УДК 327.5

А. В. Слободянюк
В. М. Задорожний

ВАЖЛИВІСТЬ КІБЕРЗАХИСТУ ДЛЯ УКРАЇНИ ТА СВІТУ

Вінницький національний технічний університет

Анотація
У *статті розглядаються військово-політичні та теоретичні аспекти сучасного стану та можливості подальшого захисту країн від можливих кібератак.*
Ключові слова: кіберзахист; кібербезпека; кібервійна; кіберпростір; кібератака.

Abstract
The article describes military-political and theoretical aspects of the current state and opportunities in further protection of countries from possible cyber attacks
Keywords: cyber defense; cyber security; cyber war; cyber space; cyber attack.

Вступ

Розвиток інформаційних та комунікативних технологій в сучасному світі досягає значних масштабів. Але разом із позитивними рисами даного розвитку завжди виникають і негативні. Так інформаційні потоки можуть використовуватися не лише в конструктивних, але і в деструктивних цілях. Вони зробили свій вплив на характер, форми і способи ведення бойових дій. У XXI столітті війни ведуться не тільки на землі, у морі, повітрі, але і в «кіберпросторі». Термін «кібервійни» і «кібертероризму» є новими видами загроз для національної і міжнародної безпеки. Тому проблема «кіберзахисту» вимагає вивчення і політологічної концептуалізації

Метою роботи є розгляд поняття «кібервійна» та «кіберзахист» й аналіз сучасного стану даної проблеми у світі.

Результати дослідження

В останній час терміни з приставкою «кібер» все частіше вживаються в міжнародно-політичному дискурсі та знаходять відображення в стратегічних доктринах не тільки держав, але і міжнародних організацій, включаючи НАТО. Термін «кібервійна» міцно увійшов у лексикон військових, фахівців з інформаційної безпеки та політиків, але серед представників експертного співтовариства немає єдиного визначення цього поняття. Американський експерт в області кібербезпеки Р. Кларк, автор книги «Кібервійна», пропонує наступне визначення: «Кібервійна – дії однієї держави з проникненням у комп'ютери або мережі іншої держави для нанесення збитків або руйнування» [1]. Вітчизняний експерт міжнародного права О. Мережко пропонує таке тлумачення: «Кібервійна – використання Інтернету і пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній, інформаційній безпеці та суверенітету іншої держави» [2]. З перерахованого вище можна охарактеризувати «кібервійну» як вид військових дій із використанням комп'ютерів та Інтернету, націлений в першу чергу на найважливіші системи функціонування та життєзабезпечення держави: електростанції, енергетичні мережі, транспортні шляхи, системи водопостачання та водовідведення тощо.

Сукупність «кібератак», які перевищують своїм загальним негативним впливом певний поріг, можуть розглядатися як початок «кібервійни». «Кібератаки», яка увійшла в історію, є є наприклад атака яка почалися 27 квітня 2007 року під час загострення російсько-естонських відносин пов'язаних з переносом пам'ятника Бронзовому солдату у Таллінні. Скоординована атака хакерів вивела на деякий час з ладу сайти парламенту Естонії, міністерств, банківських установ, засобів масової інформації. На думку деяких оглядачів, кібератака на Естонію належала до одних з найкраще організованих та масових в історії Інтернету [3].

Саме тому поняття «кіберзахист» набуває необхідності на міжнародному рівні. «Кіберзахист» – сукупність заходів організаційного, нормативно-правового, воєнного, оперативного, технічного та

іншого характеру, спрямованих на забезпечення кібербезпеки. «Кібербезпека» — стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі [4].

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.

Прикладом є вірус «Petya» який 27 червня 2017 року сталась масштабна атака останнім представником сімейства, який запозичив деякі модулі з попердніх зразків, але можливо був створений іншими розробниками та вже був вірусом-винищувачем даних, замаскованим під програму-вимагач [5]. І це є не перший подібний випадок, так 23 грудня 2015 року сталася «кібератака» на «Прикарпаттяобленерго»: : було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин. Атака відбувалась із використанням троянської програми BlackEnergy [6].

