Victoria Roller, Spartak Gogonyants & Igor Koropatnik (2019) Pravove pidgruntya zdiysnennya kiberoborony v Ukrayini [Legal background of cyber defence in Ukraine]. *Social development & Security. 9(4)*, 74 – 86. DOI: http://doi.org/10.33445/sds.2019.9.4.5

Правове підґрунтя здійснення кібероборони в Україні

Вікторія Роллер *, Спартак Гогонянц **, Ігор Коропатнік ***

** Військовий інститут Київського національного університету імені Тараса Шевченка,*
вул. Ломоносова, 81, м. Київ, 03022, Україна,
e-mail: rollervika@gmail.com,
ад'юнкт науково-організаційного відділення.

*** Національний університет оборони України імені Івана Черняховського,*
проспект Повітрофлотський, 28, м. Київ, 03049, Україна,
e-mail: hohoniants@gmail.com,
к.т.н., с.н.с.

**** Військовий інститут Київського національного університету імені Тараса Шевченка,*
вул. Ломоносова, 81, м. Київ, 03022, Україна,
e-mail: korvelll@ukr.net,
д.ю.н., доцент.

Article history:
Received: June, 2019
1st Revision: July, 2019
Accepted: August, 2019

УДК 340.13/ 342.9+ 355/359

Анотація: Сучасний світ вже не перший рік говорить про можливість ведення бойових дій у кіберпросторі. Це сталося після 2010 року, коли на прикладі Ірану світ побачив що шкідливе програмне забезпечення може здійснити суттєвий вплив на дійсність та зупинити процеси, що відбуваються у реальному світі. Наразі навіть розроблено регулювання щодо того, яким чином ці кіберпротистояння мають відбуватися та за якими правилами здійснюватися (маються на увазі теоретичні розробки які закладені у першому та другому Талліннських керівництвах).

В Україні процес нормативно- правового регулювання саме питання забезпечення кібербезпеки держави почався достатньо пізно – у 2015 році, коли була прийнята Стратегія забезпечення кібербезпеки України. Розвиток питань врегульованих цією Стратегією відбувся ще у кількох законах та інших нормативно- правових актах. Але, на жаль, існуюче нормативно правове регулювання не дає відповіді на дуже багато питань, з якими українське суспільство може зіштовхнутися у сферу панування інформаційних технологій та інтернету речей.

З 2014 року Україна перебуває у стані збройного конфлікту з агресором- Російською Федерацією. За ці роки українське військо навчилося стійко обороняти кордони та стримувати натиск агресора, але існує нове, ще незвідане поле бою – кіберпростір. У зв'язку з цим, питання порядку надання відсічі будь якому агресору у кіберпросторі є актуальними та такими, які вимагають вивчення.

У статті буде розглянуто основні положення нормативно - правового регулювання здійснення кібероборони в Україні, та теоретичний порядок проведення дій з кібероборони. Визначено основні проблемні питання законодавчого регулювання, які перешкоджають оперативно та коректно здійснювати відповідь на кібератаки проти України.

Ключові слова: кіберзахист, кібероборона, оборона України, агресія у кіберпросторі.

1. Формулювання проблеми

Якщо звернутися до стану теоретичної розробленості проблеми правового регулювання здійснення кібернетичних операцій, чи інших дій у сфері кіберпростору та їх нормативного регулювання в Україні, то можливо зробити висновок, що він на крайнє низькому рівні. Законодавство України у цій сфері фрагментарне, суперечливе та не відповідає вимогам сучасності, що фактично зводить обороноздатність України у кіберпросторі до нуля. Нормативно-правове регулювання яке існує на даний момент не враховує те, що кібератаки хоч і готуються тривалий час, але можуть відбуваються швидкоплинно, а механізми здійснення відсічі збройній агресії вимагає прийняття низки швидких управлінських рішень та обмеженого часу на їх виконання.

За різними джерелами протягом 2014-2017 років на Україну було здійснено близько 14 значних кібератак, що могли вплинути на українське суспільство та економіку [1].

1.2 Аналіз останніх досліджень та публікацій

Аналіз останніх досліджень та публікацій. Дослідженнями питань інформаційної безпеки займаються такі науковці як М.В. Арсент'єва, В.Ю. Артемов, І.В. Арістова, Є.П. Бабалик, О. М. Бандурка, О.А. Баранов, О. І. Безпалова, В.М. Брижко, А. Л. Деньщиков, Т.Г. Затонацька, Р.А. Калюжний, А. Т. Комзюк, О.П, Кучмій, В.А. Ліпкан, О.В. Логінов, Є.Д. Лук'янчиков, О. М. Музичук, В.О. Невядовський, Н.Р. Нижник. Але в той же час, питання кіберзахисту чи кібероборони наразі досліджені не достатньо. У 2018 році захищено два дисертаційних дослідження на теми: "Адміністративно-правове регулювання кібербезпеки України" Діордіци І.В. та "Інформаційна безпека у Збройних Силах України" Буги Л.В., але хоча ці дослідження і є новими, але питання здійснення кібероборони у них не розкриваються.

