УДК 341:004

Микола Камчатний,

аспірант кафедри міжнародного права
Національного юридичного університету імені Ярослава Мудрого

ЗАБОРОНЕНІ ЗАСОБИ ВЕДЕННЯ КІБЕРВІЙНИ

Статтю присвячено дослідженню заборонених засобів ведення кібервійн суб'єктами міжнародного права. У статті досліджено наявні поняття кіберзброї як засобу ведення війни, виокремлено основні характерні ознаки даного виду озброєнь. Розглянуто основні підходи до формування нових обмежувальних підходів щодо заборони використання кіберзброї. Автор вперше в українській доктрині аналізує питання виділення нового засобу ведення війни, порівнює наявні види озброєнь із новим – кіберзброєю.

Ключові слова: кібервійна, кіберзброя, міжнародне гуманітарне право, право збройних конфліктів, кіберпростір, кібератака, міжнародна інформаційна безпека.

Постановка проблеми. Протягом усієї історії людства велися війни. Навіть у прадавні часи люди досить швидко зрозуміли необхідність врегулювання певних аспектів щодо проведення збройних протистоянь. Спочатку сторони найчастіше домовлялися про обмеження використання певних видів озброєнь (наприклад, отруєних стріл). Також широко заборонялося позбавлення життя поранених осіб, отруєння колодязів, позбавлення захоплених полонених деяких частин тіла. Пізніше обмежувалося право захоплювати рабів. Усе це свідчить про чітке розуміння людства на всіх етапах його розвитку, що відсутність врегулювання у вирішенні конфліктів силовими засобами сприятиме надзвичайно жорстокому їх перебігу, значним втратам та жертвам не лише серед військових, але й серед мирного населення. З часом перелік видів озброєнь, а відповідно, і заборонених засобів ведення війни поступово збільшувалися. Нині можна з упевненістю говорити про становлення нового засобу ведення війни – кіберзброю.

Аналіз останніх досліджень. У своїх працях даної проблематики фрагментарно торкалися такі українські вчені: Д. Дубов, А. Войцехівський, О. Мережко, Ю. Разметаєва, В. Бабенко. Серед закордонних учених цій темі свої роботи присвячували: Дж. Карр (J. Carr), М. Лібіцкі (M. Libicki), Х. Лін (H. Lin), М. Магомедов, Т. Рід (T. Rid), Е. Філіол (E. Filiol), В. Хайнтшель вон Хайнег (W. Heintschel von Heinegg), Г. Шинкарецька, В. Каберник, М. Шмідт (M. Schmitt), Л. Віхул (Liis Vihul), С. Меле (Stefano Mele) та ін. Більшість авторів наголошують на тому, що використання кібернетичних засобів ведення війни є цілком реальним, а тому потребує міжнародно-правового врегулювання та відповідного закріплення.

Завданням даної статті є проведення аналізу наявних видів озброєння порівняно з новим засобом ведення війни – кіберзброєю, дослідження наслідків його застосування, з'ясування правомірності використання таких засобів з точки зору міжнародного гуманітарного права.

Виклад основного матеріалу. Вже з XIX ст. почалося активне впровадження міжнародних норм, які були спрямовані на обмеження свавілля учасників конфліктів на полі бою та поза його межами. Відповідно, протягом другої половини XIX ст. було підписано низку Гаазьких та Женевських конвенцій. На цьому етапі можна остаточно говорити про утвердження такої галузі міжнародного права, як міжнародне гуманітарне право.

Поступово держави – підписанти значної кількості угод обмежували себе у засобах та методах, що вони використовували до цього з метою отримання стратегічної переваги на полі бою. Кожен з історичних етапів розвитку людства супроводжувався і певним розвитком технологій. Наслідком цього було, відповідно, і постійне оновлення видів озброєння.

Сьогодні людство остаточно увійшло в нову еру, яку вже з упевненістю можна назвати мережевою. Відповідно до сучасного стану розвитку технологій з'являються і нові засоби ведення війни. Серед інших можна виділити також такі, що застосовуються у кіберпросторі. Засобами в даному аспекті є нові види озброєнь, що спираються на використання інформаційно-комп'ютерних технологій. Такі засоби за своєю природою значно відрізняються від загальноприйнятого розуміння терміну «зброя», проте, незважаючи на це, наслідки їх застосування можна порівняти з найбільш руйнівними з тих, що були раніше, та відомих загальному колу осіб видів озброєнь.

