ТЕОРЕТИЧНІ АСПЕКТИ ЗАСТОСУВАННЯ НОРМ І ПРИНЦИПІВ МІЖНАРОДНОГО ПРАВА ДО РЕГУЛЮВАННЯ ВІДНОСИН В КІБЕРПРОСТОРІ

Sea Perl

ЗМІСТ

ВСТУП

Розвиток і вдосконалення міжнародного права з необхідністю вимагають врахування стану розвитку технологій і пристосування міжнародно-правового регулювання до сучасного інформаційного та комунікаційного середовища. Нині життєдіяльність суспільства великою мірою переноситься у віртуальний простір, а кібернетичні загрози стали цілком реальними і дуже небезпечними як для окремих держав, так і для всієї системи функціонування міжнародних відносин. Між тим, юридичні питання в цій сфері все ще залишаються невизначеними. Міжнародне право істотно відстає від потреб практики міжнародних відносин, не містить юридично обов'язкових приписів, які визначали б поведінку держав та інших суб'єктів міжнародного права у кіберпросторі, дієвих стандартів і механізмів захисту прав людини в онлайн-середовищі. Вирішення цих проблем, не в останню чергу, залежить від теоретичного обґрунтування належності певної групи відносин у кіберпросторі до предмета міжнародного права та оцінки можливостей застосування принципів і норм міжнародного права в цій сфері.

В зарубіжній науковій літературі уже понад два десятиліття ведеться активний пошук шляхів застосування міжнародного права до відносин у кіберпросторі (N. Choucri, J. Goldsmith, A. Friedman, M. Hayes, T. Herr, P. Kesan, A. Papanastasiou, Y. Radziwill, M. Roscini, S. Shackelford, M. Shmitt, М. Демина, И. Рассолов, О. Кубышкин). В Україні більшість дослідників зверталися до вивчення окремих аспектів міджнародно-правового регулювання в сфері кібербезпеки, протидії кібертероризму чи протидії інформаційній війні (Ю. Акчурін, І. Забара, Д. Коваль, Т. Короткий Є. Литвинов, М. Малишев, О. Широкова-Мурараш, М. Яцишин та ін.). На теоретичному ж рівні можливості міжнародно-правового регулювання відносин у кіберпросторі вітчизняними вченими досліджувалися недостатньо і наукова спільнота ще досить далека від знаходження концептуального вирішення проблеми.

Наведеними обставинами обумовлюється **актуальність** обраної теми дослідження.

Метою цієї роботи є визначення можливостей застосування норм і принципів міжнародного публічного права до відносин у кіберпросторі між державами та іншими суб'єктами міжнародного права. Для досягнення зазначеної мети передбачається виконання наступних завдань: 1) визначити юридичне поняття кіберпростору; 2) з'ясувати можливість віднесення відносин, що в ньому реалізуються до предмета міжнародно-правового регулювання; 2) охарактеризувати сучасний стан міжнародно-правового регулювання в цій сфері виявити перспективи його вдосконалення; 3) встановити можливість застосування принципів міжнародного права до відносин у кіберпросторі; 4) запропонувати рекомендації щодо створення системи спеціальних міжнародно-правових принципів використання кіберпростору.

Об'єктом дослідження є відносини, що виникають між державами та іншими суб'єктами міжнародного права у зв'язку з використанням кібепростору. **Предметом** дослідження виступають теоретичні аспекти застосування норм і принципів міжнародного права до регулювання відносин в кіберпросторі.

Методологічну основу дослідження становлять сукупність методів, які в комплексі використовувалися для досягнення мети роботи. Аналітичний і логічний методи дозволили здійснити відбір та аналіз інформації за темою дослідження, виявити сутнісні ознаки кіберпростору та сформулювати його визначення. Структурно-функціональний метод дав змогу встановити основні види правовідносин у кіберпросторі. Методи порівняння, аналогії і моделювання застосовувалися в процесі встановлення відмінностей і схожості досліджуваних відносин із відносинами, що вже врегульовані сучасним міжнародним правом. При тлумаченні норм і принципів міжнародного права та встановленні можливостей їх застосування до кіберпростору використовувалися формально-юридичний, системний методи пізнання, дедукція та індукція.

РОЗДІЛ 1. ВІДНОСИНИ У КІБЕРПРОСТОРІ ЯК ПРЕДМЕТ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ

Ведення бізнесу за допомогою мережі Інтернет, існування кіберзлочинності та застосування високотехнологічних методів ведення інформаційних воєн є реаліями сьогодення. Низка регульованих правом відносин нині виникає і реалізується у специфічному середовищі, яке отримало назву «кіберпростір». Єдиного визначення цього поняття досі немає, ні на науково-теоретичному, ні на нормативному рівні. Це зумовлено, в першу чергу. складністю встановлення і врахування всіх його істотних ознак. Кіберпростір є відносно новим, проте, як очевидно вже сьогодні, знаковим у розвитку людської цивілізації явищем. Він не має аналогів і характеризується низкою специфічних ознак.

В науці існує велика кількість думок стосовно цього питання. Так В. Фурашев, аналізуючи лексичне понять «простір» та «кібернетика», «кібернетичний», робить висновок, що кіберпростір – це форма співіснування сукупності матеріальних та нематеріальних об’єктів і процесів, спрямованих на породження, сприйняття, запам’ятовування, переробку та обмін інформацією [1, с. 164]. Однак, спираючись на наведене твердження, дуже складно встановити що є складовими кіберпростору, а що ні. Відповідно, для потреб правового регулювання таке визначення не є придатним, оскільки створює складнощі у кваліфікації відносин у кіберпросторі.

О. Козуб ототожнює поняття «кіберпростір» та «Інтернет». Як заначє автор: «Кіберпростір (а саме так називають світ Інтернету) являє собою сполуку нових форм людської діяльності, нових форм комунікації, нових соціальних груп (різні віртуальні суспільства включно) тощо» [2, с. 178]. Таке визначення теж викликає заперечення, Вважаємо, що поняття кіберпростір є значно ширшим. Відносини у кіберпросторі не завжди реалізуються онлайн. Існує велика кількість локальних мереж, які теж мають бути віднесеними до

кібернетичного середовища. Відтак, Інтернет є лише складовою частиною кіберпростору.

Є. Литвинов намагається визначити поняття кіберпростору через єдність його соціальної та технічної сторін. Відносини у кіберпросторі – це, перш за все, відносини між людьми, але з іншого боку дуже часто вони здійснюються «за посередництвом» інноваційних технологій. Вчений визначає соціальну сторону кіберпростору як сукупність суспільних відносин, що виникають в процесі використання Інтернету та інших мереж, що складаються з приводу інформації, що обробляється за допомогою ЕОМ. Об'єктом даних відносин виступає не всяка інформація, а лише та, яка обертається в Мережі. Технічна сторона полягає в тому, що кіберпростір – це одночасно і складний технічний об'єкт (набір технічних і програмних засобів; сукупність інформаційних ресурсів та інформаційної інфраструктури), що забезпечує рух потоків інформації. Також вчений розмежовує поняття кіберпростір та територія. Відповідно до сучасної правової доктрини територія хоч і не завжди пов'язана з поверхнею землі, але має зв'язок з національними географічними межами, які, в свою чергу, впливають на компетенцію держав і юрисдикцію органів. Тому, на думку автора, помилково вважати, що кіберпростір – це територія, навіть зі змішаним міжнародно-правовим статусом. Це все ж міжнародний планетарний простір. Виходячи з цього, Є. Литвинов визначає кіберпростір як сферу соціальної діяльності, пов'язана з обігом інформації у Всесвітній інформаційної павутині, а також в інших інформаційно-комунікаційних мережах (регіональних, відомчих, корпоративних) [3].

