ками (Risk Management), що дозволить забезпечити національну стійкість України та використання досвіду США з організації взаємодії у сфері кібербезпеки з приватним сектором. В результаті планується реалізація конкретних проєктів міжнародної технічної допомоги щодо побудови мережі галузевих і регіональних операційних центрів безпеки (Security Operation Centre) та команд реагування (CSIRT), які передбачені Стратегією кібербезпеки України та формування за допомогою США кадрового потенціалу з кібербезпеки шляхом проведення навчальних курсів на базі CISA, тренінгів, спільних навчань.

Підсумовуючи вищевказане, можна зазначити, що міжнародна співпраця України у сфері кібербезпеки та кіберзахисту є важливою складовою та перспективним напрямком розвитку для ефективного забезпечення не лише національної безпеки нашої держави, а і безпеки європейської та загалом глобальної. Стрімкий розвиток інформаційних цифрових технологій несе не тільки користь комп'ютеризації промислової ланки, а й загрозу безпеці як цілого суспільства та держави, так і окремих громадян. Лише спільними силами можливо протидіяти кіберзагрозам шляхом вироблення єдиних підходів в боротьбі з ними, оперативного реагування та цілковитої співпраці.

Список використаних джерел

1. Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. *Юрист&Закон*. 2020. URL: http://surl.li/aqgyo
2. Рішення Ради національної безпеки та оборони України «Про Стратегію кібербезпеки України» від 26.08.2021 р. URL: http://surl.li/aqgxi
3. Демедюк С. Необхідно підвищити рівень українсько-американського діалогу у сфері кібербезпеки. URL: http://surl.li/aqgzd

Науковий керівник: к.ю.н., доцент, доцент кафедри Мануїлова К. В.

МАСЛОВСЬКА ТЕТЯНА ПАВЛІВНА

Національний університет «Одеська юридична академія»

ВИКОРИСТАННЯ СИЛИ У КІБЕРПРОСТОРІ В РАМКАХ МІЖНАРОДНОГО ПРАВА

Таке визначення, як кібервійна має співзв'язок з такими поняттями як кібервійна, кібератака кібероперація та кіберзлочин.

Для того, щоб якомога краще зрозуміти вище згадані терміни, можна звернути увагу на думку Ендрю Стормсома. Це фахівець

з інформаційних технологій та безпеки. Він пропонує префікс «кібер» видалити і застосовувати ті ж рішення, які повинні бути використанні в класичному кримінальному праві [1].

Звертаючи вашу увагу, автор наголошує на тому, що неможливо уявити будь-який акт кібервійни, який також не буде порушенням чинних законів. Тобто, кібервійна завжди є кіберзлочином, але не кожен кіберзлочин може бути визнаний актом кібервійни.

Неможливо не згадати українських вчених, а саме О.О. Мережко, який зазначає, що у міжнародному праві немає ясних та певних критерій, які допомогли б відділити акти звичайного комп'ютерного хуліганства від таких нападів, які завдяки своїй серйозності мають характер збройного нападу надержаву, або є початком збройної агресії проти певної держави [4, с. 151].

Щодо норм сучасного міжнародного права, точніше Додаткового протоколу до Женевських конвенцій від 12.08.1949 року, що торкається саме захисту жертв міжнародних збройних конфліктів (Протокол I від 08.06.1977 року), в період збройних конфліктів нападами визначаються: «акти насильства щодо противника незалежно від того, здійснюються вони під час наступу чи оборони» (ст. 49) [3].

Цей протокол розповсюджує свою дію на всі об'єкти та напади, незалежно від того, де вони розташовуються або здійснюють свою діяльність. До того ж, у 1977 р. Такого поняття, як кіберпростір формально враховано не було у положеннях цієї статті та самого поняття до того ж не існувало.

Займатися такою діяльністю можуть не тільки певні особи, групи чи організації (включаючи терористичні), а навіть й держави або коаліції держав. Кібернетичні атаки можуть здійснюватися як з іншими нападами так і окремо, що беззаперечно загрожує суверенітету та безпеці держави.

За суб'єктним складом кібернетичні напади можна класифікувати на:

1) атаки, які здійснюються або фізичними або юридичними особами, їх об'єднаннями чи державами проти фізичних чи юридичних осіб або їх об'єднань;

2) атаки, які здійснюються особами юридичними та фізичними, а також їх об'єднаннями самостійно чи за участі (сприяння, фінансування) держави проти держав чи міжнародного правопорядку;

В цих атаках мають місце факти вчинення кіберзлочинів. Вони наносять значну шкоду або навіть спричиненюють смерті людей, пошкодження чи знищення окремих об'єктів. Внаслідок таких атак можуть бути виведені із ладу навіть об'єкти критичної інфраструктури з масштабними і серйозними наслідки;

3) атаки здійснюються спеціальними підрозділами держави проти інших держав чи міжнародного правопорядку або збройними силами.