То що ж можна вважати кіберзброєю? Як і щодо багатьох сучасних термінів, які виникають у процесі відносин в інформаційно-комп'ютерних мережах, єдиного уніфікованого визначення наведеного поняття не запропоновано. Проте, спираючись на найбільш поширені визначення, можна виокремити його окремі ознаки.

В. Каберник наводить таке розуміння поняття «кіберзброя»: найрізноманітніші технічні та програмні засоби, найчастіше спрямовані на експлуатацію вразливостей у системах передачі та обробки інформації або програмо-технічних системах. Він також стверджує, що, спираючись на масштабність впливу, до кіберзброї відносять віруси типу Flame, або зомбі-мережі, які використовуються для розсилки спаму й організації розподілених атак, спрямованих на пе-

ревантаження інформаційних систем і похідну з неї відмову в обслуговуванні (так звані DOS і dDOS-атаки) [1].

Звертаючись до англомовних ресурсів, можна знайти й інші значення цього поняття. Так, наприклад, у словнику Макмілана надається досить коротке, проте містке визначення терміна кіберзброя: шкідливе програмне забезпечення, що використовується однією країною проти іншої для політичних, військових або розвідувальних цілей [2].

Оксфордський словник визначає кіберзброю як певну частину комп'ютерного програмного забезпечення або апаратного забезпечення, що використовується для ведення кібервійни [3].

С. Меле (Stefano Mele) наводить таке визначення кіберзброї: пристрій або будь-який набір комп'ютерних інструкцій, що спрямовані на незаконне пошкодження системи, яка функціонує як критична інфраструктура, її інформацію, дані або програми, що містяться в ній, або є відповідними до них, або навіть призначені для сприяння перериванню (повному або частковому) чи зміні у роботі такої системи[4].

Також можна прочитати й інше визначення Меле, яке наближає це поняття до міжнародно-правової площини. Він зазначає, що це частина обладнання, пристрою або будь-якого набору інструкцій для комп'ютерів, яка використовується у конфлікті між суб'єктами, як національними, так і не національними, з метою заподіяння (навіть непрямого) фізичного збитку обладнанню чи людям, а радше саботування чи безпосереднього пошкодження інформаційних систем чутливої цілі атакованого суб'єкта [5, с. 10].

Компанія Heimdal Security, що спеціалізується на програмних продуктах з кіберзахисту, надає таке визначення: термін «кіберзброя» означає просунутий і складний фрагмент коду, який можна використовувати для військових або розвідувальних цілей. Компанія стверджує, що термін нещодавно з'явився з військової галузі, щоб назвати шкідливе програмне забезпечення, яке можна використовувати для доступу до комп'ютерних мереж супротивника [6].

П. Паганіні визначає кіберзброю як певний комп'ютерний код, який використовується або призначений для використання з метою загрози або заподіяння фізичної, функціональної або психічної шкоди структурам, системам або живим істотам [7].

Тож, виходячи з наведених визначень, можна дійти висновку, що під кіберзброєю розуміється певне програмне забезпечення або сукупність програм, які створені або використовуються з метою завдання певної шкоди супротивнику. Проте чи можна, виходячи з подібних визначень, вважати кібернетичну зброю саме зброєю, а отже і сучасним засобом ведення війни. На нашу думку, варто все ж таки навести певні ознаки кіберзброї, що відрізнили б її від інших наявних комп'ютерних програм та систем, а також дали б змогу визначити її місце у системі озброєнь.

Для того, аби вважатися зброєю, кібернетичні засоби мають відповідати певній військовій тактичній або стратегічній меті, сюди ж, відповідно, варто віднести і заходи щодо шпигунства, крадіжки важливої військової інформації або саботажу. Як і більшість шкідливих комп'ютерних програм, що є у сучасному світі і переважно створюються хакерами з метою заволодіння коштами або персональною інформацією, програми військового типу теж націлені на втручання у певні комп'ютери, їх блоки або мережі. Проте ціллю тут має бути отримання певної військової переваги, як то встановлення контролю над деякими інформаційними передавачами, безпілотними апаратами, виведення з ладу комп'ютерної апаратури супротивника, знищення або заміна важливої тактичної інформації і таке інше.

