Рудик Владислава, *студентка групи КІ-11*

РОЛЬ КІБЕРБЕЗПЕКИ У СВІТОВІЙ ПОЛІТИЦІ

Актуальність теми. Потреба в кібербезпеці зростає, починаючи від окремих випадків і закінчуючи національною та міжнародною проблемою дипломатії та світової політики. Усі країни вважають, що кібербезпека є інструментом досягнення національних інтересів держави, оскільки більша частина сучасних теорій зосереджена на матеріальній вигоді. Тим часом деякі країни розглядають кібербезпеку як інструмент впливу на супротивників. І все ж таки, кібербезпека відіграє важливу та особливу роль у світовій політиці.

Метою дослідження є дослідження значної і зростаючої ролі кібербезпеки у світовій політиці.

Об'єктом дослідження є дослідження потреби кібербезпеки в різних сферах життя.

Предметом дослідження є особливість та важливість ролі кібербезпеки у світовій політиці

Виклад основного матеріалу. Термін «кібербезпека» означає безпеку інфраструктури в кіберпросторі, тобто даних, якими обмінюються в кіберпросторі, але перш за все людей, які використовують кіберпростір [4, с. 105]. Наше суспільство все більше стає залежним від кіберпростору - місця, де поширені кібератаки і кібервійни. Оскільки ми покладаємося на інформаційні та комунікаційні технології в усіх аспектах кіберфізичного суспільства, потреба в кібербезпеці стає все більш важливою. Кібербезпека важлива для приватних осіб, громадських і неурядових організацій, але забезпечити безпеку часто буває складно. Питання безпеки не обмежуються лише виконавчою владою, це також стосується політичних партій, постачальників енергетичної інфраструктури, міністерств, адміністративних організацій і навіть спортивних організацій (таких як Міжнародний олімпійський комітет), всі з яких стали об'єктом крадіжки інформації. Таким чином, можна сказати, що уразливість кібербезпеки впливає на всі зацікавлені сторони суспільства.

Розробка політики в галузі кібербезпеки в даний час стикається з багатьма парадоксами. Вибір одного напряму може відбуватися за рахунок іншого напрямку, але аргумент двосторонній. Політика кібербезпеки і розробка політики відбуваються в складних екосистемах, в яких повинні взаємодіяти між собою зацікавлені сторони з різних суспільств, сфер політики та урядів. Обов'язки розподілені між багатьма державними структурами на центральному та місцевому рівнях з різними проблемами, що ускладнює ініціювання колективних дій. Суспільство складається з різноманітних гравців, які, можливо, хочуть безпеки, але мають різні очікування щодо ролі уряду в наданні безпеки в кіберпросторі. Уряд може відігравати незначну або основну роль у кібербезпеці. Політики повинні діяти відповідно до потреб суспільства, формулювати політику і розподіляти ресурси, а державні установи повинні реалізовувати поставлені цілі. Це схоже на прості відносини, але ситуація набагато складніша, оскільки ролі зацікавлених сторін зазвичай суперечать, що і є парадоксальним. Отже, один з таких парадоксів полягає в тому, що уряд хоче забезпечити кібербезпеку, але в той же час хоче отримати доступ до даних осіб та організацій для спостереження.

Неможливо також застосувати універсальний підхід до «компанії». Організації різноманітні і мають різні вимоги, банк і лікарня вимагають вищого рівня безпеки, ніж ресторан. Більше того, рівень знань, досвіду компанії, їх системи, їх вразливість та можливі наслідки порушення кібербезпеки різняться. Це ускладнює розмову про компанії загалом і про те, що від них очікують у віртуальному просторі. Як їх безпека може регулюватися урядами?

Суспільство неоднорідне, і оскільки кібератаки часто не видно, люди можуть про них навіть не знати, крім повідомлень від ЗМІ. Банки, компанії, що продають кредитні картки, і магазини можуть самі ризикувати, але таким чином захищати суспільство. Парадокс полягає в тому, що, хоча організації не виграють від того, щоб зробити проблеми та атаки видимими, ця видимість необхідна для створення більшого відчуття терміновості та ініціювання дій.