1.3. Постановка завдання

Україна вже п'ятий рік веде боротьбу з агресором – Російською Федерацією. За цей час противником було застосовано різні види зброї та методи ведення війни, та методи "гібридної війни". З розвитком інформаційних технологій з'явилося нове поле проведення військових операцій – кіберпростір. Українське законодавство, яке регулює здійснення дій у кіберпросторі ще досі "молоде" та не дає відповідей щодо здійснення правовідносин у цій сфері.

Мета статті є дослідження та аналіз існуючого нормативно-правового регулювання.

2. Виклад основного матеріалу

Експерти пов'язують активність щодо проведення кібератак на Україну як з вирішенням геополітичних питань між державами світу, так і як складову

інформаційної війни Росії проти України. Кеннет Гірс спеціальний представник, NATO Cooperative Cyber Defence Centre of Excellence у інтервью ВВС Україна так коментує ситуацію з кібератаками в Україні: “Україна перебуває у дуже активному геополітичному просторі. Через те, що міжнародний конфлікт триває, будуть нові атаки, пов’язані із ключовими подіями. Так відбувається завжди. Наприклад, на Близькому Сході, як тільки посилювалося протистояння у Лівані чи секторі Гази, у Сирії, те, що відбувалося у реальному просторі, обов'язково мало відлуння і у кібер-просторі. Так само і зараз в Україні” [2].

Крім того, достатньо поширеними в Україні є інші дії, заборонені законодавством які здійснюються посередництвом використання інтернет технологій, а саме, кіберзлочинність: шахрайство, крадіжки даних та інше. Ці злочини також існують у реаліях українського суспільства, та спричиняють немало негативних наслідків для громадян України та держави загалом, але не відносяться до питання, яке розглядається у даній статті.

Приступаючи до проведення аналізу основного питання – здійснення кібероборони, необхідно детально розглянути, що у військовій справі є оборонні дії, та їх втілення- оборонний бій.

Звертаючись до теорії військової підготовки перейдемо до з’ясування що у військовій справі вважається оборонним боєм: оборона – один із видів загальновійськового бою. На початку війни оборона є найважливішим і найбільш поширеним видом бою. Оборона має на меті: відбити наступ переважаючих сил противника; завдати йому максимальних втрат; економити сили і час; утримати важливі райони (об’єкти) місцевості й тим самим створити умови для переходу в наступ.

Мета оборони досягається:

постійною розвідкою противника, своєчасним розкриттям підготовки його наступу та замислу дій;

знищенням (подавленням) засобів ураження противника, особливо його артилерії, танків, БМП, а також наземних елементів систем високоточної зброї;

своєчасним маневром, силами й засобами з неатакованих ділянок, стійким утриманням позицій та районів, проведенням рішучих контратак, нав’язуванням противнику своєї волі, створенням для нього невигідних умов бою та інше [3].

Звичайно ж ці положення застосовують для проведення оборонного бою механізованого взводу. Але, говорячи про заходи кібероборони, необхідно провести інтерпретування оборонного бою для кіберпростору. Цих положень достатньо, щоб визначити, що оборонний бій, передбачає завдання ударів у відповідь, завдання шкоди противнику та виведення його сил та засобів з ладу. Це питання є вкрай важливим, тому що якщо переносити ці правила на кіберпростір, то вбачається, що завданнями кібероборони є не тільки відбиття атаки на українські інформаційні ресурси та інші об’єкти, але і завдання супротивнику ушкодження для попередження наступних атак на Україну. Також важливим питанням є питання того, що вносячи в законодавство України термін “кібероборона” нормотворець не мав на увазі самооборону.

Крім того, якщо розглянути світову юридичну практику щодо розгляду операцій у кіберпросторі, то наявність Таллінських керівництв (Tallin Manual

1.0,2.0 on the International Law Applicable to Cyber Operations) з застосування міжнародного гумнітарного права до кібероперацій, та те, що ці керівництва були видані під егідою Центру кіберзахисту НАТО (NATO Cooperative Cyber Defence Centre of Excellence), не викликає сумніву, що світова спільнота та найбільш військово розвинені країни світу розглядають кібератаки, як такі, що можуть бути прирівняні до атаки у загальному її розумінні, а отже як такі, що вимагають дій у відповідь.