Варто зазначити, що зовсім не будь-яка комп'ютерна програма, що створена з метою втручання в іншу інформаційно-комп'ютерну мережу, є саме зброєю. Це та ситуація, коли варто відрізняти поняття «знаряддя» від поняття «зброя». Кількість програм, які можна використати не за їх призначенням, а з метою заподіяння шкоди іншому суб'єктові,є значно більшою за кількість програм, які спеціально для цього написані. Так само, як, наприклад, вила можуть бути зброєю за певних обставин, проте це не робить цей побутовий сільськогосподарський предмет зброєю. Тому визначальною ознакою є те, що кіберзброєю варто вважати насамперед спеціально створену програму або код.

Наступною ознакою має бути той факт, що використання кіберзброї має залишатися невідомим та непомітним для того суб'єкта, проти систем якого вона направлена якомога довше. Інакше супротивник зможе підготуватися до такої атаки, шкідливий код буде виявлено і вивчено з метою попередження подальших втручань чи мінімізації наслідків уже вчиненого. Тож тривалість часу, протягом якого дія (навіть і підготовча, або така, що спрямована на зараження якомога більшої кількості пристроїв у інформаційно-комп'ютерній мережі супротивника) кіберзброї залишається непомітною, є визначальною для успішного її застосування,оскільки розробка все нових атакувальних кодів вимагає значних ресурсів.

Аби вважатися саме засобом, комп'ютерний код має бути створений з метою уразити визначену ціль (наприклад, перехоплення сигналу безпілотного апарата, зміна координат у приладах для учасників наземних чи морських операцій). Для цього необхідно мати розвідні дані або доступ до аналогічних засобів, що є в учасника кіберпротистояння. Ця ознака підтверджує той факт, що і для створення, і для подальшого впровадження кіберзброї необхідний значний ресурс, а також доступ до багатьох засекречених матеріалів, який здатні забезпечити лише державні органи. Тобто створення і використання кіберзброї – це завжди високоорганізована діяльність найвищого рівня.

Окремою ознакою кіберзброї є її точність, тобто здатність вражати наперед визначені об'єкти інфраструктури супротивника. Ця ознака є важливою і з точки зору МГП, оскільки дозволяє мінімізувати вплив на інші, насампе-

ред цивільні, об'єкти, тим самим зменшуючи чи взагалі уникаючи їх ушкодження.

Також виділяється така умовна ознака, як простота застосування. Цією ознакою визначається, наскільки значні мають бути витрати для застосування даного виду кіберзброї і чи принесуть вони співрозмірний витратам результат [4].

Звісно, також можна виділити значний перелік суто технічних особливостей та ознак, які б дали змогу визначати кіберзброю, проте це виходить за межі даного дослідження.

Варто зазначити, що навіть попри активне впровадження у національні системи державних органів структур, що займаються питаннями кібербезпеки та кібероборони, кіберзброя на сьогодні має переважно наступальний характер. У більшості держав ці структури знаходять своє місце серед інших військових відділень у рамках міністерств оборони. Це означає, що держави визнають рівень загроз, які містить у собі кіберпростір, що вірогідність застосування проти них новітніх видів озброєння, а саме кіберзброї, є цілком реальною. Але водночас натепер досі не існує спільної позиції міжнародного співтовариства щодо питань, які б визначили припустимість або межі використання кіберзброї. Хоча за своїми потенційними наслідками її можна віднести до зброї масового ураження.

На жаль, використання кіберзброї, власне як і загальноприйнятої конвенційної зброї, не може гарантувати ураження лише військових цілей і об'єктів. Більше того, цей новітній вид озброєння може використовуватися з метою тиску на супротивника, залякування, втручання у внутрішні справи держави. Історичні зразки атак з використанням інформаційно-комп'ютерних технологій вже підтвердили уразливу міць концентрованих кібератак [8]. Більше того, кіберзброя вже визнається летальною зброєю [9]. Це підштовхує нас до думки про те, що цей вид озброєння цілком може вважатися окремим засобом ведення війни, а також що на використання кіберозброєнь має і буде поширюватися дія міжнародного права.