Загалом погоджуючись з підходом дослідника, вважаємо однак, що визначення поняття кіберпростору повинно вказувати також на інші його специфічні ознаки, що дозволить чітко відмежовувати це поняття від інших.

У Концепції військових операцій у кіберпросторі Департаменту сухопутних військ Міністерства оборони США знаходимо твердження, що кіберпростір складається з багатьох різних мереж, які не мають чітких кордонів і часто накладаються одна на одну. При цьому кіберпростір описується за

допомогою трьох складових: 1) фізична мережа; 2) логічна мережа; 3) кібер-персона. Фізичний мережевий шар кіберпростору складається з географічного компонента (наприклад географічне місце розташування серверу) та компонентів фізичної мережі (середовище, де безпосередньо знаходяться дані). Логічний мережний рівень складається з тих елементів мережі, які пов'язані один з одним таким чином, що абстрагуються від фізичної мережі (Форма або відносини не прив'язані до індивідуального, конкретного шляху чи вузла, наприклад, веб-сайт, розміщений на серверах у декількох фізичних місцях. Рівень кібернетичної особи складається з людей, які фактично знаходяться в мережі [4, с. 5-6].

Зазначений опис структури кіберпростору має велику практичну цінність. У той же час, викликає сумніви можливість вважати осіб, які знаходяться в мережі, частиною кіберпростору. По-першу, дана складова не є постійною і точною, по-друге, знову ж таки, орієнтуючись на потреби правового врегулювання, відзначимо необхідність відмежування суб’єктів відносин від середовища, у якому ці відносини здійснюються.

Для формулювання коректної дефініції поняття «кіберпростір», а також для оцінки того, наскільки відносини, що у ньому складаються можуть бути предметом правового регулювання взагалі і предметом міжнародно-правового регулювання, спробуємо визначити специфічні ознаки (властивостей) кіберпростору. Спільно ці властивості створюють контекст, який не відповідає традиційному уявленню про правову та міжнародну реальність, створюючи виклик традиційній будові міжнародних відносин. Кіберпростір «генерує» нові форми суспільних відносин та невідомі раніше способи реалізації усталених, нові види й закономірності конфліктів, воєн, створює нові ризики і загрози міжнародному та національному правопорядку, обумовлює запровадження специфічної термінології (кібератака, кіберзброя, кібертероризм тощо).

Професор Массачусетського технологічного університету Nazli Choucri виділяє наступні відмінності кіберпростору, що вступають в суперечність із традиційним розумінням економічної, соціальної і політичної реальності та

системи міжнародних відносин: 1) часова відмінність (Хронологічний час замінюється майже миттєвою реалізацією дії та потенційної реакції на неї); 2) фізична відмінність (Дії або рішення не обмежені географічно, просторовими рамками чи кордонами суверенних держав); 3) проникність (Комунікації і діяльність у кіберпросторі вільно проникають через державні кордони і суверенну юрисдикцію. Нині держави намагаються контролювати ці процеси, однак з різним ступенем успішності); 4) гнучкість та легкість у зміні моделей взаємодії, появі нових учасників, форм і способів відносин; 5) участь в розумінні створення нових платформ для політичного вираження і мобілізації соціальних ресурсів; 6) складність ідентифікації учасників відносин та зв'язку суб'єктів з конкретними діями, і як наслідок, відсутність належних механізмів відповідальності [5].

М. Яцишин вважає, що сутнісними ознаками кіберпростору є не фізична, а віртуальна природа та нетериторіальність. При цьому термін «віртуальний» науковець визначає, як «уявний, такий, що відображається у свідомості індивіда». Також автор зауважує, що незважаючи на таку ознаку кіберпростору, суспільні відносини та правовідносини зокрема, які виникають, змінюються чи припиняються в цьому віртуальному просторі, залишаються реальними і створюють суб'єктивні права та юридичні обов'язки для суб'єктів. Натомість ознака нетериторіальності є причиною великої кількості юридичних питань щодо визначення приналежності складових елементів правовідносин, що виникають у кіберпросторі, до відповідних правопорядків [6].

На думку І. Рассолова кіберпростір має наступні ознаки: 1) об'єднує глобальні комп'ютерні мережі та інформаційні ресурси, що не мають чітко визначеного власника та забезпечують інтерактивну комунікацію фізичних і юридичних осіб; 2) взагалі не обмежений жодними кордонами; 3) має децентралізований статус, яким повністю не володіє та не управляє жодна держава, об'єднання держав, жодна міжнародна організація, а також жоден оператор зв'язку; 4) є простором, у якому будь-яка особа може вільно діяти, висловлюватися та навіть працювати [7, с. 14-15].

На нашу думку, ознаками кіберпростору, що дозволяють сформувати поняття про нього є: 1) інформаційність (кіберпростір складається з інформаційних мереж та інших інформаційних ресурсів); 2) віртуальність (існування поза межами світу реальних речей, імітація реальності за допомогою комп'ютерних технологій); 3) нематеріальність; 4) відсутність чітких кордонів (є необмеженим і нетериторіальним, визначення юрисдикції тієї чи іншої держави стосовно відносин у кіберпросторі є досить проблематичним); 5) незалежність і автономність (кіберпростір не може належати і бути повністю контрольованим окремим суб'єктом чи суб'єктами); 6) можливість цифрової фіксації усіх вчинків людей, запису і збереження інформації про них, а отже – прогнозування людської поведінки, а іноді, навіть і непрямого спонукання до певних дій (наприклад, таргетована реклама в Інтернеті – оголошення, що демонструються тільки тим користувачам мережі, які відповідають певному набору вимог, визначених рекламодавцем – побудована на збиранні інформації про пошукові запити людини, її профілі в соціальних мережах тощо. Такий же підхід може використовуватися і для маніпулювання свідомістю людей, наприклад, при проведенні виборчих кампаній).

Отже, кіберпростір – це специфічне інформаційне віртуальне середовище, що характеризується можливістю цифрової фіксації поведінки суб'єктів та відомостей про них, не має чітких кордонів, визначеного власника і не управляється жодною державою чи міжнародним об'єднанням.

Варто зазначити, що не всі відносини, які існують в кіберпросторі є правовідносинами (наприклад, спілкування в соціальних мережах, форумах, чатах правом не регулюється, принаймні, доти, доки не створює загроз учасникам чи не зачіпає законних інтересів третіх осіб, інтересів безпеки держави тощо).

Значна частина кіберпростору є де-факто міжнародною. Лише в окремих випадках функціонування інформаційних систем знаходиться під контролем і суверенітетом держав. Це має місце, наприклад у системах, що створені державою для виконання нею своїх функцій (наприклад, система «електронна

демократія в Естонії» [8, с. 7] та пов’язані з нею правовідносини перебувають під суверенітетом Естонії). Тож, можна стверджувати, що значна частина відносин в кіберпросторі може бути врегульована саме засобами міжнародного права, як публічного, так і приватного.

У межах цієї роботи ми не ставили за мету дослідження приватних правовідносин з іноземним елементом, що реалізуються в кіберпросторі, можемо лише констатувати їх фактичну поширеність в сучасних умовах та необхідність врахування локацій не лише учасників таких відносин, але й серверів, специфіки віртуальних об’єктів, що можуть ставати об’єктами правовідносин, а також інших особливостей інформаційного середовища. З огляду на ці обставини, у більшості випадків до таких відносин можуть бути застосовані норми міжнародного приватного права відповідних держав, що стосуються таких правовідносин у реальному вимірі. Однак, зауважимо, що дана проблематика має свою специфіку і потребує окремого дослідження.

