МВС України
Харківський національний університет внутрішніх справ
Науковий парк «Наука та безпека»

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Збірник матеріалів

Міжнародної науково-практичної конференції

(м. Вінниця, 31 травня 2023 року)

Вінниця

2023

УДК [351.74:004](477)(08)
П83

Друкується згідно з рішенням оргкомітету
за дорученням Харківського національного університету внутрішніх справ
від 18.01.2023 № 3

Протидія кіберзлочинності та торгівлі людьми :
П83 зб. матеріалів міжнарод. наук.-практ. конф. (м. Вінниця, 31 трав. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». – Вінниця : ХНУВС, 2023. – 176 с.

У матеріалах конференції окреслено найбільш актуальні проблеми протидії кіберзлочинності та торгівлі людьми на сучасному етапі; проаналізовано питання правового та організаційного забезпечення протидії кіберзлочинності та торгівлі людьми; кримінально-правові, процесуальні та криміналістичні аспекти протидії цьому негативному явищу; розглянуто відповідний міжнародний досвід, а також кадрове забезпечення правоохоронних органів. Досліджено використання інформаційних технологій і технічних засобів у протидії кіберзлочинності та торгівлі людьми.

УДК [351.74:004](477)(08)

Матеріали викладено в авторській редакції з незначними коректорськими правками. За достовірність наукового матеріалу, професійного формулювання, фактичних даних, цитат, власних назв, географічних назв, а також за розголошення фактів, що не належать відкритому друку, тощо відповідають автори публікацій та їх наукові керівники.

Електронна копія збірника розміщується у відкритому доступі на сайті Харківського національного університету внутрішніх справ (http://www.univd.edu.ua) у розділі «Наука», сторінка «Конференції, семінари та круглі столи», а також у репозитарії ХНУВС (http://dspace.univd.edu.ua/xmlui/).

5. Бондар В. Протидія торгівлі людьми в умовах воєнного стану. Голос України. URL: http://www.golos.com.ua/article/361824.

6. В Україні презентували чат-бот з протидії торгівлі людьми «Залишайся в безпеці». Юридична Газета online. URL: https://yur-gazeta.com/golovna/v-ukrayini-prezentuvali-chatbot-z-protidiyi-torgivli-lyudmi-zalishaysya-v-bezpeci.html.

Одержано 01.05.2023

УДК 342.7

ТІЩЕНКО Владислав Олександрович,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ;

ЛОГВИНЕНКО Євгенія Сергіївна,
кандидат юридичних наук, доцент,
доцент кафедри конституційного
і міжнародного права факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-7687-843X

ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Україна під час широкомаштабної агресії російської федерації стикається з різноманітними видами кібератак. Агресор намагається заблокувати надання електронних послуг, що призводить до порушення прав громадян та збоїв у роботі державних органів, відбуваються фішингові атаки електронною поштою, порушується цілісність і конфіденційність персональних даних, тим самим створюється інформаційно-психологічний тиск на населення. До того ж кібертероризм та кібершпигунство в економічній сфері є не менш небезпечними, оскільки націлені на підрив економічних устоїв нашої держави та провокування соціального невдоволення населення. Тому завдання щодо створення в Україні власної ефективної й дієвої системи протидії кіберзагрозам є актуальним і саме ця сфера потребує проведення змістовних реформ.

Кіберпростір разом з іншими фізичними просторами визнано одним з театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об’єктів противника шляхом руйнування інформаційних систем, які управляють такими об’єктами.

Фундаментом дієвої системи кібербезпеки, безумовно, є ефективна нормативно-правова база, а тому слід відзначити актуальність Указу Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» від 26.08.2021 р. [1]. У ньому відповідно до зазначеної стратегії передбачено перспективи створення максимально вільного та безпечного, відкритого і стабільного кіберпростору в інтересах забезпечення прав людини. Сьогодні, коли Україна знаходиться в умовах воєнного стану, важливим є не лише для ІТ-фахівців, але й для будь-якого громадянина

мати необхідні знання щодо застосування цифрової грамотності, дотримання цифрового етикету та правил кібергігієни. З початком війни ІТ-фахівці з усієї країни долучилися до кіберполіції та зуміли дати відсіч агресору. В результаті злагоджених дій було виведено з ладу критично важливі інформаційні системи окупанта.