Розвиток «кіберзахисту» має переважати розвитку «кібератак» для запобігання подібних ситуацій. Адже повторення «кібератак» на будь-яку країну призводить до чисельних втрат. Тим паче вірусні атаки вже встигли стати звичним явищем в Україні, вони трапляються частіше, їхні наслідки дедалі серйозніші. Активність ворожої сторони та звичайних комп’ютерних шахраїв вимагає від української влади невідкладного розвитку національних засобів кібербезпеки [7].

У багатьох країнах, 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». Але найбільше розвинутий в цьому питанні Китай. Німецький експерт в області «кібербезпеки» Сандро Гейко стверджує, що в Китаї на державному забезпеченні знаходяться 15 тис. штатних хакерів [8].

У 2010 році США першими створили «кіберкомандування». Китай, Іран та інші країни теж поспішили створити свої «кібервійська» із відповідними доктринами та стратегіями. З 2011 року діє «Стратегія операцій в кіберпросторі міністерства оборони США», даний документ містить набір «стратегічних переваг в кіберпросторі», до яких відносяться оперативний зв'язок і можливості обміну інформацією та знаннями в сфері інформаційних технологій, у тому числі здійснення експертиз у сфері кібербезпеки. Додатковий акцент робиться на розвитку міжнародного співробітництва США в кіберпросторі в рамках міжнародної взаємодії, колективної самооборони, а також встановлення міжнародних норм, що регулюють кіберпростір [9].

Компанії «Center for Strategic» та «International Studies» оцінили збитки світової економіки від кіберзлочинності за 2014 рік у розмірі 445 млрд доларів. Найбільший удар від незаконних дій хакерів зазнають США, Китай, Японія та Німеччина – економіки цих країн щороку не дораховуються в цілому близько 200 млрд доларів[10]. У країнах, що розвиваються збиток набагато нижче, але він буде рости в міру збільшення проникнення Інтернету в цих регіонах. За даними дослідження, світова інтернет-економіка генерує від 3 трлн доларів на рік. Приблизно 15-20% від цієї суми забирають «кіберзлочинці» [10]. Єврокомісія заявила, що за даними на 2014 рік, мінімум 1 млн користувачів Інтернету щодня піддається «кібератакам». А сукупний збиток для бізнесу від діяльності «кіберзлочинців», за різними оцінками, становить від 89 до 250 млрд євро на рік. Звичайним користувачам буде корисно знати, що у всесвітній мережі наразі існує більше 150 тис. комп'ютерних вірусів різної модифікації [11].

В Україні на подолання «кібератак» та покращення стану «кібербезпеки» є нещодавнє ухвалення Верховною Радою проекту Закону «Про основні засади забезпечення кібербезпеки України». Законопроект № 2126а, як і більшість сучасних нормативних документів, одразу дістав скандальну репутацію. Таку, що з першої спроби його не змогли ухвалити, підтримало лише 186 депутатів. Головним зауваженням стала можливість встановити контроль держави над бізнесом. Знімалися обмеження на перевірки підприємств, які займаються криптографічним і технічним захистами. Дозволяється діяльність лише телеком-операторів, які мають системи захисту встановленого зразка. Крім того, критикувалися й певні потенційні можливості обходу системи державних закупівель ProZorro. З позитивних положень: підняття зарплат спеціалістам із кібербезпеки, що давно є однією з головних проблем для державних установ [12].

Висновки

Сьогодні головною темою обговорення у світі має стати зміцнення «кібербезпеки» та скорочення кількості «кібератак» в «кіберпросторі». Дана проблема потребує якнайшвидшого вирішення, оскільки створені зразки кіберзброї вирізняються глобальною досяжністю, практично миттєвим впливом без будь-якого способу отримання попередження про її застосування. «Кіберзахист» це

єдине, що може запобігти чисельним втратам і втручання чужих країн в безпеку інших. Адже одна програма може вивести з ладу усе необхідне для безпеки та життєдіяльності людини та країни. «Кіберзахист» повинен працювати до моменту скоєння «кібервійни», а не після перших «кібератак».