Тому вважаємо за необхідне проведення аналізу норм українського законодавства, щодо питання з'ясування походження кібератаки (саме пов'язаність з державою) адекватного реагування на кібератаки проти України та дії, які можуть бути вчинені уповноваженими особами щодо відбиття кібератаки.

Здійснення оборони загалом, та кібероборони зокрема регулюється низкою нормативно правових актів, таких як Закон України "Про оборону України", Закон України "Про основні засади забезпечення кібербезпеки України", Стратегія кібербезпеки України та іншими нормативно-правовими актами. Законом України "Про оборону України" закріплено визначення оборони України, як системи політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших заходів держави щодо підготовки до збройного захисту та її захист у разі збройної агресії або збройного конфлікту [4]. Цим же законом визначено що є збройна агресія, а саме застосування іншою державою або групою держав збройної сили проти України. Проводячи подальший аналіз цієї норми необхідно визначити, що законодавець визначає як збройну агресію (тобто застосування збройної сили). Закон України "Про оборону України" до збройної агресії проти України відносить будь-яку з таких дій:

вторгнення або напад збройних сил іншої держави або групи держав на територію України, а також окупація або анексія частини території України;

блокада портів, узбережжя або повітряного простору, порушення комунікацій України збройними силами іншої держави або групи держав;

напад збройних сил іншої держави або групи держав на військові сухопутні, морські чи повітряні сили або цивільні морські чи повітряні флоти України;

засилання іншою державою або від її імені озброєних груп регулярних або нерегулярних сил, що вчиняють акти застосування збройної сили проти України, які мають настільки серйозний характер, що це рівнозначно переліченим в абзацах п'ятому – сьомому цієї статті діям, у тому числі значна участь третьої держави у таких діях;

дії іншої держави (держав), яка дозволяє, щоб її територія, яку вона надала в розпорядження третьої держави, використовувалася цією третьою державою (державами) для вчинення дій, зазначених в абзацах п'ятому – восьмому цієї статті;

застосування підрозділів збройних сил іншої держави або групи держав, які перебувають на території України відповідно до укладених з Україною міжнародних договорів, проти третьої держави або групи держав, інше порушення умов, передбачених такими договорами, або продовження

перебування цих підрозділів на території України після припинення дії зазначених договорів [4].

До цьому переліку дій іншої держави відносно України які відносять до збройної агресії, кібератаку можливо віднести лише опосередковано. Тобто, українським законодавством кібератака напряму не визначена збройною агресією.

Продовжуючи подальший аналіз норм українського законодавства звертаємося до Закону України "Про основні засади забезпечення кібербезпеки України" і вважаємо за необхідне зазначити, що у цьому законі наведено визначення кібероборони як сукупності політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії [5].

Знов звертаючись до Закону України "Про оборону України" наголошуємо, що кібератака (жодної сили та наслідків) прямо не віднесена до збройної агресії проти України. Законом України "Про основні засади забезпечення кібероборони України" кібератака визначається як спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

На нашу думку не можна ігнорувати думку про те, що кібератака здійснена іншою державою чи за її сприяння може мати таку силу та такі наслідки, які б можливо було порівняти зі збройним нападом. Також важливим фактором звернення посиленої уваги на до цього питання є те, що країни світу активно розробляють власні концепції кібербезпеки та навіть створюють власні кібервійська у складі збройних сил.

При здійсненні теоретичного аналізу вищезазначених питань, слушним, на нашу думку, є розгляд понять, які визначені О.О. Черногором, Є.О. Живилом, В.В. Маштарілом, у розрізі розгляду питання затвердження Стратегії кібербезпеки України у 2015 році, які є важливими у сфері конфліктів у кіберпросторі, а саме:

воєнний кіберконфлікт – форма розв'язання міждержавних або внутрішньодержавних суперечностей із двостороннім застосуванням у кіберпросторі воєнної сили; основними видами воєнних конфліктів є кібервійна та збройний кіберконфлікт;

кібервійна – протиборство непримиренних держав (регіонів) у кіберпросторі із застосуванням воєнної сили для досягнення воєнно-політичних цілей, що зачіпають інтереси цих держав (регіонів) [7]. Таким чином, бажання практиків та науковців сформулювати основоположні поняття у сфері регулювання конфліктів у кіберпросторі говорить про актуальність цього питання, та необхідність проведення регулювання цього питання, для уникнення ситуацій відсутності правового регулювання дій військовослужбовців у разі вчинення кібератаки на Україну.