Нашим завданням є аналіз тієї частини кібервідносин, що виходить за межі єдиного державного врегулювання, зачіпає інтереси держав та інших суб’єктів міжнародного права, а отже, є предметом регулювання міжнародного публічного права. Відомо, що міжнародне право – це правова система, що складається з принципів і норм, якими регулюються відносини між її суб’єктами – державами, міжнародними організаціями тощо [9]. Предметом міжнародного права є суспільні відносини, що виходять за межі як внутрішньої компетенції, так і територіальних кордонів держав, відносини між суб'єктами міжнародного права.

Низка авторів як в Україні, так і за кордоном, розглядаючи конкретну проблематику стандартів кібербезпеки, протидії кіберзлочинності, інформаційним атакам однієї держави на іншу тощо, відносить їх сфери міжнародно-правового регулювання [10; 11; 12; 13; 14]. Відтак, віднесення кібервідносин до предмету регулювання міжнародного права, на нашу думку, є цілком виправданим, у разі, якщо такі відносини відповідають ознакам міжнародних за суб’єктним критерієм, тобто, їх учасниками виступають

суб’єкти міжнародного публічного права – держави, державоподібні утворення, міжнародні міжурядові організації, інші носії міжнародної правосуб’єктності.

Підтвердженням міжнародного характеру кібервідносин є і те, що питання їх регулювання, в першу чергу, в частині глобальної інформаційної безпеки ще два десятиліття тому стали предметом обговорення на міжнародній арені. Так, у 1998 році Генеральною Асамблеєю ООН ухвалено резолюцію A/RES/53/70 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» [15]. У 1999 році була прийнята оновлена резолюція A/RES/54/49 ГА ООН з аналогічною назвою, яка вказувала на небезпеку інформаційних загроз не лише у цивільній, але і у воєнній сфері [16]. В подальшому ГА ООН ухвалила низку інших резолюцій і активно продовжує працювати над питаннями міжнародної інформаційної безпеки.

Доводиться констатувати, що відносини у кібепросторі ще не здобули належного правового регулювання ні на національному рівні (що, на нашу думку, є дуже проблематичним і навряд чи буде реалізовано в найближчій перспективі), ні на міжнародному. В той же час, певні зусилля щодо вирішення цієї проблеми здійснюються міжнародною спільнотою. Юридично обов’язковими документами, спрямованими на регулювання кібервідносин, є Конвенція про кіберзлочинність (Будапештська конвенція) 2001 року, розроблена Радою Європи [17] та Додатковий протокол до неї 2003 року, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [18]. Конвенція відкрита для підписання як державами-членами Ради Європи, так і державами, що не є членами організації, але брали участь у її розробці. Зокрема, її підписали США, Канада, Японія, ПАР. Україна ратифікувала Конвенцію у 2005 році [19].

Викладене дає підстави стверджувати, що, по-перше, у кіберпросторі чи з застосуванням сучасних інформаційних технологій складаються відносини, що з необхідністю потребують правового регулювання; по-друге, зловживання інформаційними технологіями створює значні ризики і загрози як для окремих осіб, так і для держав, а, можливо, і міжнародної спільноти загалом; по-третє, з

огляду на природу кіберпростору, окремі держави навряд чи зможуть забезпечити дієве правове регулювання зазначених відносин та верховенство права в кіберпросторі. Отже, основою правопорядку у кіберпросторі мають стати саме норми міжнародного права.

Відносини у кіберпросторі є надзвичайно складними для правового впливу, однак вбачається, що створення механізму в цій сфері може спиратися на аналогії з іншими сферами міжнародно-правового регулювання. Міжнародне право з більшим чи меншим успіхом реалізує завдання щодо встановлення правового режиму ведення збройних конфліктів, використання космосу та інших видів міжнародних територій, притягнення до відповідальності осіб, винних у міжнародних злочинах. Тож, вже наявні принципи та юридичні конструкції за умов певного допасування можуть бути використані для створення моделей міжнародно-правового регулювання у сфері відносин, які здійснюються в кіберпросторі.

РОЗДІЛ ІІ. ПРИНЦИПИ ПРАВОВОГО РЕГУЛЮВАННЯ МІЖНАРОДНИХ ВІДНОСИН У КІБЕРПРОСТОРІ

2.1. Застосування принципів міжнародного права до регулювання відносин у кібепросторі

Як було нами з’ясовано у попередньому розділі, відносини у кіберпросторі можуть виступати частиною міжнародних відносин, а отже, на них поширюється дія основних принципів міжнародного права. Принципи міжнародного права відображають характерні риси міжнародного права та мають вищу юридичну силу, вони є правовою основою всіх міжнародних договорів і поширюють свою дію на ті відносини, що безпосередньо не врегульовані міжнародним договором, міжнародним звичаєм чи іншими джерелами міжнародного права [20, с. 354]. Основні принципи міжнародного права закріплені у Статуті ООН [21], Декларації про міжнародні принципи

відповідно до Статуту ООН 1970 р. [22] та Підсумковому акті ОБСЄ, підписаному в Гельсінкі 1975 р. [23]. Варто відмітити, що принципи, зафіксовані в цих документах, великою мірою дублюються, але не співпадають. Перелік, наведений у Підсумковому акті ОБСЄ 1975 р. є більш розширеним, тому вважаємо доцільним взяти саме його за основу подальшої роботи.

Наразі, на нашу думку, основоположним є принцип співробітництва держав, оскільки більшість питань, пов’язаних з діяльністю в інформаційному середовищі не є врегульованими, і лише шляхом співробітництва держав і міжнародних організацій дана проблема може бути вирішена.

Прояв дії цього принципу, спостерігаємо, наприклад, у підсумковій Декларації прийнятій в ході 42-саміту G 7 (26-27 травня 2016 року) йдеться про визнання кіберпростору доступним, відкритим, взаємопов'язаним, надійним та безпечним середовищем і основою економічного зростання та процвітання. Держави висловили свою стурбованість «поширенню використання кіберпростору в цілях тероризму», також підтвердили, що «міжнародне право, включно зі Статутом ООН застосовуються в кіберпросторі».

На саміті було також схвалено Principles and Actions on Cyber та прийнято рішення створити нову робочу групу G7 Cyber, щоб посилити координацію політики та практичного співробітництва країн G7 з метою сприяння безпеці та стабільності в кіберпросторі [24]. Principles and Actions on Cyber містить положення про визнання важливості врегулювання відносин в кіберпросторі для «захисту приватності та кібербезпеки», а також підтримання таких загальних цінностей як «свобода, демократія та права людини». Важливо, що держави G7 взяли на себе зобов’язання «вживати рішучих заходів у тісному співробітництві проти зловживання використанням кіберпростору як державними, так і недержавними суб’єктами, в тому числі терористами» [25].

Результатом співробітництва держав у сфері забезпечення верховенства права в кіберпросторі стали вже згадані Декларації ГА ООН, Будапештська конвенція 2001 року та Додатковий протокол до неї 2003 року. Певні напрацювання щодо регламентації кібербезпеки має Європейський Союз. Так, у

2016 році з була прийнята Директива ЄС з мережевої та інформаційної безпеки [26], яка передбачає стратегію забезпечення мережевої та інформаційної безпеки, визначає обов'язки держав щодо співробітництва, обміну інформацією, реагування на кіберінцеденти тощо. 23 листопада 2016 року Європарламент ухвалив незаконодавчу резолюцію «Стратегічні комунікації ЄС як протидія пропаганді третіх сторін» [27].