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Овчинский В. Холодная война 2.0 [Електронний ресурс] / В. Овчинский, Е. Ларина // цит. из Richard A. Clarke and Robert K. Knake» Cyber War: The Next Threat to National Security and What to Do About It» (Harper Collins 2010) / доклад Изборскому клубу. – Режим доступу: http://dynacon.ru/content/articles/4224/
2. Мережко О. Проблеми кібервійни та кібербезпеки в міжнародному праві [Електронний ресурс]. – Режим доступу: http://www.justinian.com.ua/article.php?id=3233.
3. Кібератаки проти Естонії (2007) [Електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/Кібератаки_проти_Естонії_(2007)
4. Проект до закону України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. - Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=55657&pf35401=348091
5. УНІАН: События недели: версия читателей УНИАН — на Украине испытали кибероружие. [Електронний ресурс] – Режим доступу: https://www.unian.net/politics/2005231-sobyitiya-nedeli-versiya-chitateley-unian-na-ukraine-ispyitali-kiberorujie-v-kieve-vzorvali-polkovnika-gur-a-v-zone-ato-s-boem-vzyali-novogo-otpusknika.html
6. Хакерська атака Росії на українську енергосистему: як це було [Електронний ресурс]. - Режим доступу: http://texty.org.ua/pg/article/newsmaker/read/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak
7. Подвійна істина кіберзахисту [Електронний ресурс] /Юрій Лапаєв // Тиждень.ua – Режим доступу: http://tyzhden.ua/Society/202550
8. Госучреждения Германии страдают от хакерских атак [Електронний ресурс]. - Режим доступу: http://www.dw.de/госучреждения-германии-страдают-от-хакерских-атак/a-16691699.
9. Савин Л. Холодная кибервойна [Електронний ресурс] / Л. Савин // Информационно-аналитический портал Геополитика. – Режим доступу: http://www.geopolitica.ru/article/holodnaya-kibervoyna#.VUAFU9Ltmkp.
10. Мировая экономика теряет 445 млрд долларов из-за «киберпреступков» [Електронний ресурс]. - Режим доступу: http://www.dailycomm.ru/m/27316/.
11. Ковалёв Н. «Началась новая техногенная эпоха – с кибервойнами, кибертерроризмом, киберпреступностью» [Електронний ресурс] / Н. Ковалёв // Интервью для интернет-газеты «Столетия». – Режим доступу: http://qps.ru/odR7k.
12. Постанова Верховної Ради України Про прийняття за основу проекту Закону України про основні засади забезпечення кібербезпеки України [Електронний ресурс]. - Режим доступу: http://zakon2.rada.gov.ua/laws/show/1524-19
13. Слободянюк А. В. Соціальні норми та цінності як невід'ємні характеристики категорії влади [Текст] / А. В. Слободянюк // Вісник Київськ. нац. ун-ту ім. Т. Шевченка. Серія "Соціологія. Психологія. Педагогіка". - Вип. 9. - Київ, 2000. - С. 5-7.
14. Слободянюк А. В. Психологія управління та конфліктологія [Текст] : навчальний посібник для практичних та семінарських занять / А. В. Слободянюк, Н. О. Андрущенко. – Вінниця : ВНТУ, 2010. – 120 с.

Задорожний Віталій Миколайович — студент групи 1ПІ-14б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: Zadorozhnyy7@gmail.com

Науковий керівник: ***Слободянюк Анатолій Володимирович*** — канд. соц. наук, доцент кафедри суспільно-політичних наук, науковий керівник лабораторії соціологічних досліджень Вінницького національного технічного університету, Вінницький національний технічний університет, м. Вінниця

Zadorozhnyi Vitalii M. — Department of Information technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: Zadorozhnyy7@gmail.com

Supervisor: ***Slobodianiuk Anatolii V.*** — PhD in Sociology, assistant professor of social and political sciences, scientific director of the laboratory of sociological researches Vinnitsa National Technical University, Vinnytsia National Technical University, Vinnytsia