СЕКЦІЯ 12

СУЧАСНІ НАПРЯМИ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ

Желясков Артур Олександрович, Чемізова Віталія Вадимівна
студенти 5-го курсу факультету міжнародно-правових відносин
Національного університету «Одеська юридична академія»

ЗНАЧЕННЯ КІБЕРБЕЗПЕКИ У ВОЄННИЙ ЧАС

У час цифрових технологій та коли термін «гібридна війна» у пошуковому вікні Google займає сходинку вище ніж будь-яка інша проблема, актуальність та значення кібербезпеки недосяжні.

Світ перевернувся в котрий раз, у 2016 році в Брюсселі міністри оборони країн НАТО прийняли рішення, яке в наступні роки стане найголовнішою загрозою людства, а саме: визнання кіберпростору оперативною зоною військових дій. Тобто, з тієї самої зустрічі суходіл, море, повітря та кіберпростір стали в один ряд. Кібербезпека та захист персональних даних стали тотожними речами.

Велика Британія у 2013 році під реалізацію першої стратегії, пов'язаної з кібербезпекою, виклала один млрд фунтів на період 2013-2015 рр., щодо другої на 2016-2021 рр. – приблизно два млрд, чим створила у королівстві повноцінний центр кібербезпеки з відповідним бюджетом на майбутній розвиток та утримання [1, с. 1-2].

Звертаємо увагу, що ми живемо в час найбільш потенціального розвитку ІТ-технологій. Мережа Інтернет протягом 20 років керує суспільством, часом, поведінкою та настроєм кожного з нас. Соціальну мережу Твітер, нещодавно, намагалися купити за майже 40 млрд доларів, а це 100-річне фінансування Великої Британії в кібербезпеку.

На даний час, проблематика та значення кіберзахисту країн досягнула вершини Олімпу. Людство власними очима спостерігає, на що здатна сила кіберпростору та яку руйнівну хвилю вона за собою несе.

Перший раз в історії людства, людина з пристроєм, що підтримує мережу Інтернет, здатна нашкодити більше, ніж людина, що погрожує нанести превентивний удар по території іншої держави. Кіберзлочин або, по-іншому, комп'ютерний злочин – це діяння у кіберпросторі або з його використанням, що завдає суспільну небезпеку певному

колу населення, відповідальність за яке передбачена міжнародними договорами та законами держав-учасниць НАТО та ЄС. Найголовнішою ознакою кіберзлочинів є мета, а саме знівечення та розкрадання суспільно-важливої інформації в системах і мережах. У період воєнного часу це дестабілізує ситуацію на території держави через втрату конфіденційних даних, постійного безладу в державних установах, знищення техніки, а найголовніше – це моральний вплив [2].

Проблематикою етимології понять кібер, кіберпростору, «гібридної війни», національної безпеки, інформаційних атак у державних і недержавних структурах займалися такі провідні українські та світові вчені, як І. Кочан, Є. Магда, Р. Грищук, В. Горбулін, В. Пядишев, О. Рибальський, М. Делягін, В. Кутирьов, Г. Мірської, І. Міхеєв, В. Хорос, В. Антипенко, В. Крутов, В. Ліпкан, У. Еко, А. Гловацькі, С. Хантінгтон, С. Хоффман та ін.

Ці величезні розуми світу вважали кібертероризм найбільшою загрозою для всієї міжнародної спільноти. Кібертероризм є наднаціональною проблемою та складається з двох основ – кіберзлочинність та тероризм. На саміті НАТО в Уельсі у 2014 р. було оголошено, що «кібератаки можуть досягати такого рівня результатів, що загрожують євроатлантичному добробуту, безпеці і стабільності… Рішення про те, коли кібератаки потребують використати статтю 5, буде прийматися Північноатлантичною радою на індивідуальній основі» [3, с. 1-2].

Кібербезпека держави потребує такого ж укріплення, як і армія. Світ перейшов до нових реалій, де вся конфіденційна інформація, вкрай важливі документи з позначкою «секретно» зберігаються в електронному форматі, а отже мають бути захищені від ймовірних кібератак.

Інформаційні технології все більше виступають каталізатором змін правових відносин у державі, стають одним із чинників досягнення максимально позитивного результату в соціальних відносинах. Але одночасно виникає проблема формування низки негативних аспектів, які пов’язані з використанням інформаційних технологій: незаконне використання авторських прав, несанкціонований доступ до приватної та секретної інформації на всіх рівнях (від приватного до державного), несанкціонований вплив на обчислювальні машини з метою виведення їх з ладу з допомогою спеціальних програм («кібертероризм»). Усі ці негативні фактори вимагають прин-

ципово нових підходів у вивченні проблем співвідношення понять «національна безпека», «адміністративно-правове регулювання інформаційних відносин» та «кібербезпека». Ці підходи повинні базуватися на досягненнях наукового аналізу, знаходячи відображення в прийнятті практичних рекомендацій щодо захисту інформаційного простору України від протиправних посягань окремих осіб та організацій [4, с. 14].

Головною ланкою, яка допоможе забезпечити безпечність та збереження як персональних, так і держаних даних, є наукові розробки в галузі адміністративного захисту інформаційної сфери та вироблення прикладних засад протидії протиправним проявам у сфері життєдіяльності держави. Прикладним аспектом розгляду питання кібербезпеки є вироблення методологічних засад забезпечення безпеки інформаційних відносин у системі адміністративної діяльності держави. В галузі кібербезпеки важливо розробити механізми генерації нових рішень, що дозволять адекватно реагувати на погрози кібербезпеки або передбачати нові погрози та вміти їм протистояти [4, с. 16].

Отже, кібербезпека держави та її населення – є неймовірно важливим аспектом, який потребує пильної уваги та заходів забезпечення особливо у воєнний час, коли всі наміри супротивника направлені на виведення з ладу та дестабілізацію внутрішнього стану країни. Це – новий фронт XXI століття, який вимагає потужного укріплення.

Список використаних джерел

1. Тарасенко Т. Чому Україна стала полігоном для кібервійни. *Юридична Газета*. 2022. С. 1-2.

2. Закон України «Про основні засади забезпечення кібербезпеки України»: Закон України від 05.10.2017 № 2163-VIII. *Офіційний веб-сайт Верховної ради України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Кулик В., Біленчук П. Стратегія забезпечення кібербезпеки в гібридній війні. *Юридичний Вісник України*. 2018. С. 1-2.

4. Лисовська Ю. П. Кібербезпека: ризики та заходи. С. 14-16.

Науковий керівник: к.ю.н, доц. Канєнберг-Сандул О. К.