Підкреслюючи важливість цих напрацювань, зауважимо, що жоден з названих документів не є саме тим необхідним результатом співробітництва держав, оскільки не регулює питання кіберпростору та кібербезпеки повною мірою. Вважаємо нагальною потребою визначення на міжнародному рівні таких понять, як «кіберпростір», «кібератака», «кіберзброя» тощо. Необхідно врегулювати питання відповідальності за кібератаки, а також розробити механізм притягнення до відповідальності. Держава повинна відповідати за неправомірні дії, і ця відповідальність повинна бути реальною і співмірною, виконуючи превентивну функцію – запобігати подібним ситуаціям. Також необхідно визначити підстави застосування кібератак у відповідь.

Пов'язаним з попереднім є принцип добросовісного виконання зобов'язань за міжнародним правом. Наразі окремого акту, що зобов'язував би держави утримуватися від протиправних дій у кіберпросторі немає, проте загальне застосування цього принципу має великий потенціал для врегулювання зазначеної сфери. У разі успішного результату співробітництва держав в врегулювання відносин у кіберпросторі, принцип добросовісного виконання зобов'язань стає основою для реалізації міжнародних договорів, що будуть прийняті задля запобігання кіберконфліктів, невикористання кіберзброї тощо.

Нормативний зміст принципу суверенної рівності держав розкрито в Декларації принципів міжнародного права 1970 р. Її положеннями передбачено, що суверенною рівністю наділені всі держави, вони мають однакові права й обов'язки та є рівноправними членами міжнародного співтовариства незалежно від відмінностей економічного, соціального, політичного або іншого характеру.

В науці існує багато концепцій державного суверенітету в розрізі кіберпростору. Проаналізувавши їх, вважаємо можливим виділити дві конкуруючі теорії з цього питання.

Перша теорія полягає в тому, що кіберпростір є глобальним і загальним, тобто фактично регулюється комплексно світовим товариством, а не кожною країною окремо. Ця теорія, однак, спотворює важливість державного регулювання і знижує роль держави у кіберпросторі [28, с. 10].

Друга теорія полягає в тому, що кіберпростір має імунітет від державного суверенітету. Одним з найбільш відомих проявів «імунітету кіберпростору» є Декларація Незалежності кіберпростору 1996 року Джона Перрі Барлоу, що була відповіддю на Акт благопристойності комунікацій Правління США, який запроваджував цензуру в Інтернеті. Дана Декларація проголошувала відсутність державної влади над кіберпростором. Автор стверджує, що «кіберпростір – є новою ерою. Цей простір є незалежним від тиранії, яку намагається нав’язати влада. При цьому вона не має ні морального права ні дієвих методів управляти кіберпростором» [29].

Противники цієї теорії стверджують, що кіберпростір не може мати імунітету від державної влади. По-перше, кіберпростір потребує контролю. Певні суб'єкти підтримують існування та функціонування кіберпростору. При цьому, роботу по контролю мережі вони здійснюють на території, що відповідно потрапляє під дію конкретної державної влади. По-друге, фінансові відносини у кіберпросторі потребують державного управління, оскільки в іншому випадку ці відносини не врегульовуються правом і їх учасники є фактично незахищеними [30]. По-третє, контент, що існує в кіберпросторі має вплив на реальний світ. Частина інформації може суперечити політиці і праву держави. Так, наприклад, у справах, що стосувалися вільного поширення дитячої порнографії в кіберпросторі, суди стверджували, що ці відносини повинні підкорятися внутрішньому закону держави. Нарешті, по-четверте, держави повинні мати контроль над кіберпростором в цілях національної безпеки [31, с. 13].

Загалом погоджуючись з наведеними аргументами, зауважимо, що держава не може поширювати свій суверенітет на частину кіберпростору тільки через те, що суб'єкти, які підтримують функціонування певної частини мережі здійснюють свою роботу на території, на яку поширюється державна влада. В умовах функціонування мультинаціональних корпорацій (наприклад, Google), що мають власні контенти в кіберпросторі та координуються з багатьох точок світу, розділення мережі на кілька частин з підпорядкуванням суверенітету окремої держави не уявляється можливим.

Проте ми підтримуємо необхідність суверенного врегулювання фінансових відносин у кіберпросторі, державне врегулювання потоків інформації для недопущення вільного розповсюдження інформації, що суперечить правовим нормам та загрожує національній безпеці держав.

Проаналізувавши значені теорії вважаємо, що жодна не може бути застосована до відносин у кіберпросторі. Обидві теорії ігнорують той факт, що кіберпростір потребує стабільності та регуляції, яку забезпечує державний суверенітет, при цьому кожна держава має реальний інтерес до здійснення свого контролю над кіберпростором. З одного боку, не всі відносини в мережі мають імунітет від державної влади, з іншого, існують певні інформаційні структури, які в цілях національної безпеки не можуть бути загальними, що виключає застосування першої теорії.

Наступною складністю в застосуванні цього принципу є визначення території на яку поширюється суверенітет однієї держави, а на яку – іншої. Чітке визначення інформаційних кордонів певної держави не є можливим, та і заборона втручання до інформаційного простору країни не видається реальною. В мережі Інтернет абонент має доступ до будь-якого сайту незалежно від місця входу в систему та територіальної локації серверу, на якому сайт розміщений.

Як уже зазначалося діяльність інформаційних систем, що створені державою для виконання нею своїх функцій, повною мірою підпадають під суверенітет і юрисдикцію цієї держави. Однак, на інші правовідносини у кіберпросторі, що не координуються органами державної влади, суверенітет не

поширюється. Отже для застосування даного принципу вважаємо за доцільне умовно поділяти кіберпростір на державний та міжнародний простір.

Відповідно до принципу невтручання у внутрішні справи держав неправомірним є втручання однієї держави в інформаційну систему іншої, з метою видалити, змінити або додати нову інформацію. Також, в контексті цього принципу доцільно згадати про ворожу пропаганду – використання будь-якої неправдивої, зміненої чи перекрученої інформації з метою пливу на населення іншої держави також є втручанням у внутрішні справи. Відповідно принцип можна розглядати в 2 аспектах: як недопущення втручання в інформаційну систему держави з метою додавання, зміни чи видалення інформації та як заборону ворожої пропаганди з використанням телекомунікаційних мереж.

Варто зауважити, що кіберпростір в основному використовується для комунікацій. При цьому, можливо, що конфіденційна інформація однієї держави може бути перехоплена, оскільки вона передається через кібер-структуру, розміщену на території іншої держави. Окрім того, з появою так званих «хмар» одна держава може зберігати конфіденційну інформацію на сервері, який знаходиться на території іншої держави. В таких випадках держава має право заявити про право власності на цю інформацію, але порушення територіального суверенітету фактично немає. Проте в разі, якщо інформація держави А, що міститься на сервері держави Б була перехвачена державою В, то саме держава Б може заявити про порушення її суверенітету. При цьому держава А, якій належить інформація, фактично є незахищеною. Саме в цьому випадку, на нашу думку, застосування принципу невтручання є найбільш важливим.

На нашу думку, кібератака – це різновид порушення принципу невтручання, який як визначив Міжнародний Суд ООН не допускає втручання в справи держави «в питаннях, в яких кожна держава відповідно до принципу державного суверенітету вільно вирішує (наприклад, вибір політичної, економічної й культурної системи та формулювання зовнішньої політики) [38].

Для застосування цього принципу важливим є визначення ознак, які свідчать про наявність незаконного втручання в справи держави. Так, Russell Buchan виділяє наступні необхідні умови: 1) скоєне діяння безпосередньо втручається в справи держави; 2) дія має примусовий характер. При цьому автор зазначає, що примусовий характер полягає в примусовій зміні політики держави, компрометуванні дій держави чи підривання авторитету державних структур [31, с. 74, 79].