Порівнюючи кіберзброю з ядерною, можна дійти висновку, що деякою мірою ці засоби є подібними. Перш за все, незважаючи на своє конвенційне закріплення, ядерна зброя не є забороненою. Відповідно, ця військова міць може використовуватися як певний засіб політичного тиску у відносинах між так званими «ядерними державами», а також у їхніх відносинах з без'ядерними, хоч це і суперечитиме Статуту ООН. Міжнародне співтовариство, підписавши декілька угод під егідою ООН, домовилося, передусім, про нерозповсюдження ядерної зброї[10]. Також багатьма країнами було підписано угоду, що заборонила випробування ядерної зброї у різних просторах [11].

Звісно, порівнювати потенційні руйнування від застосування ядерної зброї та руйнування від кібернетичної було б досить некоректно (лише тому, що від ядерної зброї шкода завдається комплексно), проте применшувати можливості кіберзагроз у XXI столітті теж не варто.

Так само доцільно було б згадати і хімічну зброю, яка теж завдає значних втрат, а також спричиняє важкі страждання у людини і, відповідно, діє на широкі маси населення і не вибірково. Досягненням міжнародного співтовариства стала спеціальна конвенція, що заборонила розробку такої зброї, а також сприяла її знищенню [12]. Також сюди можна додати і біологічну зброю, яка теж є забороненою [13].

В еру тотальної комп'ютеризації підприємств, виробництв, систем контролю на видобувних станціях, гідро- та атомних електростанціях, шахтах та багатьох інших об'єктах небезпека від використання кіберзброї зросла у рази. Будь-який з названих об'єктів може зазнати атаки з використанням інформаційно-комп'ютерних технологій. Наслідки знищення дамб (за рахунок віддаленого втручання у їх діяльність та виведення їх із ладу), зміни навігаційних даних для авіації та морського транспорту, штучного створення аварійних ситуацій на небезпечних виробництвах чи підприємствах хімічної галузі, на атомних електростанціях важко оцінити, проте зрозумілим є те, що такі втручання дозволяють поставити під загрозу життя навіть сотень тисяч людей, переважно цивільних. Варто зазначити, що спектр застосування кіберзброї є значно ширшим за наведені приклади.

Саме тому, на нашу думку, є допустимим порівняння кіберзброї зі зброєю масового ураження,оскільки натепер навіть важко точно вирахувати потенційну шкоду, яку за умов широкого використання може завдати кіберзброя. Це вкотре підтверджує, що з точки зору міжнародного права в цілому кібернетичні озброєння варто поставити в один ряд зусіманаявними забороненими міжнародним гуманітарним правом видами озброєнь і наголосити на тому, що даний вид озброєнь неможна використовувати за будь-яких умов та у будь-якому обсязі.

Якщо принцип дії вже заборонених міжнародним правом засобів ведення війни є зрозумілим, то щодо кіберзброї сьогодні ще існує багато питань. На нашу думку, варто виділити основні різновиди інформаційно-комп'ютерних технологій, що можуть бути застосовані у якості кіберзброї.

Насамперед види кіберозброєнь відрізняються залежно від задач, які постають перед тими, хто їх створює. Так, вони можуть бути націлені на викрадення, приховане відстежування або спотворення інформації. Також задачею можуть бути більш складні проникнення, що мають на меті перехоплення керування певними машинами супротивника, сукупністю комп'ютерів, що забезпечують діяльність чи комунікацію штабів або інших військових формувань. Також виділяють найбільш складні програми, які створені виключно з метою атаки на визначений об'єкт (як це було, наприклад, із вірусом Stuxnet). Відповідно до складності військової задачі формується і вартість підготовки кіберзброї.

Варто зазначити, що сьогодні, якщо розглядати потенційну ситуацію наявного конфлікту або підготування певного суб'єкта міжнародно-

го права до вчинення втручання до іншого (у кібернетичному чи іншому просторі), кіберзброя, все ж таки, буде використовуватися як допоміжний засіб ведення війни. Так, безумовним є те, що вона здатна порушити оборонні системи супротивника, вивести з ладу певну частину військової техніки, всіляко обмежити ворога, проте водночас найшвидше після такого кібернетичного нападу буде слідувати використання класичної зброї та військових систем.

