Жаборинська Ірина, ***студентка групи КІ-11***

КІБЕРВІЙНИ ТА КІБЕРТЕХНОЛОГІЇ, ЇХ РОЛЬ У ПОЛІТИЦІ

Інформаційний простір формується сьогодні не лише вербально, велику роль у цьому грають інформаційні технології. Вони стали силою, але одночасно і точкою вразливості сучасних держав, які суттєво залежать в своєму функціонуванні від них, оскільки за допомогою них ведеться не лише накопичення і обробка інформації, а й управління і виробництвом, і військовими діями. Останнім часом залежність людства від нових технологій зростає з неймовірною швидкістю. На жаль, ця загалом прогресивна тенденція несе в собі і певні негативні наслідки. Станом на 2014 р. у світі вже 2,8 млрд людей мали доступ до мережі Інтернет, налічувалося близько 10 млрд пристроїв, що під'єднані до цієї всесвітньої мережі. Спостерігається тенденція створення надзвичайно розгалуженої мережі під'єднаних до Інтернету речей, що можуть функціонувати самостійно (так званий «Internet of Things») [6]. Проте застосування таких технологій відкриває також і нові шляхи до зловживань з використанням мережі Інтернет, серед яких крадіжки, незаконний обіг заборонених товарів, надання незаконних послуг, диверсії, тероризм і навіть руйнування інфраструктури міст під час ведення війни. Це, безперечно, спонукає держави й міжнародні організації приділяти значно більшу увагу забезпеченню кібербезпеки, вимагає врегулювання цієї проблеми на міжнародному рівні.

Актуальність проблеми обумовлена також розвитком інформаційних технологій, інтенсивою інформатизацією не лише органів державного управління, але й усієї системи життєзабезпечення суспільства, виведенням проблеми забезпечення кібербезпеки на якісно новий рівень, який є практично співставним з військовою безпекою держави.

Метою дослідження є висвітлення проблеми «кібервійни» та «кібертехнологій», шляхів захисту від кібервійни, адже ці проблеми потребують політологічної концептуалізації та подальшого вивчення. Можна прогнозувати, що кібервійни відіграватимуть дедалі значущу роль у міждержавній політиці, подальшому військовому будівництві не лише держав-лідерів, а й тих, які знаходяться ще на шляху до економічного зростання та незалежності.

Отже, «**кібервійна»** — комп'ютерне протистояння у просторі Інтернету, спрямована передусім на дестабілізацію комп'ютерних систем і доступу до інтернету державних установ, фінансових та ділових центрів і створення безладу та хаосу в житті країн, які покладаються на інтернет у повсякденному житті. Міждержавні стосунки і політичне протистояння часто знаходить продовження в інтернеті у вигляді кібервійни: вандалізмі, пропаганді, шпигунстві, та безпосередніх атаках на комп'ютерні системи та сервери. Науковці небезпідставно зазначають, що при визначенні терміну «кібервійна» доцільно спиратись на трактування війни у класичному розумінні[4]

Термін «кібервійна» ввійшов в обіг військових, фахівців з інформаційної безпеки та політиків, хоча понятя не закріплено в офіційних документах на національному та міжнародному рівнях. Слово «кібер» походить від слова кібернетика, що, в свою чергу, є похідним від грецького слова kybernetike, яке дослівно перекладається як «мистецтво управління». За визначенням в англомовних словниках, «кібер» означає те, що відноситься до комп'ютерів, комп'ютерних мереж (зокрема мережі Інтернет) та віртуальної реальності; електронне середовище, в якому відбувається он-лайн комунікація. За визначенням Міжнародного союзу електрозв'язку, кіберпростір – це фізичний і нефізичний простір, що складається з комп'ютерів, комп'ютерних систем, мереж та комп'ютерних програм, комп'ютерних даних, контенту, даних трафіку та користувачів[2].

Кібервійни націлені на технічні об'єкти, реалізуються приховано й здійснюють опосередкований психологічний вплив на осіб, що приймають рішення та фахівців ІТ-сфери, задіяних в управлінні об'єктами інформаційної інфраструктури. Отже, кібервійну можна розглядати як комплексне використання можливостей сучасних інформаційних технологій для впливу і віддаленого управління критично важливими ресурсами і системами супротивника [3].Не секрет, що розвідувальні органи багатьох держав займаються шпигунством в інтернеті: збирають інформацію, зламують комп'ютерні системи інших

держав, займаються диверсійною діяльністю та економічним шпигунством. Поте, кібервійни спрямовані не тільки на збір конфіденційної інформації, а також на здійснення військових дій, здатних викликати економічний збиток, пошкодити важливу інфраструктуру, а також вплинути на результат звичайних збройних конфліктів.