Для громадян взаємозв'язок та дані, що утворюються пристроями, призвели до «безпрецедентного поліпшення якості життя». У той же час величезна кількість даних про місцезнаходження громадян, діяльність та навіть емоції породжує виклики кібербезпеці та конфіденційності. Парадокс тут полягає в тому, що ті самі дані, які можна використовувати для поліпшення якості життя, можуть бути використані і проти громадян. Незважаючи на ризики, людей часто не турбує кібербезпека. Кібербезпека подібна до інфраструктури - ми сприймаємо її як належне і усвідомлюємо її важливість лише тоді, коли стикаємось з проблемою, але тоді вже пізно. І це вже ускладнює визначення того, хто повинен нести відповідальність за дії та забезпечення кібербезпеки.

Отже, підвищення політичної свідомості в такій кількості парадоксів непросте. Часто кібербезпека розглядається насамперед як технічний виклик: якщо вона організована належним чином і виділено відповідний бюджет, більше нічого робити не потрібно. На практиці питання не такі однозначні, немає чітких обов'язків, межі важко визначити так само як і необхідний рівень безпеки.

У той же час однією з специфічних характеристик кібербезпеки є те, що межі між кіберзлочинністю, застосуванням кіберзброї і поведінкою різних політичних акторів (наприклад, спецслужб в різних державах) досить розмиті і невизначені [3]. Тому загрози кіберпростору стали фактором багатьох внутрішніх політичних і міжнародних конфліктів, і також політичної «боротьби без правил» [3]. Одним з найбільш серйозних і масштабних інцидентів за своїми наслідками конфліктів стало звинувачення з боку лідерів Демократичної партії США «російських хакерів» у вторгненні в їх інформаційні ресурси і втручанні в президентські вибори в 2016 році [3]. Тим самим було продекларовано заяву про вплив Росії на внутрішньополітичну ситуацію в США і розтиражовану версію про підтримку Росією Д. Трампа, що ледь не стало основним фактором його передбачуваного обрання президентом [3]. Такі напади, пов'язані з атаками в кіберпросторі, стали одним з найбільш важливих факторів у багатьох внутрішньополітичних конфліктах в США, та різкого загострення російсько-американських відносин [3]. Таким чином, один цей факт свідчить про величезний і зростаючий вплив процесів в кіберпросторі на внутрішню та світову політику, а також про зростаюче значення кібербезпеки в сучасному світі. Іншими словами, ці процеси стають найважливішим політичним ресурсом для акторів сучасної політики.

Висновок. Отже, наше суспільство перетворюється на кіберфізичне суспільство, яке залежить від інформаційно-комунікаційних технологій у всіх аспектах нашого повсякденного життя, що робить потребу в кібербезпеці першочерговою. А нематеріальний характер кібербезпеки, соціально-технічна залежність, неоднозначний вплив та суперечливий характер боротьби з кібербезпекою роблять це складним напрямом для політиків. Усі країни вважають, що кібербезпека є інструментом для досягнення національних інтересів держави. Тим часом деякі країни розглядають кібербезпеку як інструмент впливу на супротивників. Дійсно, кібербезпека відіграє важливу та особливу роль у світовій політиці.

Список використаних джерел

1. Кібербезпека як важлива складова всієї системи захисту держави [Електронний ресурс] – Режим доступу : https://www.mil.gov.ua/ukbs/

2. Кібербезпека в ЄС та країнах-членах: генезис та проблеми її підвищення [Електронний ресурс] – Режим доступу : http://academy.ssu.gov.ua

3. Киберпространство как новая политическая реальность: вызовы и ответы [Електронний ресурс] – Режим доступу : https://www.socionauki.ru/journal/articles/1800199/

4. The Ethics of Cybersecurity: (The International Library of Ethics, Law and Technology 21 1st ed. 2020) By Markus Christen, Bert Gordijn, Michele Loic. 105-106