Бойчура Марія Юріївна
курсант 201 навчальної групи ННІ № 3 НАВС, рядовий поліції

Науковий керівник:
Яровий Кирило Васильович
кандидат юридичних наук, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, капітан поліції

ПРОБЛЕМИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Під час широкомасштабної агресії з боку російської федерації Україна стикається з різними формами кібератак. Агресор намагається перешкодити наданню електронних послуг, що призводить до порушення прав громадян та збоїв у роботі державних органів. Також маємо справу з фішинговими атаками через електронну пошту та порушенням цілісності та конфіденційності персональних даних, що створює інформаційно-психологічний тиск на населення.

У сучасних умовах, коли Україна перебуває в умовах воєнного стану, знання про цифрову грамотність, дотримання цифрового етикету та правила кібергігієни є важливими не лише для ІТ-фахівців, але й для будь-якого громадянина. З початком війни, фахівці з ІТ з усієї країни приєдналися до кіберполіції та успішно протистояли агресору. У результаті спільних заходів було зруйновано критично важливі інформаційні системи окупанта.

Зазначена робота ґрунтується на працях відомих українських науковців, таких як Бубело Б. [1], Погорецький М. [2], Шеломенцев В. [2], Савінова Н. [3], а також інших дослідників, які внесли значний вклад у вивчення проблеми кіберзлочинів та проведення попереднього розслідування з метою притягнення винних осіб до відповідальності за ці злочини. Незважаючи на це, зазначена тема залишається актуальною та потребує подальших досліджень. Тому деякі аспекти вимагають більш детального аналізу.

Насамперед, насьогодні зростає популярність створення кібервійськ, які мають на меті не лише захист критичної інформаційної інфраструктури від кібератак, але й проведення превентивних наступальних операцій у кіберпросторі. Зазначене включає в себе здійснення атак на критично важливі об’єкти противника шляхом викривлення інформаційних систем, які керують цими об’єктами.

Важливо виділити дві ключові особливості державного регулювання у сфері захисту кіберпростору.

По-перше, в Україні безпека кіберпростору має відповідати стандартам демократичної держави та принципам верховенства права, при цьому мінімізуючи потенційні обмеження прав людини на інформацію [4].

Тому, ми погоджуємось з думкою Гнатченка Д.Д., що кіберпростір виступає як ключовий канал для обміну інформацією в сучасному суспільстві та є важливою частиною його інформаційної сфери [5, с. 49].

По-друге, на рівні адміністративно-правового регулювання процесів кібербезпеки відсутні систематичні заходи державного регулювання у сфері захисту кіберпростору, і їх перелік не є чітко визначеним [6].

Наша думка полягає в тому, що сучасна практика національного нормотворення в цьому питанні залишає певні недоліки. Тому стратегія ефективного управління системою державного регулювання в сфері захисту кіберпростору повинна бути гнучкою і враховувати сучасні виклики та реалії. Вона має бути доповненою або уточненою відповідно до нових обставин.

Отже, наша думка, для вирішення проблем інформаційного забезпечення в Україні важливо дотримуватись основних правил кібергігієни щодо боротьби з фейками: віддавати перевагу лише офіційним та перевіреним джерелам інформації, уникаючи сумнівних постів у соціальних мережах [7, с. 45]. У той же час необхідно мати на увазі, що навіть довірені медіа та офіційні особи можуть допускати помилки, особливо у період воєнного стану.

Після того, як ви дізнаєтеся важливу новину, важливо зачекати на її підтвердження або спростування. У випадку з діпфейками ситуація стає складнішою, оскільки це підроблені відеозаписи, на яких може бути зображена публічна особа та почута її промова. Наприклад, у Центрі інформаційної безпеки повідомляли, що у мережі може з’явитися відеозвернення Президента Володимира Зеленського про капітуляцію, проте це технологія машинного навчання, спрямована на заплутування слухачів та розбиття бойового духу наших громадян. У таких випадках важливо звернути увагу на наступні ознаки: неприродний тон виступу, текстуру шкіри, тіні на обличчі, «мерехтіння кадру», кліпання очей і таке інше. Головне правило – довіряти лише офіційним джерелам інформації [8, с. 5].

Враховуючи вищевикладене, слід зазначити, що для вирішення нагальних проблем важливо додатково вивчати позитивний досвід країн НАТО у сфері захисту кіберпростору, проведення кібероперацій, навчання фахових спеціалістів та інше. Крім цього, досвід останніх десятиліть зі збройних конфліктів та широкомасштабна агресія росії проти України підтверджують, що у сучасній війні перемагає той, хто швидше адаптується до нових інформаційних технологій та впроваджує їх у життя, розвиває нові воєнні доктрини і концепції, що відповідають сучасним викликам.

Список використаних джерел:

1. Бурбело Б. А. Криміналістичні основи протидії кіберзлочинності. Актуальні питання розслідування кіберзлочинів: матеріали міжнародної науково-практичної конференції (Харків, 10 грудня 2013 р.). Харків: Харківський національний університет внутрішніх справ. 2013. С. 179–182.

2. Погорецький М., Шеломенцев В. Кіберзлочини: до визначення поняття. Вісник прокуратури. 2012. № 8. С. 89–96.

3. Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти: монографія. К. : ДКС, 2011. 342 с.

4. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

5. Гнатченко Д. Д. Державне регулювання у сфері захисту кіберпростору як компонент забезпечення інформаційної безпеки України. Київ. нац. торг.-екон. ун-т, 2020.

6. Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серп. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

7. Кудінов В. А., Яровий К. В. Комплексний підхід щодо створення стійких паролів інформаційних систем спеціального призначення МВС та Національної поліції України (частина 1). Сучасна спеціальна техніка. 2023. № 3 (74). С. 42-49.

8. Шестак Я. І. Кібергігієна у інформаційному просторі в умовах воєнного стану. Кібергігієна у інформаційному просторі в умовах воєнного стану. Тези V міжнародної науково-практичної конференції: «Інформаційна безпека та комп’ютерні технології». Центральноукраїнський національний технічний університет, Кропивницький, 2022. С. 5-6.