Виділяючи кібезброю як окремий від уже усталених засіб ведення війни, варто виокремити, які саме серед наявних видів кіберзброї мають бути забороненими. Тож залежно від різних критеріїв можна виділити такі види кіберзброї: хакінг, віруси, трояни, шкідливе програмне забезпечення, логічні бомби, експлойти, генератори ключів, таргетовані атаки, використання дронів та автоматичної зброї. Деякі з них, як наслідок, можуть мати летальний характер, деякі спрямовані виключно проти техніки чи комп'ютерних систем супротивника, інші створені для отримання контролю над певною інформацією. Усі засоби ведення кібервійни також можуть бути поділені на 5 основних груп за технічним механізмом дії та особливістю застосування даного виду кіберзброї: мережева, проникаюча, попередньо встановлена, комунікаційна кіберзброя та електромагнітна зброя [14, с. 23-24].

Окремою особливістю застосування кіберзасобів є шпіонаж, що здійснюється за допомогою інформаційно-комп'ютерних технологій з метою отримання політичної, військової чи економічної переваги над супротивником. І за своїми масштабами натепер шпіонаж, мабуть, найбільш поширений вид діянь із використанням кіберзброї або інших кіберзасобів з метою вторгнення.

Не вдаючись до технічних особливостей кожного з перелічених видів кіберзброї, зазначимо, що забороненими серед них мають бути такі, що призводять до жертв, надмірних страждань чи пошкоджень цивільних фізичних об'єктів і при цьому не сприяють отриманню військової переваги. Так само мають бути заборонені такі засоби ведення кібервійни, які спрямовані на ураження невійськових об'єктів.

Звертаючись до міжнародного гуманітарного права, можна чітко визначити за аналогією, які засоби ведення кібервійни необхідно заборонити.

Аналізуючи Конвенцію про поліпшення долі поранених і хворих у діючих арміях, можна виокремити певні положення, які будуть поширюватися і на використання кіберзброї як засобу ведення кібервійни [15]. Названа конвенція зобов'язує учасників конфлікту «гуманно ставитися до осіб, які не беруть активної участі у воєнних діях», не заважати діяльності міжнародних гуманітарних організацій, дотримуватися прав поранених, хворих чи полонених осіб, не порушувати прав медичних чи духовних представників, що гарантовані конвенцією. Також сторони мають забезпечувати безпеку медичних установ, а тому, відповідно, не використовувати у том числі засоби ведення кібервійни проти них. Таке ж положення має бути застосованим і до культурних та історичних пам'яток. Конвенція також надає захист санітарному транспорту, а оскільки на сьогоднішньому етапі вже можливі ситуації застосування інформаційно-комп'ютерних технологій і на подібних машинах, літаках або морських суднах, то вони так само підпадають під заборону застосування до них кіберзброї. Це ж положення стосується і транспортних засобів міжнародних гуманітарних безсторонніх організацій.

Наступним визначним актом є Гаазька конвенція про закони та звичаї сухопутної війни 1907 року [16]. Користуючись положеннями конвенції, сторони, що знаходяться у стані конфлікту, можуть, по-перше, визначити, яке саме населення можна вважати цивільним, а яке – ні. Відповідно до цього визначаються і права, якими МГП наділяє ці обидві групи населення держави-сторони конфлікту. Окрім цього, ст. 23 Додатку до названої конвенції говорить про те, що сторони обмежені у виборі засобів ведення війни, а також вказується, що заборонено зрадницьки вбивати військове чи цивільне населення супротивника, використовувати зброю, що завдає надмірних страждань, знищувати об'єкти супротивника, окрім випадків, коли це зумовлено воєнною необхідністю, а також наводить заборонені методи, до яких ми звернемося у наступному підрозділі. Також конвенція наводить принципи, що забороняють атакувати незахищені міста чи поселення, спонукають до збереження історичних, культурних, духовних, наукових будівель та, звісно, медичних установ.