Тобто, тут йдеться про те, що коли здійснюються такі атаки, то їх можна віднести до міжнародного кібернетичного нападу.

За допомогою звичаїв та основних принципів міжнародного права можна регулювати кіберпростір, тим самим забезпечивши кібербезпеку.

Принцип суверенної рівності держав – один із основних та важливих. В ньому йдеться про те, що абсолютно люба держава володіє юрисдикцією та владою в межах своєї території, а відповідно і інфраструктури інформаційно-комп'ютерних технологій (ІКТ), що розташована на ній. Цей принцип зобов'язує держав до відповідальності, а саме, які-небудь атаки проти інших країн чи інституцій, які б могли порушити міжнародне право, не було організовано чи здійснено з її території [2].

Неможливо не виділити принцип добросусідства (ст. 74 Статуту ООН), який також покладає певні зобов'язання на кожну державу, а саме не дозволяє використовувати власну територію для таких дій, які суперечать правам інших держав [3].

Далі можна виділити принцип «не завдавати шкоди», саме в Стокгольмській декларації 1972 р. отримав нормативне закріплення, а також декларації Ріо 1992 р. та існує як звичаєва норма.

Важливого значення набув принцип належної добросовісності, який регулює кіберпростір, а також забезпечує кібербезпеку, саме цей принцип застосовується для боротьби з фінансуванням тероризму та самим тероризмом [2].

Отже, принципи є важливим елементом у міжнародному праві, які забезпечують кібербезпеку. Знову повертаємося до О.О. Мережка, а саме до монографії «Проблеми теорії міжнародного публічного та приватного права». Вчений звертає нашу увагу на проект Конвенції про заборону використання кібервійни в Інтернеті. В ст.1 проекту йдеться про наступне визначення: «кібервійна – використання Інтернету й пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній та інформаційній безпеці та суверенітету держави».

«Інтернет є спадщиною людства, яке використовується тільки в мирних цілях», – так зазначає Олександр Олександрович.

До того ж, американська транснаціональна компанія Cisco формулює кібервійну як Інтернет-конфлікт, який передбачає проникнення у комп'ютерні системи та мережі інших країн.

Також потрібно розглянути норми міжнародного права, які використовуються для регулювання засобів здійснення кібернападів або за допомогою кібернетичної зброї.

Каберник В. – начальник відділу перспективних науково-освітніх розробок Управління інноваційного розвитку Росії, звертає увагу на те, що кіберзброєю є різні технічні та програмні засоби, які спрямовують свою діяльність на експлуатацію вразливостей у системах передачі та обробки інформації або програмно-технічних системах (віруси типу Flame, зомбімережі, DOS і DDOS-атаки).

Якщо держава застосовує кібернетичну зброю, то це можна віднести до міжнародного злочину агресії. Найбільш тяжкі міжнародні злочини – це певні міжнародні правопорушення, які загрожують знищенню існуючого міжнародного порядку, порушують права та інтереси всього світового співтовариства, як правило вчиняються з неправомірним застосуванням збройних сил, інших неправомірних примусових заходів, ставлять під загрозу існування держави тощо.

Тому, якщо кібератака включає здійснення дій, передбачених кримінальним і міжнародним правом, такі діяння можуть бути кваліфіковані як кіберзлочини та міжнародні кібернетичні злочини відповідно.

Список використаних джерел

1. Bradley T. When is a Cybercrime an Act of Cyberwar? URL: https://www.pcworld.com/article/250308/when_is_a_cybercrime_an_act_of_cyberwar_html (дата звернення: 03.11.2021)
2. Matthias C. Kettemann. Ensuring Cybersecurity through International Law. URL: https://www.jstor.org/stable/26296737?readnow=1&refreqid=excelsior%3A6fb9e65c043f51fa573028c4c61c9e93&seq=4#page_scan_tab_contents (дата звернення: 03.11.2021).
3. Summary of relevant aspects of Corfu Channel case (Merits). URL: https://www.iilj.org/wpcontent/uploads/2016/08/Summary-of-and-extract-from-Corfu-Channel-Case-United-Kingdom-v-Alb ania.pdf (дата звернення: 03.11.2021).
4. Додатковий протокол до Женевських конвенцій від 12.08.1949 р., що стосується захисту жертв міжнародних збройних конфліктів (Протокол від 08.06.1977р.). URL: http://zakon.rada.gov.ua/laws/show/995_199 (дата звернення: 03.11.2021).
5. Мережко О. О. Проблеми теорії міжнародного публічного і приватного права. Київ : Юстиниан, 2010. 320 с.

Науковий керівник: к.ю.н., доцент, доцент кафедри Грушко М. В.