УДК 304

В. І. Ярська
С. Г. Денисюк

КІБЕРАТАКИ ЯК ПОЛІТИЧНА ЗБРОЯ

Вінницький національний технічний університет

Анотація
У статті проаналізовано зростаючу роль кібербезпеки у світовій політиці та використання кібератак, як методу впливу на політичний простір.
Ключові слова: кібербезпека, кібератака, інформаційна безпека, національна безпека, світова політика.

Abstract
A
Keywords: cybersecurity, cyberattack, informational security, national security, world politics.

Вступ

У міру швидкого поширення Інтернету в 1990-х рр.. хакери почали займатися кібер-пустощами, тоді як звичайні злочинці почали досліджувати потенціал кіберзлочинності, активно розвиваючи Інтернет, який пов'язує як людей, так і мережі, комп'ютерні пристрої, прилади та інші предмети. За статистикою, станом на початок 2020 р. близько 60% населення світу користується інтернетом [1].

Загроза кібератак є викликом для національної безпеки, громадської безпеки та економіки, з яким стикається кожна нація у XXI ст. Кіберпростір є вагомою рисою сучасного життя. Фізичні особи та спільноти у всьому світі спілкуються у віртуальному просторі та за його допомогою. Існування численних проблем, пов'язаних з кібербезпекою в різних сферах життя, природно збільшує політичний інтерес у їх розв'язання. Потреба в кібербезпеці зростає, починаючи від окремих випадків, і закінчуючи національним і міжнародним рівнями, тому і стає головною проблемою політики.

Основна частина

На основі різних підходів, кібербезпека розглядається як інструмент здобуття національного рівня інтересів. Усі країни вважають, що кібербезпека є інструментом досягнення національних інтересів держави, оскільки більша частина сучасних теорій зосереджена на матеріальній вигоді. Тим часом деякі країни бачать кібербезпеку, як інструмент впливу на супротивників. Ця думка базується на основі величезних руйнувань та потужності кібератак. На відміну від двох основних підходів, органи національної безпеки наголошують, на використанні кібератак для забезпечення безпеки країни, а не на матеріальній вигоді.

У травні 2007 року Європейська Комісія опублікувала повідомлення «загальна політика проти кіберзлочинності», запропонувавши визначення потрійне кіберзлочинності:

1) традиційні форми злочинів, такі як шахрайство або підробка, які і вчинені через електронні мережі зв'язку та інформаційні системи;

2) публікація незаконного вмісту на електронних носіях (наприклад, сексуальне насильство над дітьми матеріал або розпалювання расової ненависті);

3) злочини, характерні лише для електронних мереж, наприклад, напади на інформаційні системи, відмова в обслуговуванні та злом [2].

Захист життя та майна від іноземних хакерів є загальновизнаною роллю уряду, а кібер-ера вводить нові можливості для інших країн отримати матеріальну вигоду чи спричинення війни.

Економіка та національна безпека багатьох країн сьогодні повністю залежать від інформаційних технологій та інформаційної інфраструктури. Мережеві технології забезпечують функціонування інфраструктури країн у таких секторах, як енергетика, транспорт, банківська справа та фінанси,

інформація та телекомунікації, охорона здоров'я, аварійні служби, сільське господарство, харчування, вода, військова та промислова база тощо.

Класифікують три основні групи суб'єктів, які становлять загрозу в кіберпросторі:

1) організовані злочинні групи, які найбільш схильні до сектору фінансових послуг;

2) держави-спонсори, які зацікавлені в крадіжці даних, включаючи інтелектуальну власність, дослідження та розвиток підприємств, державних установ та підрядників;

3) терористичні групи, що використовують мережеві технології для проведення деструктивних дій проти національної безпеки країни.

Через різні підходи до забезпечення національної безпеки та через різне розуміння питань безпеки, у світовій політиці не існує єдиного підходу, погодженого в кіберпросторі. Держави намагаються укласти двосторонні угоди. Один із існуючих методів узгодження підходів до кібербезпеки – це резолюції ООН. Посилаючись на ці резолюції, щодо ролі науки і техніки, політики виражають занепокоєння тим, що ці технології та засоби, потенційно можуть бути використані для цілей, які не відповідають цілям підтримки міжнародної стабільності та безпеки та можуть негативно вплинути на цілісність інфраструктури держав на шкоду їх безпеці як у різних сферах.

ООН закликає держави-члени сприяти у подальшому врахуванні існуючих та потенційних загроз у сфері інформаційної безпеки, а також можливі заходи щодо обмеження загроз, що виникають у цій галузі, відповідно до потреби, для збереження вільного потоку інформації на багатосторонньому рівні. Ціль таких заходів може бути здійснена шляхом вивчення відповідних міжнародних концепцій, спрямованих на посилення глобальної безпеки інформаційні та телекомунікації систем.

Висновки

Уряди держав повинні розглянути існуючі та потенційні загрози в сфері інформаційної безпеки та можливі спільні заходи щодо їх вирішення, для запобігання кібератак. Відповідно до цього підходу, основою забезпечення режиму кібербезпеки є Резолюція Генеральної Асамблеї ООН про боротьбу із злочинним зловживанням інформаційними технологіями та глобальною культурою кібербезпеки, положення яких спрямовані на боротьбу з тероризмом, а також положення Конвенції Ради Європи про кіберзлочинність. Дійсно, кібербезпека відіграє важливу та особливу роль у сучасній світовій політиці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Укрінформ. До середини року більш як половина населення світу буде користувачами сомереж. *Укрінформ*. URL: https:// www.ukrinform.ua/rubric-technology/2870117-do-seredini-roku-bils-ak-polovina-naselenna-svitu-bude-koristuvacami-socmerez.html

2. Архіви Європейської Комісії. *Офіційний веб-портал Європейської Комісії*. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF

3. Архіви Організації Об'єднаних Націй. *Офіційний веб-портал Організації Об'єднаних Націй*. 2013. URL: http://undocs.org/A/68/552 – Назва з екрану

Ярська Вікторія Ігорівна – студентка групи 1ІСТ-17б, факультету комп'ютерних систем та автоматики, Вінницький національний технічний університет, м. Вінниця, e-mail: vikavichenka@gmail.com

Денисюк Світлана Георгіївна – доктор політичних наук, професор, професор кафедри суспільно-політичних наук, Вінницький національний технічний університет, м. Вінниця, e-mail: svetadenisiyk@gmail.com

Yarska Victoria Igorivna – student of 1IST-17b, Faculty of Computer Systems and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: vikavichenka@gmail.com

Svitlana G. Denysiuk – Doctor of Politician science (Eng.), professor, professor of social and political sciences department, Vinnytsia National Technical University, Vinnytsia, e-mail: svetadenisiyk@gmail.com