Більш сучасним не нормативним актом, в якому кіберзброя зазначається вже як засіб ведення війни, є Талліннський Посібник (Tallinn Manual on the International Law Applicable to Cyber Warfare). У ньому засобам та методам ведення війни присвячено окремий розділ. Зокрема, ним забороняється використовувати засоби та способи, що спричиняють зайві травми або непотрібні страждання [17, с. 119]. При цьому зазначається, що кіберзброя – це кібернетичні засоби ведення війни, які розроблені, використовуються, спрямовані на те, аби викликати травми або спричинити смерть особам, або завдати шкоду чи руйнування об'єктам, спричиняючи, у свою чергу, такі наслідки, щоб вважати кібероперацію атакою. Колектив авторів також підкреслює, що кіберінфраструктура, яка пов'язує комп'ютерну систему з ціллю, не є засобом, оскільки об'єкт має бути під контролем атакуючої сторони, щоб включати засоби ведення війни. Як і у звичаєвому гуманітарному праві, забороняється використовувати засоби та способи кібервійни, які за своїм характером є нерозбірливі. Засоби кібервійни будуть вважатися такими, коли вони не можуть бути: спрямовані на конкретну військову ціль або обмежені у їх впливі, як це передбачено правом збройних конфліктів. Тобто мають такий характер, що вони без будь-яких розбіжностей наносили б удари по військовим цілям та цивільним особам чи об'єктам. Таким чином, цей принцип обмежує сторону конфлікту у необачному чи неприцільному використанні засобів ведення

кібервійни, а відповідно, спонукає до ретельного виваження та направленого застосування кіберзброї лише у воєнних цілях. Посібник також наводить заборону на воєнні репресалії проти полонених, цивільних осіб, які знаходяться hors de combat, а також проти медичних працівників, установ, транспорту та обладнання, також забороняються атаки проти різноманітних цивільних об'єктів, об'єктів природнього середовища та критичної інфраструктури.

Варто також погодитися з наведеним у Посібнику твердженням, відповідно до якого держави зобов'язані оцінювати власні наявні засоби ведення кібервійни, а також приводити їх у відповідність до Додаткового Протоколу I до Женевських конвенцій 1949 року, а саме ст. 36, що стосується нових видів озброєнь [18].

Підготоване у 2017 році друге видання Талліннського Посібника (Tallinn Manual 2.0 ont he International Law Applicable to Cyber Operations) в цілому повторило вже наведені заборонені засоби ведення кібервійни [19].

Серед усіх обмежень засобів ведення війни також можна окремо приділити увагу тим, які стосуються навколишнього природнього середовища, оскільки, як вже зазначалося, безліч об'єктів, які здатні значно погіршити екологічну ситуацію, вже є частиною загальної інформаційно-комп'ютерної мережі, а тому стають потенційним об'єктом для вчинення кібератак. Так, ще 1976 року була підготовлена Конвенція про заборону воєнного або будь-якого іншого ворожого використання засобів впливу на природне середовище [20]. Таким чином, можна визначити додатковий принцип щодо заборони використання засобів ведення кібервійни, а саме вчинення таких атак на такі визначені об'єкти, що в подальшому становитимуть загрозу погіршення екологічної ситуації, зміни або знищення природних ресурсів, впливу на погодні умови чи клімат. Оскільки за певних обставин досягти таких наслідків можна, використовуючи лише або включно кіберзброю.

На наш погляд, також окремої заборони потребує посередництво третіх сторін у вчиненні кібератак, тобто надання державі, що має на меті здійснення кібератаки, у користування потужностей власних кібернетичних інфраструктур, що суперечило б наявним міжнародним нормам. Оскільки кіберсфера і так характеризується надвисоким ступенем складності визначення похідної точки вчинення кібератаки, то подібні дії сторонніх учасників конфлікту значно ускладнять процес атрибуції вчинених діянь державі чи то агресору, чи учаснику існуючого кіберконфлікту.

Тож, проаналізувавши основні документи міжнародного гуманітарного права, варто дійти висновку, що його норми відповідають сучасним викликам у зв'язку зі створенням нових видів озброєння. Залишається відкритим питання: чи варто державам прагнути до роззброєння і у новій кібернетичній сфері, адже руйнівні потужності кіберзброї значно вищі, ніж у багатьох відомих існуючих видів озброєнь. Оскільки Статутом ООН все ж таки передбачається насамперед мирний процес вирішення спорів, то, можливо, вже наближається час, коли ці новітні засоби будуть закріплені на міжнародному рівні нормативно [21]. Чи все ж таки, якщо відмовитися від новітніх озброєнь буде аж занадто складно, державам варто розпочинати заходи щодо зміцнення довіри [22, с. 11]? Бо, як стверджує І. Лукашук, завдання таких заходів полягає у попередженні погіршення відносин у результаті взаємного непорозуміння і подальше створення впевненості [23, с. 166]. Хоча ці питання переважно стосувалися питань роззброєння у світі, проте їх актуальність і в еру розвитку кібернетичних озброєнь применшувати не варто. Але, на жаль, нині ми бачимо тенденцію до збільшення можливостей держав не лише у питаннях кібероборони, а й у розвитку наступальних кіберзасобів.

