі процедури притягнення до відповідальності? Ще одна проблема – конфлікт з правами інших людей. Наприклад, деякі українці висловлюють свою думку в Інтернеті про військових, які дислокуються поруч з їх місцями проживання, розкриваючи таким чином таємницю місцезнаходження цих підрозділів.

Важливим правом для кіберпростору є право на приватність, прайвесі або (у формулюванні ст. 17 Міжнародного пакту про громадянські та політичні права) захист приватного життя і репутації [22]. Це право може використовуватися у справі регулювання кібервійни, якщо кібероперації призвели до розкриття особистих даних або їх фальсифікації.

Перспективи регулювання кібервійни за допомогою права прав людини пов'язані також з виділенням нової когорти прав, які можуть поступово набувати статусу фундаментальних, наприклад, право на Інтернет і право на анонімність у комунікаційних мережах. Останніми роками право на Інтернет набуває серйозного значення, в деяких державах воно визнано одним з основних. На думку П. Сухорольского, "хоча найближчим часом малоймовірно широке міжнародне закріплення загального права на анонімність, слід ураховувати її значення у створенні правових норм. Основою такого регулювання має бути визнання принципів пріоритету прав і свобод людини, адекватного і виправданого державного контролю, забезпечення вибору опцій, що дозволяють анонімність, мінімізації збирання та об-

робки персональних даних" [*23,* 47]. Обидва ці права потенційно застосовні в питаннях кібервійни через тісний зв'язок проблем анонімності, Інтернету і доступу до інформації.

Розширення змісту традиційних прав також може вплинути на правове регулювання кібервійни і кіберпростору. Насамперед це стосується результатів розвитку нових технологій для людини. Такі приклади, як іплантанти, штучні органи і багато інших досягнень, у тому числі комп'ютерно-технологічні, змінюють уявлення про особисту недоторканність або точку початку життя, чи поняття фундаментального права на фізичну недоторканність. Як зазначається, "не має бути ніякого відображення "один до одного" між фізичними межами органічного, цілісного людського тіла та юридичними межами прав, що з цього випливають" [*24,* 2]. Тим більше ці межі не збігаються у випадках поєднання органічного тіла з продуктами нових технологій.

Отже, при спробах правового регулювання кібервійни, застосування правових інструментів ми стикаємося з низкою проблем.

По-перше, є питання з визначенням війни, агресії та застосування сили. Специфіка методів і засобів кібервійни не сприяє проясненню цих термінів, навпаки, спроби класифікувати кіберзагрози лише породжують нові правові виклики.

По-друге, виникають труднощі з визначенням учасників кібервійни як щодо розподілу приватних і державних акторів, так і щодо дистанційної участі. Невирішені питання участі приватного сектора суспільства, кібератак та інших дій приватних осіб, які призводять до міждержавних конфліктів, участі на боці якоїсь держави без офіційного дозволу, відповідальності держави за дії своїх громадян у кіберпросторі тощо. Наприклад, є багато ресурсів та об'єднань, створених приватними суб'єктами для протидії російській кіберагресії в Україні: Український щитоносець або Інфосотня України. Крім того, конкретні особи, які йдуть у кібератаку, можуть бути досить слабко пов'язані з державами-супротивниками, адже не потрібно укладати контракт або отримувати громадянство для того, щоб вступити до віртуальних військ. Приміром, на захист інтересів України стали проукраїнські хакери, які живуть в інших країнах. Як пише В. Бут, "поняття віддаленості оператора від наслідків його або її діяльності посилюється труднощами, що, швидше за все, виникнуть у визначенні, а потім у демонстрації того, по-перше, хто здійснив дану кібероперацію, по-друге, від імені якої держави або організації, якщо такі є, операція була проведена, і, по-третє, яка її мета" [*15,* 587].

По-третє, ускладнена ідентифікація самих дій у рамках кібервійни. Наявність певних кіберзагроз важко довести. Крім того, існують неявні дії, а також закладені міни в мережах противника, які можуть роками чекати свого часу. Хто гарантує, що в технологічних досягненнях, якими обмінюються держави, немає прихованих функцій і можливостей?