Також вважаємо, що на конфіденційну інформацію однієї держави, що розташована на сервері іншої, поширюється суверенітет першої держави, оскільки в даному випадку вирішальне значення має не територія, на якій дана інформація зберігається. Підтвердженням цього може слугувати рішення Міжнародного Суду ООН у справі між Східним Тимором і Австралією (2014 рік). Східний Тимор стверджував, що Австралія направила своїх агентів у офіс австралійського адвоката, який виступав юридичним радником у Східному Тіморі для збору конфіденційної інформації, що стосується судових процесів між двома державами. Цей офіс був фізично розташований в Австралії. Східний Тимор звернувся до Міжнародного Суду заявивши, що «Австралія, захопивши документи та дані, порушила суверенітет Східного Тимора» і що «Австралія повинна негайно повернути до призначеного представника Східного Тимора всі вищезазначені документи і дані, а також знищити кожну копію таких документів та даних, що знаходяться в володінні або контролі Австралії» [33].

Вирішуючи справу, Міжнародний Суд зазначив, що «на цьому етапі розгляду справи Суд не зобов'язаний остаточно визначити, чи існують права, які Східний Тимор бажає захистити; потрібно лише вирішувати, чи дійсні права, на які претендує Східний Тимор в позові, і для яких він вимагає захист».

Важливо відзначити, що Міжнародний суд визнав права Східного Тимору «дійсними» і видав тимчасову постанову про те, що «Австралія не повинна жодним чином втручатися у зв'язки між Східним Тимором та його юридичними радниками »[33].

Важливе значення для регулювання відносин у кіберпросторі має принцип рівноправності та самовизначення народів. Будь-які пропагандистські дії, спрямовані на викривлення реальності і впливу на самовизначення певної спільноти є неправомірними. Ніхто не може втручатися в інформаційні системи чи здійснювати пропаганду, з метою порушення цього принципу.

Через неможливість застосовувати класичну зброю у кіберпросторі, значну специфіку має принцип незастосування сили чи погрози силою. Наразі, офіційне міжнародно-правове визнання інформаційних атак агресією чи інших кіберзасобів – зброєю, відсутнє, тож кваліфікація застосування кіберзброї як порушення принципу незастосування сили є проблематичною.

В своєму Дорадчому висновку про законність використання ядерної зброї, Міжнародний суд ООН визначає, що ст. 2, 4, 51 і 42 Статуту ООН «не стосуються конкретної зброї. Вони застосовуються до будь-якого застосування сили, незалежно від зброї, що використовується» [34]. Відповідно, можна стверджувати що теж саме стосується і використання кіберзброї.

Варто зазначити, що низка країн включають кібертехнології в свої воєнні доктрини. Так. США мають на своїй території спеціальні військові частини з кіберекспертними підрозділами, а Пентагон обстоює позицію, що комп'ютерні віруси – це ще одна система озброєння, дешевша і швидша, ніж ракета, більш прихована і не менш руйнівна [35]. Неодноразово заявляли про те, що будуть оцінювати кібератаки як акти війни вищі посадові особи Російської Федерації, Великої Британії та інших держав. Міністр оборони Естонії прирівнює кібер-блокади до морських блокад на порти, що перешкоджають доступу держави до інших частин світу [36, с.306]. При цьому, відсутність міжнародно-правового визнання інформаційних атак агресією ставить під сумнів можливість міжнародно-правового захисту держав від застосування кіберзброї іншими державами чи приватними особами але за сприяння державних структур.

Отже, застосування сили – це застосування спеціальних хакерських програм, для того щоб змінити, доповнити або видалити частину інформації, або паралізувати чи повністю зруйнувати інформаційну систему певної країни.

Варто відмітити, що прикладів погрози застосування кіберзброї у сучасному світі порівняно небагато. Загалом, це випадки, коли було здійснено атаку на інформаційну систему певної країни, і відбуваються контратаки у відповідь. Принцип незастосування сили чи погрози застосування забороняє подібні дії. Відповідно до нього, жодна держава чи структура, під егідою держави не може застосовувати кіберзброю до інформаційної системи іншої держави.

Пов'язаним з попереднім є принцип мирного врегулювання спорів. В цьому контексті значний інтерес представляє Міжнародна стратегія співробітництва в кіберпросторі, спільно створена Міністерством закордонних справ та Адміністрацією кіберпростору Китаю. Відповідно до Стратегії, «міжнародне співтовариство має дотримуватися цілей та принципів, закріплених в Статуті ООН, зокрема незастосування сили та мирного врегулювання спорів, з метою забезпечення миру та безпеки в кіберпросторі. Всі країни повинні протидіяти ворожості та агресії, запобігати нарощуванню озброєнь та конфліктам в кіберпросторі і врегульовувати спори мирним шляхом» [37]. Документ, не маючи жодної юридичної сили, фактично є одним з проявів визнання державами необхідності мирного вирішення конфліктів, що виникають у кіберпросторі.

Варто зауважити, що визначення організатора кібератаки є доволі складним процесом. У більшості випадків держави не зізнаються в своїй винуватості, а повністю заперечують звинувачення в їхню сторону. Проте атака не припиняється. Відповідно потерпіла держава застосовує силу у відповідь. При цьому міжнародне право не виключає можливості застосування сили у відповідь до втручання Ради Безпеки ООН, але таке застосування має бути повинно бути співрозмірним. Відтак, застосування кібератак у відповідь є можливим, проте, до належного врегулювання такої відповіді та визначення органу, який повинен втрутитися у разі застосування кіберзброї, дане питання залишається відкритим.

Вважаємо, що держава має право застосувати кіберзброю у відповідь на кібератаку своєї інформаційної системи, але дана атака повинна відповідати

критеріям необхідності, пропорційності (не завдавати більшої шкоди ніж це необхідно, для того, щоб дати відсіч нападнику), орієнтації на інформаційні мережі державних структур без шкоди цивільним об'єктам критичної інфраструктури та населенню. Самооборона повинна бути спрямована на запобігання подальшій агресії та припинитися після досягнення її цілей.

Наведені критерії є загальними, потребують деталізації, адже на практиці можуть виникати питання, наприклад, про те, хто і як визначає співмірність кібератак у відповідь, які конкретно об'єкти можуть бути об'єктом атаки тощо.

Що ж стосовно мирного вирішення конфлікту, воно видається можливим, коли обидві сторони визнають наявність інциденту і мають намір врегулювати конфлікт. У сучасному світі не було випадків мирного врегулювання кібератак. Держава або застосовує кібератаку у відповідь, або намагається захистити свою інформаційну систему іншим шляхом, але визнання подібних ситуацій як конфлікту і пропозицій мирного вирішення ситуації наразі не було. На нашу думку, це обумовлено тим, що інформаційні конфлікти не є відкритими і офіційно не вважаються збройними конфліктами. Держава агресор не визнає здійснення нею атаки. Встановити безсумнівну винуватість держави надзвичайно складно. Найчастіше атака висвітлюється як дія конкретної особи, що немає безпосереднього зв'язку з державою.

Вважаємо, що повинна бути сформована нормативна база, відповідно до якої кіберконфлікти будуть прирівняні до інших збройних конфліктів. У такому разі буде можливим і мирне їх врегулювання.

Принципи непорушності кордонів та територіальної цілісності держав фактично неможливо застосувати до кібервідносин, оскільки, як зазначалося раніше, не є реальним визначення і встановлення чітких кордонів у кіберпросторі. Аналогічно неможливо встановити конкретно на території якої держави функціонує та чи інша інформаційна мережа. Цей принцип можна застосовувати в тому аспекті, що жодна держава не може втручатися та/або встановлювати контроль над діяльністю інформаційних мереж, що координуються органами іншої держави. Проте, варто зауважити, що це

питання більш тісно пов’язане з суверенітетом певної держави ніж з принципами непорушності кордонів та територіальної цілісності держав.