Насамперед, потрібно дотримуватись важливого правила кібергігієни у боротьбі з фейками: читати лише офіційні та перевірені джерела, а не сумнівні пости в соцмережах. Водночас потрібно пам'ятати, що в умовах воєнного часу навіть надійні медіа та офіційні особи можуть помилятися. Прочитавши важливу новину, треба дочекатися її спростування чи підтвердження. Щодо діпфейків, то тут складніша ситуація, оскільки це підроблене відео, на якому можна побачити публічну особу та відповідно почути її промову. Так, у Центрі інформаційної безпеки повідомляли, що у мережі може з'явитися відеозвернення Президента Володимира Зеленського начебто про капітуляцію. Однак це технологія машинного навчання використовується з метою заплутати слухача і зламати бойовий дух наших громадян. У цьому випадку слід звернути увагу на наступні ознаки: неприродній тон виступу, текстуру шкіри, тіні на обличчі, «мерехтіння кадру», кліпання очей тощо. І головне – довіряти лише офіційним засобам інформації [2, с. 5].

Варто виокремити дві важливі особливості державного регулювання у сфері захисту кіберпростору. Перша полягає у тому, що відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» безпека кіберпростору повинна відповідати вимогам демократичного державного устрою та верховенства права при зведеному до мінімуму потенційному обмеженні права людини на інформацію [3]. О. Яременко пояснює це тим, що кіберпростір є своєрідним «провідником» інформації для процесів і є домінуючою частиною інформаційної сфери сучасного суспільства. Друга особливість полягає в тому, що на рівні адміністративно-правового регулювання процесів кібербезпеки, заходи державного регулювання у галузі захисту кіберпростору не визначаються систематично, і вони не мають чіткого переліку. Отже головною передумовою державної регуляторної політики у сфері захисту кіберпростору є створення нормативної та термінологічної бази в галузі кібербезпеки. На наш погляд, сьогодні національна практика нормотворення з цього питання не є достатньою. Тому стратегія ефективного функціонування системи державного регулювання у сфері захисту кіберпростору має враховувати виклики і реалії сьогодення, доповнюватись або ж уточнюватись відповідно до новоутворенних обставин [4, с. 49]. Також важливим є вивчення позитивного досвіду країн НАТО у сфері захисту кіберпростору, проведення кібероперацій, підготовки фахових спеціалістів тощо [5, с. 169].

Таким чином, практика збройних конфліктів останніх десятиліть та широкомаштабна агресія росії проти України свідчать, що в сучасній війні перемагає той, хто швидше оволодіває новими інформаційними технологіями та втілює їх у життя, бере на озброєння нові воєнні доктрини і концепції, які відповідають реаліям сьогодення. Перемагають ті, у кого командири не тільки самі використовують нові технології та ідеї, а й добре знають, які з них може використовувати противник.

Список використаних джерел

1. 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

2. 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»*. Ценральноукраїнський національний технічний університет, Кропивницький, 2022. С. 5-6.

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

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

5. Даник Ю. Г. Сучасні інформаційні технології в забезпеченні національної безпеки і оборони: реалії та тенденції розвитку. *Modern Information Technologies in the Sphere of Security and Defence* № 1(31), 2018.

Одержано 26.04.2023

УДК 343.431-053.2

ФІЛІПСЬКА Наталія Олександрівна,
кандидат юридичних наук,
старший викладач кафедри конституційного
і міжнародного права факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-9558-9422

ДІТИ І МОЛОДЬ ЯК ПОТЕНЦІЙНІ ЖЕРТВИ ТОРГІВЛІ ЛЮДЬМИ У КІБЕРПРОСТОРІ

Сучасна людина не може уявити свого існування без результатів досягнень сучасної науки та техніки, особливо у сфері інформаційних технологій. Використання гаджетів, які мають постійний доступ до Всесвітньої мережі Інтернет, успішно забезпечують потреби людини у інформації, спілкуванні, бізнесі, отриманні державних послуг, спрощують безліч побутових процесів – оплата товарів та послуг, купівля-продаж тощо. Однак, так же успішно використовуються ці технології і у вчиненні злочинних дій. Економіки європейських держав та США зазнають серйозної шкоди від кіберзлочинності. Згідно з дослідженням, у 2018 році кіберзлочинність принесла в США щонайменше 1,5 трильйона доларів прибутку [1, с. 18].

На жаль, злочинці йдуть у ногу з часом, технологіями та удосконалюють методи своєї незаконної діяльності. Це стосується і торгівців людьми. Злочинці у цій сфері також успішно використовують сучасні досягнення для залучення нових жертв, організації незаконної експлуатації людей, при цьому, жертвами можуть бути і чоловіки, і діти, і представники вразливих верств населення (мігранти, люди з обмеженими можливостями тощо). Слід розуміти, що в поняття «торгівля людьми» входить ціла низка окремих, часто вкрай небезпечних злочинів – проституція та інші форми сексуальної експлуатації, примусова праця, рабство або подібна практика поводження, незаконна торгівля органами або людьми, примусове жебракування, використання дітей як комбатантів, примусовий шлюб