По-четверте, дуже складно розрахувати наслідки дій, вчинених у рамках кібервійни. Шкода від кіберзагроз може бути пряма і непряма, моментальна і відкладена. Виникають проблеми навіть з визначенням впливу на цивільне населення, якщо супротивник використовував, наприклад, дистанційне вимкнення систем постачання. Також слід пам'ятати про можливість настання наслідків через великий проміжок часу і враховувати моральну шкоду та вплив на психіку людей.

Необхідно зупинитися на деяких особливостях кібервійни Російської Федерації проти України, які ускладнюють можливе правове регулювання проблеми на національному рівні.

Передусім, це тривалий характер кіберконфлікту. Якщо у випадках кібератак стосовно Естонії у 2007 р. чи Грузії у 2008 р. ми маємо більш-менш чітку періодизацію, то у випадку України часові рамки протистояння охоплюють роки, якщо не десятиріччя (можливо, 2004–2015 рр.). Ворожі дії проти України в кіберпросторі тривають з різним ступенем інтенсивності, переходячи в гострі фази, коли остання намагається вийти з-під орбіти російського впливу.

Другою особливістю російсько-української кібервійни є тісний зв'язок з війною інформаційною. Інформаційна складова – одна з головних у тиску Російської Федерації на Україну, так само, як і економічна (торгові конфлікти, ембарго, газові контракти). Як зазначає В. Гусаров, "на передній план у цій війні вийшли російські інформаційні операції для завоювання інформаційної переваги в Україні" [25]. Основні опори інформаційної війни такі: географічна, історична, економічна, мовна близькість; невизначена національна ідентифікація частини населення; взаємопроникнення культур; орієнтація багатьох політичних сил на тісну співпрацю з російською стороною і пряма підтримка з Російської Федерації (фінансова та ідеологічна). Основні напрями цієї інформаційної війни задають проросійські ЗМІ та громадські діячі, спираючись на міфологію радянської епохи й ототожнення образу Росії з усіма реальними і вигаданими перевагами минулого. Також популярними інструментами є негативні маркери свідомості (фашизм, нацизм, бандерівці). Патерналістська свідомість значної частини населення також зміцнює позиції російської сторони, а додаткові бали набираються нею за рахунок гри на страхах перед нестабільністю і потрясіннями, пережитими українцями за останні два десятиріччя. На жаль, Російська Федерація використала свій неабиякий вплив на Україну для її знищення як незалежної держави. І цим тільки посилила розбіжність у наших політичних режимах, менталітеті та ціннісному виборі.

Третя особливість пов'язана з приватними учасниками кібервійни. Популярна в Україні фраза описує те, що відбувається, як війну українського народу (при паралізованій українській державі) з російською державою (при паралізованому російському народові). Це, звичайно, перебільшене уявлення про події, але воно має певні підстави для існування. Зокрема, це твердження правдиве стосовно участі проукраїнськи налаштованих осіб, що об'єдналися у приватні ініціативи, а також щодо випадків злиття зусиль громадянського суспільства і держави в кіберпротистоянні. Прикладами можуть бути робота Інформаційно-аналітичного центру Ради національної безпеки і оборони України, призначення кандидатів від громадськості на державні посади, передавання волонтерам деяких питань забезпечення армії, в тому числі спецзв'язку та кіберзахисту.

Четверту особливість протистояння втілює "внутрішній чинник" кібервійни. Як не шкода визнавати, але й реальний військовий конфлікт, і його віртуальна частина має прихильників агресії Російської Федерації всередині України. Якоюсь мірою війна проти України має змішаний характер, ускладнюється громадянським конфліктом на сході країни. А у випадку з кіберзагрозами визначити, де внутрішній конфлікт, а де ні, стає ще складніше.

П'ята особливість характеризується незвичайністю політико-правової ситуації в Україні. Серйозне протистояння, в тому числі у кіберпросторі, почалося в умовах постреволюційного, постмайданного суспільства, певного розколу в соціумі й дискусій з приводу легальності та легітимності тих чи інших дій.