Принцип поваги до прав і свобод людини повинен застосовуватися незалежно від того де відбуваються правовідносини, у реальному світі чи у кіберпросторі. Загальна декларація прав людини 1948 року визначає, що ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, тайну його кореспонденції або на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань [38]. Відповідно це право порушується, коли інший суб’єкт втручається до особистих даних, кореспонденції тощо іншої особи. Сучасні технології дозволяють «зламати» будь-які сторінки, замки чи зашифровану інформацію. Проте, така діяльність є протиправною і порушує право людини на недоторканність кореспонденції, особистого життя. Коли ж атака спрямована на інформаційну систему цілої держави, то відповідно порушуються права всіх її громадян, а також інших осіб, інформація про яких, наявна в цій системі. Це глобальне порушення прав і свобод. Неврегулювання цього питання на міжнародному рівні призводить до того, що ніхто не може бути певен, що його інформація в кіберпросторі є захищеною від стороннього втручання. На нашу думку, особа повинна бути впевненою в захисті її прав і свобод, як в реальному світі, так і віртуальному. Саме тому держави та міжнародні організації зобов’язані врегулювати питання, пов’язані з відносинами в кіберпросторі.

Даний принцип має і іншу сторону застосування. Свобода вираження думки є основою для будь-якої демократії та процесу демократизації. Не слід забувати, що права людини дійсно призначені для захисту окремих осіб, а не політичних систем та їх дій. Тому неможливо обмежувати ці права з міркувань національної безпеки.

2.2. Спеціальні міжнародно-правові принципи використання кіберпростору

Як показано вище, більшість основних принципів міжнародного права мають пряме застосування до відносин у кіберпросторі. Проте, з огляду на специфіку кіберпростору доцільним є розроблення системи спеціальних міжнародно-правових принципів, застосовуваних до відносин у кіберпросторі. На нашу думку, такі принципи мають відображати природу кіберпростору та правовідносин, що реалізуються в мережі, з огляду на об'єктивні потреби правового регулювання. Відповідно, вважаємо можливим виділити наступні засади, що мають обумовлювати поведінку держав і інших суб'єктів міжнародного права у кіберпросторі.

1). Принцип автономності та незалежності кіберпростору. Кіберпростір не має визначеного власника. Жоден суб'єкт, група суб'єктів чи організація не можуть цілісно управляти кіберпростором. Його не можна привласнити, продати чи купити. Ним можна лише користуватися. Кіберпростір існує незалежно від волі суб'єктів. Він є автономним, і не може врегульовуватися якоюсь міжнародною організацію чи органом державної влади. У цьому аспекті варто розрізняти поняття кіберпростору та відносин у кіберпросторі. Кожна особа може бути ініціатором створення відносин у кіберпросторі, але не може впливати на його фактичне існування. Аналогічно, орган чи організація може здійснювати вплив на правовідносини в мережі, але не впливає безпосередньо на саму мережу. У разі здійсненні кібератаки, наслідком є не зруйнування кіберпростору певної держави (організації), а зруйнування відносин які існують в інформаційному середовищі, і на які була націлена атака.

2). Принцип визнання відсутності кордонів кіберпростору. Оскільки кіберпростір не є територією в класичному значенні, він не має окремих ознак територіальності, однією з яких є визначення кордонів. Низка країн все ж здійснювали спроби у визначенні власних кіберкордонів. Так, прикладом може бути спроба визначити кордони кіберпростору США, запропонована

полковником Сухопутних військ США Jeffery R. Schilling. Він пропонує кілька підходів, до визначення кордонів кіберпростору. Перший полягає в тому, щоб просто стверджувати, що кордони кіберпростору відображають фізичні національні кордони США. Другий підхід до визначення національної межі кіберпростору передбачає визначення будь-яких логічних доменів або мереж, контрольовані організаціями, розташованими в межах юрисдикції США, підпорядкованих політиці та захисту США, незалежно від глобальної позиції IT-систем, що складають ці віртуальні середовища [39, с. 8-9]. Варто зазначити, що дані підходи не були реалізовані, оскільки це дійсно неможливо з огляду на показані нами вище об'єктивні характеристики кіберпростору. Вбачається, що державам варто визнати нереальність визначення кордонів кіберпростору, адже він не є територією, яка поділена на частини, належні окремим суверенам.

3). Принцип невтручання в державний сектор кіберпростору. Відповідно до цього принципу жоден суб'єкт міжнародного права не має право втручатися до державного сектору кіберпростору іншої країни. Фактично, ми не можемо реально поділити кіберпростір на частини, і встановити внутрішні кордони. Проте, як розглядалося нами у першому розділі, відносини у кіберпросторі можуть піддаватися та не піддаватися державному впливу. Відповідно, вважаємо, що ті інформаційні вузли кіберпростору, які безпосередньо створені за волею держави, для забезпечення виконання її функцій, а також контролюються та регулюються державною владою, є державним сектором кіберпростору. Дані правовідносини мають адміністративний характер підпорядкування. Саме через них реалізуються відносини з держави з населенням певної території. На такі відносини поширюється виключно суверенітет конкретної держави, інші ж суб'єкти не можуть втручатися в них.

Цей принцип ґрунтується на суверенітеті держав і випливає з того, що даний сектор включає в себе найбільш важливі суспільні відносини, які забезпечуються державною владою. Він конкретизує загальні міжнародно-правові положення щодо невтручання у внутрішні справи держави. До внутрішніх справ держави належать всі відносини, що є складовою частиною

державного сектору кіберпростору. На нашу думку, ця конкретизація є обов'язковою, оскільки відсутність дефініції надає можливість суб'єктам-порушникам, стверджувати, що їхні дії не порушують принципи права.

Складовою принципу має бути також заборона ведення злочинної пропаганди. Вона означає, що жоден суб'єкт міжнародного права не може втручатися в інформаційну систему іншого, з метою видалення, додавання, перекручення інформації, щоб викривити ставлення до цього суб'єкта, підірвати його авторитет тощо.

4) Поєднання державного, міжнародного регулювання та самоуправління у кіберпросторі. Відповідно до нього, держава здійснює управління власним державним сектором. Міжнародне управління реалізується стосовно правовідносин, які за своєю природою є міжнародними і не підкоряються національним правопорядкам. Самоуправління реалізується в сфері суспільних відносин, що не регулюються правом.

5) Принцип нейтралітету кіберпростору та запобігання міжнародним конфліктам у ньому. Нейтралітет кіберпростору означає заборону застосування кіберзброї. Фактично заборонити розроблення різних шкідливих інформаційних програм неможливо. Пропонуємо заборонити використання таких програм в інформаційному середовищі, за аналогією заборони використання зброї в космосі. Відповідно до цього принципу необхідним є створення спеціальних міжнародно-правових механізмів недопущення ворожого використання кіберпростору, оскільки, як вже було показано нами, сучасне міжнародно-правове регулювання не є повністю придатним для цілей протидії застосуванню сили чи погрози силою у кіберпросторі.

6) Принцип пропорційності (співрозмірності) необхідної самооборони в кіберконфліктах. Проблема пропорційності є однією з найбільш складних і неінтерпретованих для кіберпростору. Очевидно, з часом вона буде проаналізована в доктрині і визначена практикою міжнародних судів. Поки що її слід інтерпретувати за аналогією, відповідно до чинних норм міжнародного права збройних конфліктів. Контратака повинна дозволятися лише у

виняткових випадках, якщо інші механізми протидії не дають результату. Положення Статуту ООН, які стосуються застосування сили, можуть бути застосовані до кібернетичної війни, навіть з огляду на те, що Статут приймався задовго до появи кібертехнологій. Відсутність спеціальних міжнародно-правових норм стосовно інформаційної війни не дає державам підстав діяти проти інших держав без обмежень.