На відміну від кібер-атак минулого зараз кібервійна являє собою загрозу для національної безпеки країн і сприймається багатьма як серйозна загроза безпеці держави. Крім того, розвідувальні організації багатьох країн займаються шпигунством використовуючи інтернет: збирають інформацію, зламують комп'ютерні системи інших держав, займаються диверсійною діяльністю та економічним шпигунством. За визнанням спеціалістів, лідерами у веденні кібервійни зараз є Китай та Росія. Зокрема Китай звинувачували у організації атак на сайти Сполучених Штатів, Німеччини, Індії. Росія використовує інтернет не тільки для збору інформації, але й для організації масованих атак на недружні країни. Росія, як і Китай, однак заперечують причетність державних установ до організації атак. Беруть участь у кібервійнах і українські хакери. Так після подій навколо акту вандалізму на Говерлі, сайти Євразійського союзу молоді, який взяв відповідальність за їхнє проведення, були атаковані з України. У відповідь зазнали атак сайти президента України та СБУ [4]..

Уже є досвід використання кіберзброї в суто технічному смислі. Це вірус **Stuxnet**, що був розроблений в США і застосований Ізраїлем для атаки на ядерні об'єкти Ірану. Причому експерти чітко визнали його застосування незаконним. Світ отримав новий простір. Наявність його автоматично породжує можливості для атаки, оскільки чим важливішим він стає, тим сильнішими будуть наслідки такої атаки. А майбутнє буде тільки підвищувати статус кіберпростору. [5].

У зв'язку з розвитком нових технологій рівень кібервійни постійно вдосконалюється. Деякі держави починають приділяти захистові від кібервійни належну увагу — виділяють необхідні кошти для організації систем захисту і підтримують спеціальні підрозділи, основною задачею яких є вдосконалення інтернетної безпеки країни та захисту від нападів. Так, міністерство оборони США розробло власну стратегію для кіберпростору, яку назвало першою. У ній констатується, що атаки супротивників стали більш чисельними, і більш ускладненими. Акцентується, що деякі кібератаки можуть прийти з середина, а не ззовні[5]..

У багатьох державах, таких як США, Ізраїль, Франція, Німеччина, Росія, Індія, Іран, Пакистан, Південна і Північна Корея – вже давно з'явилися структури у збройних силах, які відповідають за ведення «кібервійни». З усіх держав, включно з Китаєм, саме США досягли найбільш вражаючих успіхів у створенні кібервійськ – їхня модель національного багатокомпонентного «кіберщита» є зразком для багатьох країн завдяки її ефективності, але недосяжна через захмарну вартість.

Висновки: «Кібервійни» і «кібертероризм» є порівняно новими видами загроз для національної і міжнародної безпеки. Сьогодні «кібервійна» – не далеке майбутнє, а реальність, і вона здатна захопити весь світ, оскільки комп'ютери і сервери, що беруть участь в ній, можуть перебувати в будь-якій точці планети. Питання кібербезпеки дедалі гостріше стає проблемою не лише національного рівня, а тому вимагає розширення міжнародно-правового співробітництва між суб'єктами міжнародного права задля збереження миру і недопущення розв'язання кібернетичних війн, які можуть супроводжуватися і кінетичними.

Література

1. *Почепцóв. Г. Г. Інфовійни в кіберпросторі / Г.Почепцов / [Електронний ресурс – Режим доступу*
2. *Oxford Dictionaries. [Електронний ресурс] - Режим доступу: : http://www.oxforddictionaries.com/definition/english/cyber*

3. *Геннадій Карпюк. У світі вже тривають «гарячі» та «холодні» кібервійни. [Електронний ресурс] - Режим доступу: http://na.mil.gov.ua/36184-u-sviti-vzhe-trivayut-garyachi-ta-xolodni-kibervijni.*
4. *Друг В., Матковський В. Кібервійни, Інтернет-розвідка / В.Друг [Електронний ресурс] Режим доступу: http://www.polpravozhit.in.ua/2015/05/blogpost_4.html*
5. *Запорожець, О. Ю. Кібервійна: концептуальний вимір / О. Ю. Запорожець // Актуальні проблеми міжнарод них відносин. – 2014. – Вип. 121 (частина І). – С. 80–86.*
6. *Камчатний М В. Історія міжнародно-правового регулювання питань, пов'язаних із застосуванням комп'ютерних технологій / М. Камчатний / [Електронний ресурс] – Режим доступу https://cyberleninka.ru*
7. *Томахів В.Я. Політологія. Навчальний посібник, 2-ге вид., доп / В.Я. Томахів. — Тернопіль: ТНЕУ, 2017. — 183 с. [Електронний ресурс] - Режим доступу: https://www.twirpx.com/file/2364502/*
8. *Чигур, Р. Ю. Феномен глобалізації: соціально-філософський аналіз / Р. Ю. Чигур // Наукові записки Національного університету «Острозька академія»: Серія «Філософія», Острог, 2015.– Випуск 18.– С. 96-102*
9. *Гончарук, Т. В. Філософія сучасного українця у форматі інноваційного суспільства / Т. В. Гончарук // Наукові записки. Сер. Філософія. – Острог : Національний університет «Острозька академія», 2011. – Вип. 9.*
10. *Гурик, М. І Декомунізація як шлях побудови україноцентристської моделі історичної пам'яті / М І. Гурик // Актуальні проблеми філософії та соціології.– 2016. – Вип. 11. – С. 26-29.*