Насамкінець, шоста особливість – відсутність адекватної та актуальної державної інформаційної стратегії та стратегії кіберзахисту в Україні. Крім того, що Російська Федерація ніколи не розглядалась як імовірний супротивник, фактично немає заздалегідь підготовлених планів, але є необхідність учитися відповідати на кіберзагрози в процесі конфлікту.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Таким чином, перед Україною стоїть питання національної стратегії у кіберпросторі. Це має бути гнучка стратегія, що передбачає як порівняно мирні, усталені варіанти інформаційного та віртуального стримування (*deterrence*), так і надзвичайні ситуації. Вона має враховувати ефективність і мобілізаційні можливості приватних осіб та одночасно напівпаралізованність і небажання реформ з боку значної частини публічної влади, а також спиратися на міжнародне право та найкращі доробки національного права інших держав.

Важливий чинник – специфіка "поля бою", тобто кіберпростору. За словами Н. Мельцер, "кіберпростір – єдиний повністю рукотворний домен. Він створюється, під-

тримується, належить і управляється разом зацікавленими сторонами, державними і приватними, всім світом і постійно змінюється у відповідь на технологічні інновації" [3]. Через специфіку кіберпростору й швидку змінюваність інформаційних технологій кіберзагрози можуть впливати на національну і міжнародну безпеку досить непередбачувано. Серед нових викликів, які готують кібертехнології, можна виділити такі, як використання технологій для здійснення ворожих дій та актів агресії; втручання до цивільної інфраструктури; дестабілізація суспільно-політичної ситуації; поширення неправдивої інформації та маніпулювання свідомістю; знищення або блокування комп'ютерних систем і мереж тощо.

Перспективи зміни системи міжнародної безпеки досить туманні, проте вже зрозуміло, що багато інститутів і механізмив неефективні або недостатньо ефективні, що демонструє українсько-російський конфлікт. Проблема ще й у тому, що окрема держава практично не зможе протистояти можливим кіберзагрозам сучасності, якщо покладатиметься тільки на свої розробки і виключить інформаційний обмін з іншими.

Слід також звернути увагу на те, що правові доктрини національної кібербезпеки не завжди встигають змінитися так швидко, як технології. Не потрібно забувати, що навіть у технологічно розвинених, демократичних державах суттєвим законодавчим і правозастосовним змінам щодо відповідних питань передує серйозне громадське обговорення, що збільшує час реакції на просування кібертехнологій. У державах, що прагнуть до демократичного режиму, до цього можуть додаватися інші перешкоди, такі як корупція або конфлікт інтересів представників публічної влади.

У відкритому, глобальному інформаційному суспільстві та кіберпросторі можливе спільне підтримання балансу у сфері міжнародної безпеки, а також міждержавні союзи. Поєднання національної та міжнародної стратегій кіберзахисту, опора на приватних і державних акторів, динамізм – ось приблизний рецепт для безпеки кіберпростору.

Насамкінець, слід визначити тенденцію, яка справедлива для будь-яких загроз безпеки, в тому числі кіберзагроз – підвищення транснаціональної взаємозалежності. Отже, навіть якщо в Україні був би виключно цивільний конфлікт, його вплив вийшов би за межі національної правової системи.

Список використаних джерел:

1. Andress J. Cyber warfare: Techniques, tactics and tools for security practitioners / Andress J., Winterfeld S., Rogers R. – Amsterdam : Syngress/Elsevier, 2011. – 289 p.

2. Maskun S. H. Cyber Security: Rule of Use Internet Safely / S. H. Maskun // Journal of Law, Policy and Globalization. – 2013. – Vol. 15. – P. 20–24.

3. Melzer N. Cyberwarfare and International Law [Електронний ресурс] / N. Melzer // UNIDIR. – 2011. – Режим доступу : http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

4. Gartzke E. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth / E. Gartzke // International Security. – Fall 2013. – Vol. 38. – No. 2. – P. 41–73.

5. Городенко Л. Мережеве суспільство та мережеві комунікації / Л. Городенко // Інформаційне суспільство: науковий журнал, Інститут журналістики КНУ імені Тараса Шевченка. – 2011. – № 14. – С. 55–58.