7) Принцип відповідальності держав за порушення вимог щодо заборони ведення злочинної пропаганди, нейтралітету кіберпростору та пропорційності заходів у відповідь. Попередженню кіберконфліктів могло б сприяти прийняття міжнародного документа, який визначив би принципи добросовісної поведінки держав у сфері інформаційної безпеки. Зокрема, пропонуємо включити до нього зобов'язання держав не вести ворожу пропаганду і нести міжнародно-правову відповідальність за кібератаки. Оскільки безпосередніми виконавцями кібератак і поширювачами неправдивої ворожої інформації є, як правило, приватні особи, вважаємо за потрібне передбачити відповідальність держав за інформаційну діяльність, пов'язану з їх територією та юрисдикцією. На прикладі україно-російського конфлікту бачимо, що розповсюдження брехливих повідомлень у ЗМІ, свідоме перекручування медіа, зареєстрованими в РФ чи фінансованими звідти, фактів на шкоду нашій державі, спроби насадження ідеології, яка заперечує існування української нації і державності, є системною практикою. Низка особливо недолугих «фейків» навіть була спростована самими їх поширювачами, однак жоден телеканал чи журналіст не поніс відповідальності за неправдиве інформування суспільства. Видається можливим передбачити зобов'язання держав встановлювати відповідальність і застосовувати її заходи до осіб, які свідомо (а якщо довести умисне перекручування фактів неможливо – неодноразово) розповсюджували ворожі до іншої держави неправдиві повідомлення. У разі, якщо держава не робить цього, слід визнавати факт інформаційної війни і покладати відповідальність на державу.

8) Принцип поєднання зусиль держав у побудові глобальної системи кібербезпеки має передбачати взаємну допомогу держав у цій сфері та гармонізацію національних законодавств. У першу чергу, допомога має надаватися країнам, що розвиваються і не мають власних технологій та фінансових ресурсів для створення ефективних систем кіберзахисту.

9) Принцип обміну інформацією про кіберзагрози та координації взаємодії між державами. Обмін інформацією про загрози, вразливість та навіть непояснені аномалії в інформаційних системах є критично важливим для забезпечення безпеки держав і міжнародної спільноти в цілому, оперативного реагування на проблеми, що виникають. Потреба ж у координації, крім іншого, особливо необхідна з огляду на нетериторіальність кіберпростору, відсутність кордонів та утрудненість визначення локації дій і суб'єктів.

10) Принцип заборони торгівлі інформацією про приватних осіб та компанії, технології і продукти, які ними використовуються, вразливі елементи кібербезпеки приватного сектору. Непоодинокими є випадки, коли держави це роблять з метою досягнення власних цілей [40]. Незалежно від того, наскільки правомірними і необхідними є такі цілі, міжнародна спільнота має засудити і заборонити подібну практику, запровадивши відповідні запобіжні норми.

11) Принцип захисту права на доступ до Інтернету. У липні 2012 року Рада ООН з прав людини визнала необхідність захисту цього права [41]. Світу вже відомі спроби встановлення меж такого доступу, наприклад, запроваджені КНР, через заборону доступу до іноземних сайтів, розміщення гіперпосилань на них або фільтрування результатів пошуку у пошукових системах [42]. Такі дії держав свідчать про значні обмеження демократичних свобод та тенденції до тоталітаризму, а отже, мають бути заборонені міжнародним правом.

Підсумовуючи викладене, варто зазначити, що міжнародно-правові акти, що врегульовували б питання відносин в кіберпросторі та закріпили б наведені принципи є необхідними, враховуючи зростання ролі мережі в житті суспільства, а наведений перелік принципів має стати їх стрижневою основою.

ВИСНОВКИ

Проведене в роботі дослідження дало змогу сформулювати наступні висновки.

1. Кіберпростір – це специфічне інформаційне віртуальне середовище, що характеризується можливістю цифрової фіксації поведінки суб'єктів та відомостей про них, не має чітких кордонів, визначеного власника і не управляється жодною державою чи міжнародним об'єднанням.

2. Ознаками кіберпростору, що дозволяють сформувати поняття про нього є: а) інформаційність (кіберпростір складається з інформаційних мереж та інших інформаційних ресурсів); б) віртуальність (існування поза межами світу реальних речей, імітація реальності за допомогою комп'ютерних технологій); в) нематеріальність; г) відсутність чітких кордонів (є необмеженим і нетериторіальним, визначення юрисдикції тієї чи іншої держави стосовно відносин у кіберпросторі є досить проблематичним); д) незалежність і автономність (кіберпростір не може належати і бути повністю контрольованим окремим суб'єктом чи суб'єктами); е) можливість цифрової фіксації усіх вчинків людей, запису і збереження інформації про них.

3. У кіберпросторі чи з застосуванням сучасних інформаційних технологій складаються відносини, що з необхідністю потребують правового регулювання. Зловживання інформаційними технологіями створює значні ризики і загрози як для окремих осіб, так і для держав і міжнародної спільноти загалом. З огляду на природу кіберпростору, окремі держави навряд чи зможуть забезпечити дієве правове регулювання зазначених відносин та верховенство права в кіберпросторі. Отже, основою правопорядку у кіберпросторі мають стати саме норми міжнародного права.

4. Віднесення кібервідносин до предмету регулювання міжнародного права є цілком виправданим, у разі, якщо такі відносини відповідають ознакам міжнародних за суб'єктним критерієм, тобто, їх учасниками виступають суб'єкти міжнародного публічного права – держави, державоподібні утворення,

міжнародні міжурядові організації, інші носії міжнародної правосуб'єктності. Вже наявні принципи та юридичні конструкції за умов певного допасування можуть бути використані для створення моделей міжнародно-правового регулювання у сфері відносин, які здійснюються в кіберпросторі.

5. Основні принципи міжнародного права мають пряме застосування до регулювання міжнародних відносин у кіберпросторі з урахуванням специфіки цих відносин. В окремих випадках їх слід інтерпретувати за аналогією, переносячи нормативні моделі реальних міжнародних відносин на відносини, що здійснюються у віртуальному середовищі, але мають справляють реальний вплив на держави і міжнародну спільноту загалом.

6. Пропонується до спеціальних міжнародно-правових принципів використання кіберпростору віднести: принцип автономності та незалежності кіберпростору; визнання відсутності кордонів кіберпростору; невтручання в державний сектор кіберпростору; поєднання державного, міжнародного регулювання та самоуправління у кіберпросторі; принцип нейтралітету кіберпростору та запобігання міжнародним конфліктам у ньому; принцип пропорційності (співрозмірності) необхідної самооборони в кіберконфліктах; принцип відповідальності держав за порушення вимог щодо заборони ведення злочинної пропаганди, нейтралітету кіберпростору та пропорційності заходів у відповідь; поєднання зусиль держав у побудові глобальної системи кібербезпеки; принцип обміну інформацією про кіберзагрози та координації взаємодії між державами; принцип заборони торгівлі інформацією про приватних осіб та компанії, технології і продукти, які ними використовуються, вразливі елементи кібербезпеки приватного сектору; принцип захисту права на доступ до Інтернету.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності / В. М. Фурашев // Інформація і право. – 2012. – № 2(5). – С. 162–175.

2. Козуб О. О. Кіберпростір як середовище породження і самореалізації принципу космополітизму / О. О. Козуб // Гуманітарний вісник ЗДІА. – 2010. – Випуск 43. – С. 176–179.