Ці поняття наразі не закріплені в українському законодавстві, але на нашу думку хоча б теоретично необхідно окреслювати ці поняття, оскільки вони дозволяють провести відмежування звичайної кібератаки та кібератаки, яку необхідно розцінювати як акт агресії. На практиці застосування військ та сил момент надання відповіді на кібератаку є надзвичайно важливим та вимагає чіткого законодавчого регулювання.

Розвиваючи думку про те, що країни світу створюють власні кіберпідрозділи, необхідно розглянути те правове підґрунтя, яке вони використовують. Першочергово необхідно звернутися до Резолюції Генеральної асамблеї ООН, яка дає визначення Агресії [8]: “Агрессией является применение вооруженной силы государством против суверенитета, территориальной неприкосновенности или политической независимости другого государства, или каким-либо другим образом, несовместимым с Уставом Организации Объединенных Наций, как это установлено в настоящем определении”.

Влучної позиції дотримується Афродіта Папанастосі, яка звертається до думки, що враховуючи, що контекст визначення статті 2 (4) Статуту Організації Об'єднаних Націй не може бути використаний для класифікації кібератак між державами, необхідно провести аналіз поняття «агресії». Чи може кібератака розглядатись як четверта міжнародна злочинність, що підпадає під юрисдикцію Міжнародного кримінального суду, піднімаючи індивідуальну кримінальну відповідальність глави держави, за умови встановлення необхідного зв'язку з хакером- або групою хакерів? Відповідна література на цю тему намагалася зрівняти кібернапади з актами агресії, використовуючи в якості початкового пункту Консенсусне визначення агресії, прийняте Генеральною Асамблеєю ООН у Резолюції 3314 (XXIX) у 1974 році. У спробі класифікувати кібератаки під нововизначеним злочином агресії, труднощів завдає термін «збройні сили». Чи можна вважати кібер-війну «зброєю» відповідно до традиційного значення? Міжнародне право не дає конкретного визначення зброї. Оксфордський словник визначає озброєння як «зброю», яке, у свою чергу, визначається як «інструменти або засоби, призначені або використані для нанесення тілесних ушкоджень або фізичного пошкодження». Таким чином, кібер-війна безумовно потрапляє в рамки цього визначення. Проте, якщо звернутися до практики держав на глобальному рівні, буде очевидно, що кібер-сили починають становити окрему гілку кожної армії технологічно розвинених держав. Таким чином, якщо визнати, що кібер-сила може бути частиною збройних сил держави, кібератаки дуже легко потрапляють під юридичні рамки актів (a), (b), (c), (d) і (e) агресії, як зазначено вище. Що стосується (g), то кібератаки здійснюються хакерами, які можна

вважати “найманцями”, припускаючи, що держава наймає їх для проведення цільових кібер-атак. Отже, операції з кібер-війни можуть потенційно відповідати визначенню злочину агресії, як це передбачено у статті 8 bis [9].

Якщо дотримуватися такої логіки, то країни своєю фактичною поведінкою (а саме створення кіберпідрозділів у складі збройних сил) відносять кібератаки до актів агресії. Це теоретичне питання хвилює науковців не тільки в Україні, так і у всьому світі, оскільки наразі зі створенням цілих кібер підрозділів у арміях країн світу питання щодо моменту початку здійснення кібероборони для відбиття кібератаки саме як акту агресії залишається невирішеним.

Продовжуючи дослідження щодо здійснення кібероборони далі можемо зазначити, що Відповідно до Стратегії Кібербезпеки України на Міністерство оборони України та Генеральний штаб відповідно до компетенції покладено функції – здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснення військової співпраці з НАТО, пов’язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз; забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахисту власної інформаційної інфраструктури [10].

Закон України “Про основні засади забезпечення кібербезпеки України” у пункті 4 статті 8 таким чином визначає їх повноваження: “Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб’єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану”.

В той же час, в Указі Президента України “Про Положення про Міністерство оборони України” [11] не визначено завдань чи повноважень у сфері кібероборони. Повноваження у сфері забезпечення безпеки інформаційного простору та середовища визначено у пунктах 5, 8, 43-45 статті 4 вищезазначеного Указу, де визначено: “Міністерство оборони України проводить розвідувальну та інформаційно-аналітичну діяльність в інтересах національної безпеки та оборони держави; здійснює постійний моніторинг інформаційного середовища, виявляє потенційні та реальні інформаційні загрози в оборонній сфері, проводить попереджувальні інформаційні заходи; забезпечує розвиток інформаційної інфраструктури та ресурсів, впровадження новітніх інформаційних технологій у сфері оборони; провадить діяльність із технічного захисту інформації для потреб Міноборони України;” Інших повноважень у цій сфері для Міністерства оборони України не визначено. Таким чином, Положення про Міністерство оборони України не регулює питання здійснення Міністерством оборони України повноважень у сфері здійснення кібероборони України”