6. Сас В. В. "Электронное правосудие" как элемент "сетевого общества": теоретические проблемы / В. В. Сас // Юридическая наука. – 2012. – № 2. – С. 101–104.

7. Специалисты Государственной службы специальной связи и защиты информации Украины отбили все атаки на сервера Центральной избирательной комиссии // 28 мая 2014 [Електронний ресурс]. – Режим доступу : http://www.dstszi.gov.ua/dstszi/control/ru/publish/article?art_id=114141&cat_id=112494&mustWords=%D0%A6%D0%98%D0%9A&searchPublishing=1

8. Назарук Т. “Картинку Яроша” розмістили під унікальною адресою. На ОРТ її знали / Т. Назарук // 28 липня 2014 [Електронний ресурс]. – Режим доступу : http://www.osvita.mediasapiens.ua/material/31222

9. Zhang L. A Chinese perspective on cyber war / L. Zhang // International Review of the Red Cross. Humanitarian debate: Law, policy, action. – 2012. – № 94 (886). – P. 801–807.

10. Backstrom A. New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews / A. Backstrom, I. Henderson // International Review of the Red Cross. Humanitarian debate: Law, policy, action. – 2012. – № 94 (886). – P. 483–514.

11. Lin H. Cyber conflict and international humanitarian law / H. Lin // International Review of the Red Cross. Humanitarian debate: Law, policy, action. – 2012. – № 94 (886). – P. 515–531.

12. Arquilla J. The Advent of Netwar: Analytic Background / J. Arquilla, D. Ronfeldt // Studies in Conflict and Terrorism. – 1999. – Vol. 22. – No. 3. – P. 193–206.

13. Мережко А. А. Конвенция о запрещении использования кибервойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете). Проект [Електронний ресурс] / Мережко А. А. // Український центр політичного менеджменту. – Режим доступу : http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57

14. Hathaway Oona A. The Law Of Cyber-Attack / Oona A. Hathaway // California Law Review. – 2012. – Vol. 100. – No. 4. – P. 817–885.

15. Booth W. Some legal challenges posed by remote attack / W. Booth // International Review of the Red Cross. Humanitarian debate: Law, policy, action. – 2012. – № 94 (886). – P. 579–595.

16. Tomkins A. National Security and the Due Process of Law / A. Tomkins // Current Legal Problems. – 2011. – Vol. 64. – P. 215–253.

17. Charter of the United Nations, June 26, 1945, 59 Stat. 1031, T.S. 993, 3 Bevans 1153, entered into force Oct. 24, 1945.

18. G.A. Res. 58/199, U.N. Doc. No. A/RES/58/199 (Jan. 30, 2004).

19. G.A. Res. 64/211, U.N. Doc. No. A/RES/64/211 (Mar. 17, 2010).

20. Droege C. Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians / C. Droege // International Review of the Red Cross. Humanitarian debate: Law, policy, action. – 2012. – № 94 (886). – P. 533–578.

21. Universal Declaration of Human Rights, G.A. res. 217A (III), U.N. Doc A/810 at 71 (1948).

22. International Covenant on Civil and Political Rights (of 16 December 1966, entered into force 23 March 1976) G.A. res. 2200A (XXI), U.N. Doc. A/6316 (1966), 999 UNTS. 171.

23. Сухорольский П. М. Право на анонімність як суттєвий елемент прав людини / П. М. Сухорольский // Правова інформатика. – 2013. – № 1 (37). – С. 39–48.

24. Ramachandran G. Against the Right to Bodily Integrity: Of Cyborgs and Human Rights / G. Ramachandran // Denver University Law Rewiew. – 2009. – Vol. 87. – P. 2–57.

25. Гусаров В. Силы информационных операций России: каким должен быть ответ Украины? Эксперт Центра военно-политических исследований по вопросам информационной безопасности для Информационно-аналитического центра Совета национальной безопасности и обороны Украины [Електронний ресурс] / В. Гусаров // 4 октября 2014. – Режим доступу : http://www.sprotyv.info/ru/news/5931-sily-informacionnyh-operaciy-rossii-kakim-dolzhen-byt-otvet-ukrainy