3. Литвинов Є. П. Щодо питання про визначення поняття «інтернет-право» / Є. П. Литвинов // Часопис Академії адвокатури України. – 2013. – № 3. – С. 1–6.

4. The United States Army's Cyberspace Operations. Concept Capability Plan 2016-2028. 22 February 2010. Available at: https://fas.org/irp/doddir/army/pam525-7-8.pdf

5. Choucri Nazli. Emerging Trends in Cyberspace:Dimensions & Dilemmas Conference on Cyberspace: Malevolent Actors, Criminal Opportunities and Strategic Competition Mathew B. Ridgeway Center, University of Pittsburgh

6. Яцишин М. Ю. Особливості визначення поняття «кіберпростір» як особливого середовища міжнародно-правового регулювання [Електронний ресурс] / М. Ю. Яцишин, Е. П. Грановська. – Режим доступу : http://www.vuzlib.com.ua/articles/book/34063-Osoblivosti_viznachennja_ponj/1.html.

7. Рассолов И. М. Право и Интернет. Теоретические проблемы: монография / И. М. Рассолов. – 2-е изд., доп. – М. : Норма, 2009. – 384 с.

8. Грицяк Н. В. Електронна демократія : навч. посіб. / Н. В. Грицяк, С. Г. Соловйов; за заг. ред. д-ра наук з держ. упр., проф. Н. В. Грицяк. – К. : НАДУ, 2015 – 66 с.

9. Шемшученко Ю. С. Міжнародне право / Юридична енциклопедія в 6-ти томах. – К. : Видавництво «Українська енциклопедія» ім. М. П. Бажана, 2002. – Т. 3. – С. 669.

10. Кубышкин А. В. Международно-правовые проблемы обеспечения информационной безопасности государства : дисс. … канд. юрид. наук: 12.00.10 – Международное право ; Европейское право [Электронные ресурс] / А. В. Кубышкин;. – М., 2002. – Режим доступа : http://lawbook.online/regulirovanie-pravovoe-mejdunarodnoe/mejdunarodno-pravovyie-problemyi-obespecheniya.html

11. Широкова-Мурараш О. Г. Кіберзлочинність та кібертероризм як загроза інформаційній безпеці: міжнародно-правовий аспект / О. Г. Широкова-Мурараш, Ю. Р. Акчурін // Інформація і право. – 2011. – № 1(1). – С. 76-81.

12. Міжнародні стандарти з кібербезпеки та їх застосування в Україні (матеріали круглого столу м. Харків, 19 квіт. 2016 р.) / за ред. А. П. Гетьмана, Б. М. Головкіна. – Х. : Право, 2016. – 88 с.

13. Papanastasiou A. Application of International Law in Cyber Warfare Operations. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1673785

14. Hayes C. Law of Cyber Warfare / Carol M. Hayes and Jay P. Kesan // International Encyclopedia of Digital Communication and Society (Wiley-Blackwell), 2014 (Forthcoming). Illinois Public Law Research Paper No. 14-26. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2396078

15. Developments in the field of information and telecommunications in the context of international security UN General Assembly A/RES53/70.: Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement

16. Developments in the field of information and telecommunications in the context of international security UN General Assembly A/RES/54/49. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/777/13/PDF/N9977713.pdf?OpenElement

17. Конвенція про кіберзлочинність [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/994_575

18. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/994_687

19. Про ратифікацію Конвенції про кіберзлочинність : закон від 07.09.2005 № 2824-IV. – [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/2824-15

20. Савчук К. О. Поняття та зміст принципів міжнародного права у працях Всеволода Пійовича Даневського / К. О. Савчук // Часопис Київського університету права. – 2015. – № 3. – С. 354–357.

21. Статут Організації Об'єднаних Націй і Статут Міжнародного Суду [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/995_010.

22. Декларація про принципи міжнародного права, що стосуються дружніх відносин та співробітництва між державами відповідно до Статуту Організації Об'єднаних Націй [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/995_569.

23. Заключний акт Наради з безпеки та співробітництва в Європі [Електронний ресур]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/994_055.

24. G7 Ise-Shima Leaders' Declaration G7 Ise-Shima Summit, 26-27 May 2016. Available at: http://www.mofa.go.jp/files/000160266.pdf

25. G7 Principles and Actions on Cyber. Ise-Shima, Japan, May 27, 2016 Available at: http://www.g8.utoronto.ca/summit/2016shima/cyber.html

26. Network and Information Security (NIS) Directive. (EU) 2016/1148. Available at: https:// ec.europa.eu/digital-single-market/news/network-and-information-security-nis-directive

27. EU strategic communication to counteract propaganda against it by third parties 2016/2030 (INI) – Available at: 23/11/2016 http://www.europarl.europa.eu/oeil/popups/summary.do?id=1465158&t=d&l=en

28. Patrick W Franzese. Sovereignty In Cyberspace: Can It Exist? Available at: https://www.law.upenn.edu/live/files/3473-franzese-p-sovereignty-in-cyberspace-can-it-exist

29. John Perry Barlow. A Cyberspace Independence Declaration, Available at: http://w2.eff.org/Censorship /Internetcensorshipbills/barlow_0296.declaration

30. Jack L. Goldsmith & Tim Wu. Who Controls The Internet?: Illusions Of A Borderless World 29-46 (Oxford Univ. Press 2006). Reviewed by: Robert C. Sanfilippo. Available at: http://jost.syr.edu/wp-content/uploads/who-controls-the-internet_illusions-of-a-borderless-world.pdf

31. Russell Buchan. The International Legal Regulation of State-Sponsored Cyber Espionage // International Cyber Norms:Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch4.pdf

32. Militarv and Puramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986. Available at: http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

33. Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia). Overview the Case. Available at: http://www.icj-cij.org/en/case/156

34. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1. C.J. Reports 1996, p. 226. Available at: http://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

35. Lewis. J. To Protect the U.S. Against Cyberwar, Best Defense is a Good Offense, U.S. News and World Report, 29 April 2010. Available at: www.usnews.com/articles/opinion/2010/03/29/to-protect-the-us-against-cyberwar-best-defense-is-a-good-offense.html

36. Radziwill Y. Cyber-Attacks and the Exploitable Imperfections of International Law. Available at:

https://books.google.com.ua/books?id=RydACgAAQBAJ&pg=PA306&lpg=PA306&dq=www.nato-pa.int/default.asp?SHORTCUT+%3D1782&source=bl&ots=t7wNyAHmhC&sig=awfUndY3WzfMGKS-PPjjJ0ZwuR4&hl=ru&sa=X&ved=0ahUKEwiZrJKV-IvZAhVBsywKHXCKBRoQ6AEINDAB#v=onepage&q=www.nato-pa.int%2Fdefault.asp%3FSHORTCUT%20%3D1782&f=false

37. International Strategy of Cooperation on Cyberspace. China Daily. Updated: 2017-03-02 07:46. Available at: http://www.chinadaily.com.cn/opinion/2017-03/02/content_28401127.htm

38. Загальна декларація прав людини [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/995_015.

39. Jeffery R. Schilling. Defining Our National Cyberspace Boundaries. Strategic Research Project. U.S. Army War College. Available at: http://indianstrategicknowledgeonline.com/web/Defining%20our%20national%20cyberspace%20boundaries.pdf

40. The Digital Arms Trade, The Economist, March 30, 2013. Available at: aka.ms/Economist-Digtial-Arms

41. HRC Affirms that Human Rights Must Also Be Protected on the Internet (Resolution Text). Available at: http://geneva.usmission.gov/2012/07/05/internet-resolution

42. Philipp W. How China Is Blocking Tor / Philipp Winter, Stefan Lindskog. - 2 Apr. 2012. – Available at: https://arxiv.org/pdf/1204.0447.pdf