Щодо Генерального штабу Збройних Сил України, то в Указі Президента України “Про Положення про Генеральний штаб Збройних Сил України” [12]

визначено такі повноваження Генерального штабу Збройних Сил України у сфері дослідження:

бере участь в організації використання повітряного, водного, інформаційного простору держави;

організовує в межах компетенції відкритий, спеціальний, фельд'єгерський зв'язок, забезпечує у Міністерстві оборони та Збройних Силах здійснення заходів з організації моніторингу та оцінки захищеності інформації, захисту інформації та кібербезпеки в інформаційно-телекомунікаційних системах;

організовує і здійснює комплекс заходів щодо забезпечення охорони державної таємниці, криптографічного та технічного захисту інформації, протидії технічним розвідкам, захисту іншої інформації з обмеженим доступом у Збройних Силах, надання електронних довірчих послуг у Збройних Силах;

організовує та здійснює контроль за станом охорони державної таємниці, захисту іншої інформації з обмеженим доступом, криптографічного та технічного захисту інформації, протидії технічним розвідкам, аудиту інформаційної безпеки у Збройних Силах;

бере участь у взаємодії з Державною службою спеціального зв'язку та захисту інформації України у здійсненні заходів щодо підготовки і застосування (використання) інформаційних систем загального доступу, телекомунікаційної мережі загального користування та загальнодержавних систем спеціального зв'язку до використання в інтересах оборони;

бере участь у створенні національної системи кібербезпеки та проведенні її періодичного огляду;

організовує планування та виконання в межах компетенції заходів з підготовки держави до відбиття воєнної агресії в кіберпросторі (кібероборони), координує виконання завдань з підготовки до кібероборони органами виконавчої влади, органами місцевого самоврядування та іншими складовими сил оборони;

організовує планування кібернетичних операцій Збройних Сил та інших складових сил оборони;

забезпечує у взаємодії з Державною службою спеціального зв'язку та захисту інформації України та Службою безпеки України кіберзахист інформаційної інфраструктури Міністерства оборони і Збройних Сил;

здійснює забезпечення інформаційної безпеки у Збройних Силах та протидію системним і масштабним діям проти інтересів України в кіберпросторі іноземними державами (групами держав), зокрема із залученням кібер підрозділів збройних сил іноземних держав, шляхом використання спеціальних засобів (кібер озброєнь);

Додатково статтею 5 вищезазначеного Положення визначено що: "Генеральний штаб для виконання покладених на нього завдань має право в установленому порядку: залучати до проведення навчань щодо реагування на кібератаки та кіберінциденти за погодженням із керівниками представників органів державної влади та органів місцевого самоврядування, інших складових сил оборони;"

Таким чином, Положення про Генеральний штаб Збройних Сил України визначає основоположні завдання Генерального штабу ЗСУ не тільки у сфері

забезпечення кібербезпеки, але і здійснення повноважень щодо проведення дій кібероборони. Ці твердження є основоположними, такими, що не розкривають конкретного порядку здійснення цих заходів, але закріплюються повноваження Генерального штабу Збройних Сил України на виконання цих заходів.

Законодавчо передбачено такий порядок здійснення Відсічі збройній агресії проти України. У відповідності до Закону України "Про оборону України": "У разі збройної агресії проти України або загрози нападу на Україну Президент України приймає рішення про загальну або часткову мобілізацію, введення воєнного стану в Україні або окремих її місцевостях, застосування Збройних Сил України, інших військових формувань, утворених відповідно до законів України, подає його Верховній Раді України на схвалення чи затвердження, а також вносить до Верховної Ради України подання про оголошення стану війни.

Органи державної влади та органи військового управління, не чекаючи оголошення стану війни, вживають заходів для відсічі агресії. На підставі відповідного рішення Президента України Збройні Сили України разом з іншими військовими формуваннями розпочинають воєнні дії, у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі [12].

3. Висновки і перспективи подальших досліджень

Таким чином, підсумовуючи викладений матеріал можемо зробити такі важливі висновки:

1. Орієнтуючись на світову практику та положення зазначені у законодавстві України кібератаки можна віднести до актів агресії, хоча прямого посилання на кібератаку як акт агресії положення українського законодавства не містять. При цьому законодавством також не встановлено якої сили та наслідків має бути кібератака щоб бути віднесеною до акту агресії. У цьому випадку логічно використовувати аналогію права щодо міжнародних норм стосовно кібератак та практики теоретичного дослідження цього питання до появи нормативно- правового регулювання цього питання в Україні.