Так, вже відомим є той факт, що військовослужбовці США використовували засоби ведення кібервійни під час операцій проти Ісламської держави, а також у 2011році під час операції у Лівії [24]. Кіберзброя використовувалася паралельно із класичними озброєннями і мала на меті переривати, порушувати процеси командування та управління ІДІЛ, змусити їх втратити довіру до своїх мереж, перевантажувати мережі так, щоб вони не змогли функціонувати, і докладати всіх зусиль, щоб терористи втратили здатність керувати та контролювати свої наявні сили [25].

Висновки

Отже, як висновок варто зазначити, що питання заборони використання засобів ведення кібервійни є надзвичайно актуальним і потребує всебічного вивчення та закріплення на міжнародному нормативному рівні. Держави світу входять у новий етап розвитку їхніх відносин, що буде характеризуватися збільшенням напруги в інформаційно-комп'ютерних мережах, де вони можуть і вже активно впроваджують свою зовнішню політику [26]. Оскільки прогрес дозволяє нам виокремлювати новий вид озброєнь, то міжнародне право має зробити все можливе задля дотримання ідей миру та безпеки, задля запобігання цивільним жертвам під час збройних конфліктів, де також використовується і кіберзброя, задля мінімізації негативного впливу кібернетичних озброєнь на цивільні об'єкти та природне середовище. Єдиним правильним шляхом є об'єднання зусиль і досягнення всебічного консенсусу з критичних питань, що регулюють відносини держав у кіберпросторі. Наукові пошуки з питань аналізу заборонених засобів ведення кібервійн у міжнародному інформаційному просторі мають бути продовжені.

Список використаних джерел:

1. Каберник В. В. Центр военно-политических исследований / В. В. Каберник // Кибервойна и кибероружие. [Электронный ресурс]. – Режим доступа: http://eurasian-defence.ru/?q=node/3115.

2. Macmillan Dictionary. [Electronic resource]. – Access mode : http://www.macmillandictionary.com/dictionary/british/cyber-weapon.

3. English Oxford Living Dictionaries. [Electronic resource]. – Access mode : https://en.oxforddictionaries.com/definition/cyberweapon.

4. Hackmageddon. Information Security Timelines and Statistics [Electronic resource]. – Access mode : http://www.hackmageddon.com/2012/04/22/what-is-a-cyber-weapon/.

5. Cyber-weapons: legal and strategic aspects Version 2.0. Observatory Infowarfare and Emerging Technologies / Stefano Mele. – Machiavelli Editions. –June 2013.

6. Heimdal Security. [Electronic resource]. – Access mode : https://heimdalsecurity.com/glossary/cyber-weapon.

7. Pierluigi Paganini. Cyber Weapons. – April 3, 2012. [Electronic resource]. – Access mode : http://securityaffairs.co/wordpress/3896/intelligence/cyber-weapons.html.

8. Камчатний М. В. Історія міжнародно-правового регулювання питань, пов'язаних із застосуванням комп'ютерних технологій / М. В. Камчатний // Проблеми законності. – 2016. – № 134. – С. 199–207.

9. Department of Defence Law of War Manual. Office of General Counsel Department of Defense, 2015. – WashingtonDC.

10. Договор о нераспространении ядерного оружия : одобрен резолюцией 2373 (XXII) Генеральной Ассамблеи от 12 июня 1968 года, [Электронный ресурс]. – Режим доступа: http://www.un.org/ru/documents/decl_conv/conventions/npt.shtml.

11. Договор о запрете испытаний ядерного оружия в атмосфере, в космическом пространстве и под водой. [Электронный ресурс]. – Режим доступа: http://www.un.org/ru/documents/decl_conv/conventions/pdf/nuclear_seabed.pdf.

12. Конвенция о запрещении разработки, производства, накопления и применения химического оружия и о его уничтожении. Принята в Париже 13 января 1993 года. [Электронный ресурс]. – Режим доступа: http://www.un.org/ru/documents/decl_conv/conventions/chemweapons.shtml.

13. Конвенция о запрещении разработки, производства и накопления бактериологического (биологического) оружия и токсинов и его уничтожении (Женева, 1972 г.) [Электронный ресурс]. – Режим доступа: http://www.un.org/ru/documents/decl_conv/conventions/bacweap.shtml.

14. Бабенко В. Г. Основні групи кіберзброї та особливості її застосування // Актуальні задачі та досягнення у галузі кібербезпеки, Матеріали Всеукраїнської науково-практичної конференції (23–25 листопада 2016 року, м. Кропивницький).

15. Конвенція про поліпшення долі поранених і хворих у діючих арміях [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/995_151/page.

16. Гаазька конвенція про закони та звичаї сухопутної війни 1907 року [Електронний ресурс]. – Режим доступу: https://www.icrc.org/rus/resources/documents/misc/hague-convention-iv-181007.htm.

17. Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare // Cambridge University Press.

18. Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооружённых конфликтов [Электронный ресурс]. – Режим доступа: https://www.icrc.org/rus/assets/files/2013/ap_i_rus.pdf.

19. Michael N. Schmitt, Liis Vihul. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. – Cambridge University Press, 2017.

20. Конвенция о запрещении военного или любого иного враждебного использования средств воздействия на природную среду. [Электронный ресурс]. – Режим доступа: http://www.un.org/ru/documents/decl_conv/conventions/hostenv.shtml.

21. Charter of the United Nations and Statute of the International Court of Justice. San Francisco – 1945. [Electronic resource]. – Access mode : https://treaties.un.org/doc/publication/ctc/uncharter.pdf.

22. Заключительный акт СБСЕ, Хельсинки 1975. [Электронный ресурс]. – Режим доступа: https://www.osce.org/ru/mc/39505?download=true.

23. Лукашук И. И. Международное право. Особенная часть / И. И. Лукашук. – Москва, Вольтерс Клувер, 2005.

24. Nakashima, E. (2011). "U.S. Cyberweapons Had Been Considered to Disrupt Gaddafi's Air Defenses". The Washington Post (October 17, 2001). [Electronic resource]. – Access mode : http://articles.washingtonpost.com/2011-10-17/world/35276890_1_cyberattack-air-defenses-operation-odyssey-dawn.

25. Department of Defense Press Briefing by Secretary Carter and Gen. Dunford in the Pentagon Briefing Room. Feb. 29, 2016. [Electronic resource]. – Access mode : https://www.defense.gov/News/Transcripts/Transcript-View/Article/682341/department-of-defense-press-briefing-by-secretary-carter-and-gen-dunford-in-the/.

26. ABC. Margot O'Neill, Lateline Examines the Future of Cyber Warfare. 2015. [Electronic resource]. – Access mode : http://www.abc.net.au/lateline/content/2015/s4350126.htm.

Статья посвящена исследованию запрещенных средств ведения кибервойн субъектами международного права. В статье исследованы существующие понятия кибероружия как средства ведения войны, выделены основные характерные признаки данного вида вооружений. Рассмотрены основные подходы к формированию новых ограничительных подходов относительно запрета использования кибероружия. Автор впервые в украинской доктрине анализирует вопрос выделения нового средства ведения войны, сравнивает существующие виды вооружений с новым –кибероружием.

Ключевые слова: кибервойна, кибероружие, международное гуманитарное право, право вооруженных конфликтов, киберпространство, кибератака, международная информационная безопасность.

The article is devoted to the investigation of prohibited means of conducting cyberwar by subjects of international law. The article explores the existing concepts of cyber weapons as a means of warfare, identifies the main characteristics of this type of weapons. The main approaches to the formation of new restrictive approaches regarding the prohibition of the use of cyber weapons are examined. For the first time in the Ukrainian doctrine the author analyzes the issue of allocating a new means of warfare, compares existing types of weapons with the new type – cyber weapons.

Key words: cyberwar, cyber weapon, international humanitarian law, the law of armed conflicts, cyberspace, cyberattack, international information security.