2. Законодавство України встановлює повноваження Міністерства оборони України та Генерального штабу Збройних Сил України щодо здійснення кібероборони України. При цьому у відповідних актах що регулюють діяльність цих органів таким чином врегульовано їх повноваження: Указ Президента України "Про Положення про Міністерство оборони України" [11] ні серед завдань, ні повноважень Міністерства оборони України не визначає завдань чи повноважень у сфері кібероборони. Повноваження у сфері забезпечення безпеки інформаційного простору та середовища визначено у пунктах 5, 8, 43-45 статті 4 зазначеного Указу. Щодо Генерального штабу Збройних Сил України, то в Указі Президента України "Про Положення про Генеральний штаб Збройних Сил України" [12] визначено такі основні повноваження Генерального штабу Збройних Сил України у сфері кібероборони: здійснює забезпечення інформаційної безпеки у Збройних Силах та протидію системним і масштабним діям проти інтересів України в кіберпросторі іноземними державами (групами

держав), зокрема із залученням кібер підрозділів збройних сил іноземних держав, шляхом використання спеціальних засобів (кібер озброєнь); Таким чином, у разі здійснення кібератаки на Україну яку необхідно розцінювати як агресію, Генеральний штаб Збройних Сил України має повноваження щодо організації оборони України у кіберпросторі.

3. Порядок здійснення оборони України визначений на даний момент не завжди може бути достатньо ефективним для початку оборонних дій під час кібератаки, оскільки потребує певного часу на реалізацію, в той час як кібератаки можуть відбуватися швидкоплинно. У такому випадку до оголошення стану війни підрозділи що здійснюють кібероборону можуть проводити заходи щодо відсічі агресії, які більш схожі на самозахист.

Author details (in Russian)

Правовая основа осуществления кибероборонь в Украине

Виктория Роллер *, Спартак Гогонянц **, Игорь Коропатник ***

** Военный институт Киевского национального университета имени Тараса Шевченко,*
ул. Ломоносова, 81, г. Киев, 03022, Украина,
e-mail: rollervika@gmail.com,
адъюнкт научно-организационного отделения.

*** Национальный университет обороны Украины имени Ивана Черняховского,*
Воздухофлотский проспект, 28, г. Киев, 03049, Украина,
e-mail: hohoniants@gmail.com,
к.т.н., с.н.с.

**** Военный институт Киевского национального университета имени Тараса Шевченко,*
ул. Ломоносова, 81, г. Киев, 03022, Украина,
e-mail: korvelll@ukr.net,
д.ю.н., доцент.

Аннотация: Современный мир уже не первый год говорит о возможности ведения боевых действий в киберпространстве. Это произошло после 2010 года, когда на примере Ирана мир увидел, как вредоносное программное обеспечение может осуществить существенное влияние на действительность и остановить процессы, происходящие в реальном мире. Сейчас даже разработаны регулирования относительно того, каким образом эти киберпротивостояння должны проходить и по каким правилам осуществляться (имеются в виду теоретические разработки заложенных в первом и втором Таллиннской руководствах).

В Украине процесс нормативно-правового регулирования именно вопроса обеспечения кибербезопасности государства начался достаточно поздно – в 2015 году, когда была принята Стратегия обеспечения кибербезопасности Украины. Развитие вопросов урегулированных этой Стратегией состоялся еще в нескольких законах и других нормативно-правовых актах. Но, к сожалению, существующее нормативно правовое регулирование не дает ответа на очень многие вопросы, с которыми украинское общество может столкнуться в сферу господства информационных технологий и интернета вещей.

С 2014 года Украина находится в состоянии вооруженного конфликта с агрессором-Российской Федерацией. За эти годы украинское войско научилось устойчиво защищать границы и сдерживать натиск агрессора, но существует новое, еще неизведанное поле боя-

киберпространство. В связи с этим, вопрос порядка предоставления отпора любому агрессору в киберпространстве актуальны и такие, которые требуют изучения.

В статье будут рассмотрены основные положения нормативно-правового регулирования осуществления кибероборонь в Украине, и теоретический порядок проведения действий кибероборонь. Определены основные проблемные вопросы законодательного регулирования, которые препятствуют оперативно и корректно осуществлять ответ на кибератаки против Украины.

Ключевые слова: киберзащита, кибероборона, оборона Украины, агрессия в киберпространстве.

Author details (in English)

Legal background of cyber defence in Ukraine

Victoria Roller *, Spartak Gogonyants **, Igor Koropatnik ***

** Military Institute of Taras Shevchenko National University of Kyiv,*
81, Lomonosov str., Kyiv, 03022, Ukraine,
e-mail: rollervika@gmail.com,
Post-graduate.

*** The National Defense University of Ukraine named after Ivan Cherniakhovskyi,*
28, Povitroflotsky av, Kyiv, 03049, Ukraine,
e-mail: hohoniants@gmail.com,
Candidate of Military Science (PhD), Senior Researcher,
Chief of Scientific Research Department.

**** Military Institute of Taras Shevchenko National University of Kyiv,*
81, Lomonosov st., Kyiv, 03022, Ukraine,
e-mail: korvelll@ukr.net,
Dr. of Science, Associate Professor.

Abstract: The modern world is not the first year talking about the possibility of conducting hostilities in cyberspace. This happened after 2010, when on the example of Iran the world saw that malicious software could have a significant impact on reality and stop the processes taking place in the real world. At the moment, even regulation has been developed on how these cyber confrontations are to take place and on what rules to take place (the theoretical developments laid out in the first and second Tallinn Manuals are meant).

In Ukraine, the process of legal regulation of securing the cybersecurity of the country is precisely the issue, which began to explore quite late in 2015, when the Strategy for the Cybersecurity of Ukraine was adopted. The development of issues regulated by this Strategy has been carried out in several laws and other normative legal acts. But, unfortunately, the existing legal regulation does not answer many questions that Ukrainian society may face in the sphere of the dominance of information technology and the Internet of things.

From 2014, Ukraine is in a state of armed conflict with an aggressor-the Russian Federation. Over the years, the Ukrainian army has learned to stably defend the borders and restrain the aggressor's attack, but there is a new, yet unknown battlefield - cyberspace. In this regard, the question of how to resist any aggressor in the cyberspace is relevant and required to be studied.

The article will discuss the main provisions of the normative and legal regulation of the implementation of the cyber defense in Ukraine, and the theoretical procedure for carrying out actions on the cyber defense. The main issues of legislative regulation are identified, which hinder the prompt and correct implementation of the response to cyber attacks against Ukraine.

Keywords: cyber protection, cyber defense, defense of Ukraine, aggression in cyberspace.

Використана література

1. Найбільші кібератаки проти України з 2014 року/Інфографіка від 08 липня 2017 року/ Журнал "Новое время". URL: https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html
2. Маленькі зелені байти атакуватимуть частіше – експерти з кібероборони/Анастасія Зануда/ BBC Україна/ 30 січня 2017. URL: https://www.bbc.com/ukrainian/features-38758423
3. Тактична підготовка артилерійських підрозділів: підручник / П. Є. Трофименко, Ю. І. Пушкарьов, С. П. Латін та ін. – Суми: Сумський державний університет, 2012. – 776 с. URL: https://buklib.net/books/37546/
4. Закон України "Про оборону України" від 06.12.1991 № 1932-XII/ Редакція від 04.11.2018. URL: https://zakon.rada.gov.ua/laws/show/1932-12
5. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 №2163-VIII; Редакція від 08.07.2018. URL: https://zakon.rada.gov.ua/laws/show/2163-19
6. День, когда загадочная кибератака парализовала Украину/Кристиан Борис/ BBC Future/ 6 липня 2017. URL: https://www.bbc.com/ukrainian/vert-fut-russian-40509165
7. Черноног О.О., Живило Є. О., Машталір В. В. Стратегія забезпечення кібернетичної безпеки Збройних Сил України; Інтерактивний дискурс у контексті інформаційної безпеки держави. URL: https://sit.nuou.org.ua/article/download/75532/71520
8. Визначення агресії; Резолюція Генеральної Асамблеї ООН 3314 (XXIX) від 14.12.1974. URL: https://zakon.rada.gov.ua/laws/show/995_001-74;
9. Afroditi Anastasiou Papanastasiou/ Cyber Warfare Operations as Aggression in International Law. URL: http://cyberwarlaw.eu/cyber-warfare-operations-as-aggression-in-international-law
10. Рішення РНБО від 27.01.2016 "Про Стратегію кібербезпеки України". URL: https://zakon.rada.gov.ua/laws/show/n0003525-16
11. Указ Президента України від 06.04.2011 № 406/2011, Редакція від 04.02.2019 "Про Положення про Міністерство оборони України". URL: https://zakon.rada.gov.ua/laws/show/406/2011
12. Указ Президента України від 30.01.2019 № 23/2019 "Про Положення про Генеральний штаб Збройних Сил України". URL: https://zakon.rada.gov.ua/laws/show/23/2019?find=1&text=%EA%B3%E1%E5%F0#w11

References

1. Naybil′shi kiberataky proty Ukrayiny z 2014 roku/Infografika/ Zhurnal "Novoe vremya"[The largest cyber attacks against Ukraine since 2014 / Infographics from July 08, 2017] / Magazine "New time"/URL:https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html [In Ukranian]
2. Anastasiya Zanuda/ Malen′ki zeleni bayty atakuvatymut′ chastishe - eksperty z kiberoborony// BBC Ukraina/ [Little green bytes will attack more often - Cyberspace experts] / BBC Ukraine / January 30, 2017/ URL:https://www.bbc.com/ukrainian/features-38758423 [In Ukranian]
3. Trofymenko P. E., Pushkar′ov Y. I., Latin S. P. ta in/Taktychna pidhotovka artyleriys′kykh pidrozdiliv : pidruchnyk. Sumy : Sums′kyy derzhavnyi universytet, 2012. 776 s. [Tactical preparation of artillery units: textbook] / Sumy State University, 2012. 776 p./URL: https://buklib.net/books/37546/ [In Ukranian]
4. Zakon Ukrainy "Pro oboronu Ukrayiny" vid 06.12.1991 № 1932-XII/ Redakciya vid 04.11.2018/[Law of Ukraine "On the Defense of Ukraine" dated December 6, 1991, No. 1932-XII / Ed. 04/11/2018 /] URL: https://zakon.rada.gov.ua/laws/show/1932-12 [In Ukranian]
5. Zakon Ukrainy "Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny" vid 05.10.2017 № 2163-VIII; Redaktsiya vid 08.07.2018 [Law of Ukraine "On the Basic Principles of

Cybersecurity Protection of Ukraine" dated October 5, 2017, No. 2163-VIII; Revision from 08.07.2018] URL:https://zakon.rada.gov.ua/laws/show/2163-19 [In Ukranian]
6. Kristian Boris/ Den', kogda zagadochnaya kiberataka paralizovala Ukrainy// BBC Future/ 6 lipnya 2017 [The day when the mysterious cyber attack paralyzed Ukraine] / BBC Future / 6 July 2017 /URL: https://www.bbc.com/ukrainian/vert-fut-russian-40509165 [In Russian]
7. Chernonoh O.O., Zhyvylo YE. O., Mashtalir V. V. “Stratehiya zabezpechennya kibernetychnoyi bezpeky Zbroynykh Syl Ukrayiny; Interaktyvnyy dyskurs u konteksti informatsiynoyi bezpeky derzhavy” [Strategy of providing cybernetic security of the Armed Forces of Ukraine; Interactive Discourse in the Context of State Information Security] URL: https://sit.nuou.org.ua/article/download/75532/71520 [In Ukranian]
8. Vyznachennya ahresiyi; Rezolyutsiya Heneral′noyi Asambleyi OON 3314 (XXIX) vid 14.12.1974 [Definition of aggression; Resolution of the General Assembly of the United Nations 3314 (XXIX) of 14.12.1974]/ URL:https://zakon.rada.gov.ua/laws/show/995_001-74 [In Russian]
9. Afroditi Anastasiou Papanastasiou/ Cyber Warfare Operations as Aggression in International Law. URL: http://cyberwarlaw.eu/cyber-warfare-operations-as-aggression-in-international-law/ [In English]
10. Rishennya RNBO vid 27.01.2016 Pro Stratehiyu kiberbezpeky Ukrayiny [Decision of the National Security and Defense Council dated January 27, 2016 On the Strategy of Cybersecurity of Ukraine]. URL: https://zakon.rada.gov.ua/laws/show/n0003525-16 [In Ukranian]
11. Ukaz Prezydenta Ukrayiny vid 06.04.2011 № 406/2011, Redaktsiya vid 04.02.2019 “Pro Polozhennya pro Ministerstvo oborony Ukrayiny” [Decree of the President of Ukraine dated 06.04.2011 № 406/2011, Revision of 04.02.2019 "On the Regulations on the Ministry of Defense of Ukraine"] / URL: https://zakon.rada.gov.ua/laws/show/406/2011 [In Ukranian]
12. Ukaz Prezydenta Ukrayiny vid 30.01.2019 № 23/2019 “Pro Polozhennya pro Heneral′nyy shtab Zbroynykh Syl Ukrayiny” [Decree of the President of Ukraine dated January 30, 2019 No. 23/2019 "On the Regulations on the General Staff of the Armed Forces of Ukraine"] / URL: https://zakon.rada.gov.ua/laws/show/23/2019?find=1&text=%EA%B3%E1%E5%F0#w11 [In Ukranian]